Portfolio optimization of structural safety measures for dynamic 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

We develop a method to support the selection of cost-efficient portfolios of structural safety measures for dynamic systems. The method captures the temporal evolution of component failures and the dynamics of accident scenarios. We represent combinations of events possibly leading to system failure through Dynamic Bayesian Networks. Then, we identify all Pareto optimal portfolios of safety measures which are cost-efficient in minimizing the residual risk of the system. The portfolios are found by a computationally efficient algorithm, which considers budget and feasibility constraints of the safety measures. The method is illustrated by revisiting the accident scenario of a vapour cloud ignition occurred at Universal Form Clamp in Bellwood, Illinois, U.S. on 14 June 2006. The results are shown for different costs of implementing the safety measures, which provides additional insights on risk management.

Keywords: Risk Analysis, Safety measures, Risk Importance Measures, Dynamic Bayesian Networks, Portfolio Optimization.

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

1 Introduction

The selection of measures to reduce the risk of industrial accidents is a crucial decision in safety management. In industrial practice, this task is addressed through an iterative procedure based on Risk Importance Measures (RIM, [1]) to evaluate the impacts of changes in the reliability of individual system components on the system risk. Safety measures are selected to reduce the failure probabilities of those components whose impact on the system risk is the highest. The procedure is iterated until the budget for safety measures is depleted or the risk is reduced to acceptable levels.

In a recent study [2], we showed that the RIM-based iterative procedure does not necessarily lead to a cost-efficient allocation of the safety measures. Rather, this can be achieved by selecting safety measures in the framework of Portfolio Decision Analysis [3]. Thus, we proposed a methodology which builds on Bayesian Network (BN) to model sequences of events that can lead to accidents. This probabilistic model helps assess the system risk and compute the optimal portfolios of safety measures which minimize the residual risk. It thus responds to the need for intuitive and computationally efficient methodologies for risk analysis [4, 5, 6]. Bayesian Networks are useful in that they (i) circumvent the limitations of binary representation of failure processes by encoding multi-state events, (ii) extend the concepts of AND/OR gates to provide more flexibility to model the accident scenarios and (iii) help combine expert judgements and quantitative knowledge for risk estimation [2].

However, the methodology does not account for the time-dependent interactions of events [7, 8]. Thus, it may fail to consider severe outcomes of accident scenarios which depend on the order, timing and magnitude of the component failures [9, 10, 11].

In this paper, we extend the methodology to time-dependent accident scenarios by explicitly encoding the dynamic behaviour of engineering systems. For this extension, we rely on Dynamic Bayesian Networks (DBNs), which generalize BNs by connecting nodes over successive time steps [12]. DBNs have been successfully applied in various fields, like networked information systems [13], medical science [14], simulation analysis [15] and also reliability engineering. For instance, Boudali et al. [16] investigate discrete-time BNs for dynamic systems and illustrate their capabilities in the risk assessment and safety analysis of complex process systems. Barua et al. [17] propose a risk assessment methodology for dynamic systems based on a DBN capturing the changes of the component states over time. However, neither one of these approaches addresses the selection of safety measures.

Khankzad et al. [18] use DBNs to consider the allocation of safety measures in dynamic systems by maximizing the risk reduction and cost-efficiency. Their approach targets the riskiness of single accident scenarios by comparing the impacts of alternative safety measures before the most effective ones are selected. However, the analysis of the single accident scenarios may be very demanding in complex systems in which the number of such scenarios can be large. Furthermore, by comparing only the individual safety measures to each other, the procedure

fails to consider the impact of combinations of safety measures on the system. Consequently, the resulting solutions can be suboptimal [2].
We propose a methodology based on Portfolio Decision Analysis [3] to compute cost-efficient portfolios of safety measures for dynamic systems. In particular, we consider structural safety measures for time-dependent accident scenarios. Structural safety measures are installed before the system is into operation, thus they are not dynamically activated or deactivated depending on the specific states of the system. On the other hand, we do not consider safety measures such as failure-recovery processes of the system components, control system actions and operator actions.
The rest of the paper is structured as follows. Section 2 presents the methodology, including the formulation of the DBN and the probabilistic model. Section 3 revisits an earlier case study concerning the accident scenario of a vapour cloud ignition [19] and analyses the portfolios of safety measures based on the dominance condition over successive time steps. Section 4 discusses the potential of the proposed methodology. Finally, Section 5 concludes the paper and outlines extensions for future research.

2 Problem formulation

The formulation of a DBN for reliability engineering is undertaken by analysing the process system in detail. This analysis often starts from the development of Fault Trees and Event Trees [20].
Formally, a DBN is a Directed Acyclic Graph (DAG) consisting of a composition of dependent BNs evolving over the time steps $\tau \in \mathbb{T} = \{0, 1, ..., \mathcal{T}\}$. Specifically, the set $V = \{1, ..., N\}$ represents the system components $i \in V$, whose state at time τ is described by the random variable $X^i(\tau)$. In the DBN, the node $V^i(\tau)$ represents the random variable $X^i(\tau)$, whereas directed arcs indicate causal dependencies between nodes. In particular, causal dependences between nodes at time $\tau \in \mathbb{T}$ are defined by the internal arcs

$$E_{int}(\tau) = \{[V^j(\tau) \rightarrow V^i(\tau)] | i \in V;\, j \in V;\, i \neq j\}, \tag{1}$$

where $[V^j(\tau) \rightarrow V^i(\tau)]$ indicates that the state of component $j \in V$ at time τ influences the state of component $i \in V$ at the same time. The internal arcs $E_{int}(\tau)$ can be different for each DAG

$$\mathcal{G}(\tau) = \{(v, e) | v \in V(\tau),\, e \in E_{int}(\tau)\}, \tag{2}$$

where $V(\tau) = \{V^i(\tau) | i \in V\}$ is the set of nodes $V^i(\tau)$.
The DBN also considers causal dependences between nodes at different time steps to capture the dynamic behaviour of accident scenarios. These dependencies are encoded by the external arcs $E_{ext}(\tau)$ such that $E_{ext}(0) = \emptyset$, i.e., at time $\tau = 0$ there are no dependencies to previous

time steps. For $\tau > 0$, we define the external arcs as

$$E_{ext}(\tau) = \{[V^j(\tau - \delta) \to V^i(\tau)] | i \in V;\, j \in V;\, \delta \in \{1, ..., \tau\}\}. \tag{3}$$

The DBN at time $\tau \in \mathbb{T}$ is then represented by the DAG

$$\mathcal{B}(\tau) = \{(v, e) | v \in V(\delta),\, e \in E_{int}(\delta) \cup E_{ext}(\delta),\, 0 \leq \delta \leq \tau\}. \tag{4}$$

The immediate predecessors of node $V^i(\tau)$ are indicated by set

$$V^i_-(\tau) = \{j \in V(\tau - \delta) | [V^j(\tau - \delta) \to V^i(\tau)] \in E_{int}(\tau) \cup E_{ext}(\tau);\, \delta = 0, ..., \tau\}. \tag{5}$$

Thus, all nodes can be partitioned into the set of *leaf nodes* $V^L = \{V^i(\tau) | V^i_-(\tau) = \emptyset,\ \tau \in \mathbb{T}\}$ and its complement set of *dependent nodes* $V^D = \{V^i(\tau) | V^i_-(\tau) \neq \emptyset,\ \tau \in \mathbb{T}\}$.
The residual risk of the system is evaluated at one or multiple safety target nodes $V^T \subseteq V$, which represent the final outcomes of the accident scenario on safety, asset operation and environment. Safety measures can be implemented on a subset of components $V^A \subseteq V$ at the outset of the accident scenario to mitigate the risk of the system.
Formally, at component $i \in V^A$ the set of alternative safety measures is $\mathbb{A}^i = \{1, ..., |\mathbb{A}^i|\}$, where the operator $|\cdot|$ indicates the cardinality of the set. The binary variable z^i_a represents the choice on safety measure $a \in \mathbb{A}^i$, which will affect nodes $V^i(\tau)$ at every time $\tau \in \mathbb{T}$. Specifically, the binary variables z^i_a is 1 if a is applied for any time $\tau \in \mathbb{T}$, and 0 otherwise.
Thus, the portfolio of safety measures $A \in \mathsf{X}_{i \in V^A} \mathbb{A}^i$ is defined by vector $\mathbf{z}$, which is the concatenation of vectors $\mathbf{z}^i = (z^i_1, ..., z^i_{|\mathbb{A}^i|})$, where the operator $\mathsf{X}_{i \in V^A}$ is the Cartesian product of sets $\mathbb{A}^i$. There are no safety measures available for components $i \in V \backslash V^A$: this is modelled by $\mathbb{A}^i = \emptyset$ so that $|\mathbb{A}^i| = 0$. The size of the binary vector $\mathbf{z}$ is $\mathcal{M} = \sum_{i \in V^A} |\mathbb{A}^i|$.
The binary vector $\mathbf{z}$ is built such that

$$z_k = z^{j^*}_\lambda \tag{6}$$

where

$$j^* = \min\{j \in V^A | \sum_{i=1}^{j} |\mathbb{A}^i| \geq k\}, \tag{7}$$

$$\lambda = k - \sum_{i < j^*} |\mathbb{A}^i|. \tag{8}$$

2.1 Probability model

The realization s of the random variable $X^i(\tau)$ belongs to the discrete set of states $\mathbb{S}^i$, which consists of events with different contributions to the risk of the system [21]. Uncertainty about the realization of $X^i(\tau)$ at nodes $V^i(\tau) \in V^L$ is modelled through the probability mass distribution $\mathbb{P}^s_{X^i(\tau)} = \mathbb{P}[X^i(\tau) = s] \geq 0$ such that

$$\sum_{s \in \mathbb{S}^i} \mathbb{P}^s_{X^i(\tau)} = 1,\ \forall i \in V^L. \tag{9}$$

The model supports the selection of cost-efficient safety measure(s) for each component from a finite number of alternatives, by accounting for the implementation costs c_a^i and the impact on the failure probabilities of the components at each time step $\tau \in \mathbb{T}$.
Without losing generality, we assume that the safety measures at component $i \in V^A$ are mutually exclusive. This implies that at most one safety measure can be selected from set $\mathbb{A}^i$ so that

$$\sum_{a \in \mathbb{A}^i} z_a^i \leq 1, \quad \forall i \in V^A. \tag{10}$$

Applying a safety measure $a \in \mathbb{A}^i$ at leaf nodes $V^i(\tau) \in V^L$ modifies the probability distribution by turning $\mathbb{P}^s_{X^i(\tau)}$ into $\mathbb{P}^s_{X_a^i(\tau)}$, where

$$\sum_{s \in \mathbb{S}^i} \mathbb{P}^s_{X_a^i(\tau)} = 1, \quad \forall a \in \mathbb{A}^i. \tag{11}$$

Then, the marginal probability of the realization $s \in \mathbb{S}^i$ at leaf node $V^i(\tau) \in V^L$ is

$$\mathbb{Q}^s_{X^i(\tau)}(\mathbf{z}) = \begin{cases} \mathbb{P}^s_{X^i(\tau)}(\mathbf{z}), & \text{if } z_a^i = 0 \; \forall a \in \mathbb{A}^i \\ \sum_{a \in \mathbb{A}^i} z_a^i \; \mathbb{P}^s_{X_a^i(\tau)}(\mathbf{z}), & \text{otherwise} \end{cases}. \tag{12}$$

The total probability of the realization $s \in \mathbb{S}^i$ at dependent node $V^i(\tau) \in V^D$ depends on the states of its predecessors. To model this relationship, we define the random variable $\mathbf{X}^i_-(\tau)$ as the $|V^i_-(\tau)|$-dimensional vector composed of the random variables $X^j(\tau - \delta)$ for all $j \in V^i_-(\tau)$, $\delta = 0, ..., \tau$. Let $\mathbb{S}^i_-(\tau)$ be the Cartesian product of the sets of states $\mathbb{S}^j$ of all the predecessors $j \in V^i_-(\tau)$, then the vector $\mathbf{x}^i_-(\tau) \in \mathbb{S}^i_-(\tau)$ represents a possible realization of $\mathbf{X}^i_-(\tau)$.
The calculation of the total probabilities $\mathbb{Q}^s_{X^i(\tau)}$ starts from the leaf nodes $V^i(0) \in V^L$ and proceeds to the dependent nodes $V^i(0) \in V^D$ in the order of increasing node depth

$$\mathcal{D}^i(0) = \begin{cases} 0, & V^i_-(0) = \emptyset \\ 1 + \max_{j \in V^i_-(0)} \mathcal{D}^j(0), & V^i_-(0) \neq \emptyset \end{cases}. \tag{13}$$

After having solved the DAG $\mathcal{G}(0)$, the calculation of the total probabilities $\mathbb{Q}^s_{X^i(\tau)}$ proceeds by increasing the time step $\tau \geq 1$ progressively in the order of the node depth

$$\mathcal{D}^i(\tau) = \begin{cases} 0, & V^i_-(\tau) = \emptyset \\ 1 + \max_{j \in V^i_-(\tau)} \mathcal{D}^j(\tau), & V^i_-(\tau) \neq \emptyset \end{cases}. \tag{14}$$

This procedure is needed because the calculation of the total probability $\mathbb{Q}^s_{X^i(\tau)}$ depends on the total probabilities $\mathbb{Q}^s_{X^j(\tau)}$ of all predecessors $j \in V^i_-(\tau)$.
The conditional probability of state $s \in \mathbb{S}^i$ at dependent nodes $V^i(\tau) \in V^D$ is

$$\mathbb{Q}^s_{X^i(\tau)|\mathbf{x}^i_-(\tau)}(\mathbf{z}) = \sum_{a \in \mathbb{A}^i} z_a^i \; \mathbb{P}^s_{X_a^i(\tau)|\mathbf{x}^i_-(\tau)}(\mathbf{z}) \tag{15}$$

where $\mathbb{P}^s_{X_a^i(\tau)|\mathbf{x}^i_-(\tau)}$ is the conditional probability of state $s \in \mathbb{S}^i$ of component $i \in V$, given that its predecessors are in states $\mathbf{x}^i_- \in \mathbb{S}^i_-(\tau)$ of its predecessors and the safety measure $a \in \mathbb{A}^i$ is

implemented.

Based on the conditional independence of the predecessors $V^i_-(\tau)$ resulting from the d-separation [22], the total probability $\mathbb{Q}_{\mathbf{x}^i_-(\tau)}$ of the vector of states $\mathbf{x}^i_-(\tau) \in \mathbb{S}^i_-(\tau)$ is the product of the total probabilities of the states $\mathbf{x}^i_-(\tau) \in \mathbb{S}^i_-(\tau)$. Thus, the total probability of the realization $s \in \mathbb{S}^i$ can now be expressed recursively as

$$\mathbb{Q}^s_{X^i(\tau)}(\mathbf{z}) = \sum_{\mathbf{x}^i_-(\tau) \in \mathbb{S}^i_-(\tau)} \left[\sum_{a \in \mathbb{A}^i} z^i_a \, \mathbb{P}^s_{X^i_a(\tau)|\mathbf{x}^i_-(\tau)}(\mathbf{z}) \right] \mathbb{Q}_{\mathbf{x}^i_-(\tau)}(\mathbf{z}), \tag{16}$$

where the first summation is taken over all possible realizations $\mathbf{x}^i_-(\tau) \in \mathbb{S}^i_-(\tau)$. Here the total probability $\mathbb{Q}^s_{X^i(\tau)}$ is a multiplicative function of the safety measures that have been applied along the paths leading from the leaf nodes to the dependent nodes $V^i(\tau) \in V^D$.

The portfolio of safety measures $\mathbf{z}$ for mitigating the residual risk of the system is evaluated in terms of the expected disutility of safety targets $V^T \subset V$ over one or more time steps. Specifically, for the portfolio $\mathbf{z}$ the expected disutility of the safety target $t \in V^T$ at time τ is

$$\mathbb{U}_{X^t(\tau)}(\mathbf{z}) = \sum_{s \in S^t} \mathbb{Q}^s_{X^t(\tau)}(\mathbf{z}) \cdot u^s_{X^t}, \tag{17}$$

where $u^s_{X^t}$ is the disutility of the severity of state $s \in S^t$. Specifically, $u^s_{X^t} = 0$ if state $s \in \mathbb{S}^t$ does not involve any harmful consequences and $u^s_{X^t} = 100$ if state $s \in \mathbb{S}^t$ is the consequence of highest severity. If $|\mathbb{S}^t| > 2$, the other intermediate states can be assigned disutilities in the range $(0, 100)$ by expert judgements relative to the states with disutilities of 0 and 100. Estimates for $u^s_{X^t}$ for each $s \in \mathbb{S}^t$ can be elicited through trade-off weighing approaches SWING [23] or SMARTS [24].

2.2 Dominance structure

The optimization model minimizes the expected disutility $\mathbb{U}_{X^t(\tau)}(\mathbf{z})$ over the time steps $\tau \in \mathbb{T}$ by accounting for the constraints of risk acceptability and feasibility. Among the feasibility constraints, the overall cost of the portfolio must not exceed the budget constraint B.

Let $\mathcal{M} = \sum_{i \in V^A} |\mathbb{A}^i|$ be the size of the binary vector $\mathbf{z}$. The set of feasible portfolios is defined by a set of $\mathcal{L}$ linear inequalities whose coefficients are in the matrix $H \in \mathbb{R}^{\mathcal{L} \times \mathcal{M}}$ ($h^\ell_j = [H]_{\ell j}$) and vector $\mathbf{b} = [b^1, ..., b^{\mathcal{L}}] \in \mathbb{R}^{\mathcal{L}}$. The set of feasible portfolios is

$$\mathbf{Z}_F = \{\mathbf{z} \in \{0,1\}^{\mathcal{M}} | H\,\mathbf{z} \leq \mathbf{b}\}, \tag{18}$$

where $\leq$ holds componentwise. Specifically, the selection of safety measures needs to fulfil the constraints related to the uniqueness of the selected safety measure(s) for each component by Eq. (10) and the budget constraint

$$\sum_{i \in V^A} \sum_{a \in \mathbb{A}^i} z^i_a \, c^i_a \leq B. \tag{19}$$

It is possible to specify additional constraints to represent the properties of the system. For instance, if the safety measures for improving the reliability of component $i \in V$ and component $j \in V$ are mutually exclusive, then

$$\sum_{a \in \mathcal{A}^i} z_a^i + \sum_{a \in \mathcal{A}^j} z_a^j \leq 1. \tag{20}$$

Conversely, if at least one safety measure at components $i \in V$ and $j \in V$ must be applied, the corresponding constraint is

$$\sum_{a \in \mathcal{A}^i} z_a^i + \sum_{a \in \mathcal{A}^j} z_a^j \geq 1. \tag{21}$$

If there are components for which specific regulatory limits apply, a possible approach is to introduce additional constraints so that the total probability $\mathbb{Q}^s_{X^t(\tau)}$ of failure states $s \in \mathcal{S}^t$ does not exceed an acceptable threshold $\epsilon^s_{X^t}$ such that

$$\mathbb{Q}^s_{X^t(\tau)}(\mathbf{z}) \leq \epsilon^s_{X^t}, \quad \forall \tau \in \mathbb{T}. \tag{22}$$

The values of $\epsilon^s_{X^t}$ are usually provided by regulatory offices: the constraints must be respected for the risk to be acceptable. However, it is possible that no portfolios are feasible for the set of currently available constraints.

The set of non-dominated portfolios of safety measures consists of those feasible portfolios for which no other feasible portfolios has an equal or lower disutility for all time steps and strictly lower for at least one time step. Thus, it is necessary to determine the entire Pareto optimal frontier defined by the dominance condition

$$\mathbf{z}^* \succ \mathbf{z} \;\Leftrightarrow\; \begin{cases} \mathbb{U}_{X^t(\tau)}(\mathbf{z}^*) \leq \mathbb{U}_{X^t(\tau)}(\mathbf{z}) & \text{for all } \tau \in \mathbb{T} \\ \mathbb{U}_{X^t(\tau)}(\mathbf{z}^*) < \mathbb{U}_{X^t(\tau)}(\mathbf{z}) & \text{for some } \tau \in \mathbb{T} \end{cases}, \tag{23}$$

for any pair of feasible portfolios $\mathbf{z}, \mathbf{z}^* \in \mathbf{Z}_F$.

Our optimization algorithm determines the set of non-dominated portfolios of safety measures as

$$\mathbf{Z}_{ND} = \{\mathbf{z}^* \in \mathbf{Z}_F | \nexists\, \mathbf{z} \in \mathbf{Z}_F \; s.t. \; \mathbf{z} \succ \mathbf{z}^*\}. \tag{24}$$

Analogously to Liesiö et al. [25, 26], the core index $CI(a)$ is defined as the share of non-dominated portfolios that include the safety measure $a \in \mathbb{A}^i$

$$CI(a) = \frac{|\{\mathbf{z}^* \in \mathbf{Z}_{ND} | z_a^i = 1\}|}{|\mathbf{Z}_{ND}|}. \tag{25}$$

The analysis of the core indexes helps identify those safety measures that should be selected or rejected. If the core index of a safety measure is 1, the safety measure is included in all non-dominated portfolios; on the other hand, if the core index is 0, the safety measure is not included in any non-dominated portfolio. Finally, safety measures whose core index is in the range $(0, 1)$ require further analysis in order to be selected or rejected [27].

2.3 Optimization algorithm

We propose an implicit optimization algorithm to identify the non-dominated portfolios $\mathbf{z}^*$ of safety measures over time steps. The algorithm (an adaptation of Liesiö [28]) computes the set $\mathbf{Z}_{ND}$ of non-dominated portfolios $\mathbf{z}^* \in \mathbf{Z}_{ND}$ that minimize the expected disutility $\mathbb{U}_{X^t(\tau)}(\mathbf{z}^*)$ for every time step $\tau \in \mathbb{T}$. A portfolio of safety measures corresponds to the binary vector $\mathbf{z} = [z_1, ..., z_{\mathcal{M}}]$, which is the concatenation of vectors $\mathbf{z}^i$, $\forall i \in V^A$ as described by Eq. (6).

The algorithm first initializes the sets $\mathbf{Z}^*$ and $\mathbf{Z}_D$ as empty sets. Specifically, the set $\mathbf{Z}^*$ includes potential non-dominated portfolios whereas set $\mathbf{Z}_D \subseteq \mathbf{Z}^*$ includes dominated portfolios belonging to $\mathbf{Z}^*$. Both sets are updated at every iteration of the algorithm. If the solution of not installing any additional safety measure is feasible, the portfolio $\mathbf{z} = [0, ..., 0]$ is included in the set $\mathbf{Z}^*$ as a potential non-dominated solution.

The algorithm enumerates the possible portfolios starting from $\mathbf{z} = [0, ..., 0]$ by pursuing two main parts: *Forward-loop* and *Backtrack step*. The *Forward-loop* progressively sets $z_k = 1$ in an increasing order of the index variable k. If the portfolio $\mathbf{z} \in \mathbf{Z}_F$ is not dominated by any $\mathbf{z}^* \in \mathbf{Z}^*$, the algorithm updates the set $\mathbf{Z}^*$ by including the portfolio $\mathbf{z}$ and removing any dominated portfolios $\mathbf{Z}_D = \{\mathbf{z}^* \in \mathbf{Z}^* | \mathbf{z} \succ \mathbf{z}^*\}$.

The *Forward-loop* can only increment the values $z_{k+1}, ..., z_{\mathcal{M}}$. Thus, if the portfolio $\mathbf{z}$ is infeasible and cannot be made feasible by setting $z_j = 1$ for some indexes $j \in \{k+1, ..., \mathcal{M}\}$, there is no need to continue the *Forward-loop*, because such a continuation would produce infeasible portfolios only. This fathoming condition avoids the enumeration of all $2^{\mathcal{M}}$ possible portfolios. Alternatively, the *Forward-loop* terminates when k reaches $\mathcal{M}$ whereafter the algorithm backtracks. The *Backtrack step* sets $z_{\mathcal{M}} = 0$, identifies the greatest index k such that $z_k = 1$ and sets $z_k = 0$. If such an index does not exist, the algorithm terminates; otherwise the *Forward-loop* is repeated. When the algorithm terminates, the set $\mathbf{Z}^*$ contains the set of non-dominated portfolios $\mathbf{Z}_{ND}$.

The algorithm has been coded in C++ programming language and linked to GeNIe Modeler, a development environment for reasoning in graphical probabilistic models, developed by BayesFusion LCC and available at `http://www.bayesfusion.com/`.

Initialization: $\mathbf{z} = [0, ..., 0]$; $k \leftarrow 1$; $\mathbf{Z}^* \leftarrow \emptyset$; $\mathbf{Z}_D \leftarrow \emptyset$; ;
if $\mathbf{z} \in \mathbf{Z}_F$ **then**
  $\mathbf{Z}^* \leftarrow \mathbf{z}$;
end
while $k > 0$ **do**
  Forward-loop:
  while $k \leq \mathcal{M}$ **do**
    $z_k \leftarrow 1$;
    if $\mathbf{z} \in \mathbf{Z}_F$ and $\mathbf{z}^* \not\succ \mathbf{z}\ \forall \mathbf{z}^* \in \mathbf{Z}^*$ **then**
      $\mathbf{Z}_D \leftarrow \{\mathbf{z}^* \in \mathbf{Z}^* | \mathbf{z} \succ \mathbf{z}^*\}$;
      $\mathbf{Z}^* \leftarrow \mathbf{z} \cup \{\mathbf{Z}^* \backslash \mathbf{Z}_D\}$;
    end
    if $\sum_{j=1}^{k} z_j\ h_j^\ell + \sum_{j=k+1}^{\mathcal{M}} \min\{0, h_j^\ell\} > b^\ell$ for some $\ell = 1, ..., \mathcal{L}$ **then**
      Break *Forward-loop*;
    end
    $k \leftarrow k + 1$;
  end
  Backtrack step:
  $z_{\mathcal{M}} \leftarrow 0$;
  $k \leftarrow \max[\{j | z_j = 1\} \cup \{0\}]$;
  if $k > 0$ **then**
    $z_k \leftarrow 0$;
    $k \leftarrow k + 1$;
  end
end
$\mathbf{Z}_{ND} \leftarrow \mathbf{Z}^*$;

Algorithm 1: The implicit enumeration algorithm.

3 Case study

We illustrate our methodology by revisiting the accident scenario of a vapour cloud ignition occurred at Universal Form Clamp in Bellwood, Illinois, U.S. on 14 June 2006. In this accident, previously analysed by Khakzad el al. [19], a flammable vapour cloud of heptane and mineral spirits overflowed from an open top mixing and heating tank. The vapour cloud ignited when it came into contact with unknown ignition sources. The accident led to one death, two injuries and significant business interruption.

In this system, the heat is provided to the tank by steam coils, whereas a temperature sensor and a pneumatic unit are installed on the tank to control operations. In addition, an operator

is checking the temperature with an infrared thermometer and he/she is expected to intervene in case of emergency. Finally, the exhaust ventilation system is installed on top of the tank to control possible vapour emissions (Figure 1).

Insert Figure 1 here.

According to the full-scale investigation conducted by the Chemical Safety Board [29], a malfunction of the temperature control system allowed the steam valves to be open long enough that the mixture heated to its boiling point, thus generating a high volume of vapour. Because the local ventilation system failed due to a broken fan belt, the vapour cloud spilled from the tank and finally ignited when exposed to an unknown ignition source. In the investigation, it was also found that even if the ventilation system had been working, it would not have had enough capacity to collect such a high volume of vapour.
Following the accident description, Khakzad et al. [19] developed the Fault Tree and Event Tree in Figure 2 to model the accident scenario and investigate the effectiveness of the safety measures. The detailed procedure to convert the Fault Tree and Event Tree to Bayesian Network is provided in the same article [19].

Insert Figure 2 here.

In this case study, we extend the Bayesian Network to a DBN to consider the temporal evolution of some events (immediate/delayed ignition) and the performance of the detection systems. Figure 3 shows the DBN, in which the safety target is *Consq*. Depending on the success or failure of the safety measures, the accident scenario has nine possible outcomes.

Insert Figure 3 here.

Specifically, the DBN accounts for $\mathcal{T} = 5$ time steps for the components following the Top Event *Vapour* due to the rapid dynamics of the accident scenario in case of vapour overflow. In Figure 3, the temporal delay δ is specified by the squared number over the respective arc. If there is no number on arc, there is no delay. For instance, the squared number $\delta = 1$ on the arc connecting *Sprinkler* to *Ignition* indicates the causal dependence of *Ignition=Spark* at time τ to the event *Sprinkler=Activation* at time $\tau - 1$ (Figure 4).

Insert Figure 4 here.

Because the vapour cloud is not toxic, any fatalities or injuries can be attributed to the vapour ignition. Note that the activation of safety measures *Sprinkler* and *Alarm* are influenced by *Ignition=Spark* or Top Event *Vapour=Overflow*, as shown by the causal dependence represented by the arcs. Specifically, the events *Sprinkler=Activation* and *Alarm=Activation* occur if vapour is ignited (*Vapour=Overflow* and *Ignition=Spark*), but with failure probabilities equal to 0.04 and 0.0013, respectively. Nevertheless, *Sprinkler* and *Alarm* can also be activated by a specific amount of vapour concentration in the air even if it is not ignited (*Vapour=Overflow* and *Ignition=No_spark*), but with a failure probability equal to 0.3 and 0.225, respectively. Table 1 specifies the conditional probability tables of *Alarm* and *Sprinkler*.

Insert Table 1 here.

Table 2 lists the system components, their symbols and their failure probability according to the analysis by Khakzad et al. [19].

Insert Table 2 here.

In addition, we assume that the activation of *Sprinkler* reduces the probability of delayed ignitions by 50%, as detailed in Table 3 (last row, columns 3 and 4).

Insert Table 3 here.

For this reason, the event *Sprinkler=Activation* would lead to a safer mode compared to its failure even if there is no fire (*Ignition=No_spark*). Thus, consequences C_1 and C_2 are less severe than C_3 and C_4, respectively: this information is helpful in the elicitation of the disutility functions and can be used to specify inequality constraints representing the ranking of the outcome severity. The third column of Table 4 shows illustrative values of disutility $u^s_{X^t}$ quantifying the severity of state $s \in S^t$, which have been defined through the trade-off weighing approach SWING [23]. Table 4 lists the nine possible outcomes of the accident scenario with the state *Safe* representing the outcome that the Top Event has not occurred (*Vapour=Controlled*).

Insert Table 4 here.

For the failure probabilities in Table 2, the probabilities of the outcomes of the accident scenario are calculated and reported in Table 5 for each time step $\tau \in \mathbb{T}$.

Insert Table 5 here.

The optimization model minimizes the expected disutility of the negative outcomes represented by safety target *Consq* through the application of safety measures on some selected system components.

Table 6 lists the alternative safety measures (second column) that can be applied on specific components (first column). Illustrative costs and updated failure probabilities of the components are reported in the last two columns of Table 6. In particular, the safety measure *Synergy* refers to a combination of *Calibration test* and *Sensor*: if both systems are installed, this synergy effect yields benefits which are greater than those of installing both safety measures as if they were independent. The updated failure probabilities of *Sprinkler* and *Alarm* refer to the two different failure scenarios detailed in Table 1.

Insert Table 6 here.

The optimization model in Section 2 identifies the non-dominated portfolios of safety measures which minimize the expected disutility of the safety target *Consq*. Solutions have been found for different values B of the budget constraint, described by Eq. (19).

Figure 5 shows the minimum expected disutility of the accident scenario for each time step $\tau \in \mathbb{T}$. The minimum expected disutility can be obtained by applying the non-dominated portfolio of safety measures that has been selected from the dominance structure of the portfolios as described by Eq. (23). For multiple non-dominated portfolios at a given budget level B (horizontal axis in Figure 5), the graph shows the minimum value of expected disutility of the safety target.

At the budget level $B = 0$, the graph shows the expected disutility as if no safety measure is applied to the system. By increasing the budget, more effective safety measures can be applied to reduce the residual risk of the system, evaluated by the expected disutility of safety target *Consq*.

The possibility of immediate ignition is the underlying cause for the expected disutility at time $\tau = 0$. Later, the activation of *Sprinkler* decreases the probability of ignition and consequently the expected disutility at time $\tau = 1$. Finally, the expected disutility of the following time steps increases due to the possibility of delayed ignition.

Insert Figure 5 here.

Figure 5 provides additional information for defining the requisite budget to meet safety targets and to quantify the reduction rates of risk by increasing the budget.

By setting the budget constraint at $B = 600$ k€, the optimization model identifies 3 non-dominated portfolios

$$\mathbf{z}_1 = [a_2^2;\ a_3^7;\ a_3^8;\ a_2^{14};\ a_3^{18};\ a_2^{19};\ a_1^{20}]$$

$$\mathbf{z}_2 = [a_2^2;\ a_3^7;\ a_2^8;\ a_2^{14};\ a_3^{18};\ a_2^{19};\ a_2^{20}]$$
$$\mathbf{z}_3 = [a_2^2;\ a_3^7;\ a_1^8;\ a_2^{14};\ a_3^{18};\ a_2^{19};\ a_3^{20}].$$

The analysis of the core indexes in Figure 6 shows that the safety measures *Duplication*, *Synergy*, *Condition monitoring*, *Hypoxic air technology* and *Quick response* must be implemented, whereas the selection of the safety measures on *A_ valve* and *Alarm* may require further analysis.

Insert Figure 6 here.

In this case, there are only a few non-dominated portfolios, thus the solutions can be analysed individually to select the optimal one. Specifically, Figure 7 shows that portfolio $\mathbf{z}_1$ dominates the other two solutions at time steps $\tau \geq 1$, but the zoomed frame at the initial time step $\tau = 0$ highlights a higher expected disutility of 0.13% and 0.45% in comparison to portfolios $\mathbf{z}_2$ and $\mathbf{z}_3$, respectively. If these increases are not deemed to be significant, then portfolio $\mathbf{z}_1$ could be recommended as the optimal solution.

Insert Figure 7 here.

4 Discussion

The case study shows one of the main advantages of employing Portfolio Decision Analysis to select cost-efficient combinations of safety measures. The methodology does not target the effects on risk of the single components, but rather it identifies non-dominated portfolios that minimize the residual risk of the system. This procedure overcomes the limitations of selecting the safety measures based on the iterative computation of RIMs [2].

The implicit enumeration algorithm proposed to identify the non-dominated portfolios is computationally viable. In our example, the computation took approximately one minute on a personal computer (Intel Core i5-5300 CPU). The optimization algorithm has been linked to GeNIe Modeler, a development environment for reasoning in graphical probabilistic models, which efficiently calculates the total probabilities of the target nodes at each time steps. The computation time depends on the number of alternative safety measures which modify the probability distributions of the component states. Nevertheless, the fathoming condition improves the algorithm efficiency by avoiding the enumeration of all $2^{\mathcal{M}}$ possible portfolios.

In addition, GeNIe Modeler makes it possible to revise the probabilistic model through changes of the nodes and/or arcs of the DBN. The code accounts for safety measures that involve the introduction/removal of components or dependencies between them. Specifically, changes due to the introduction/removal of components makes it necessary to introduce/remove the respective

nodes and to elicit/revise the corresponding probability tables. In contrast, changes in dependencies modify the dimensions and parameters of the conditional probability tables. Finally, the methodology accommodates multiple states for each component. This makes the model more realistic, although it increases the effort of eliciting the conditional probability tables.
Thanks to this comprehensive DBN representation, the optimization model distinguishes the optimal solution between a single reliable component or a combination of less reliable ones by minimizing the residual risk of the system. Note that safety measures can impact the probability distribution of the component states at a subset of time steps, even though they are implemented at the outset of the accident scenario.
For multiple non-dominated portfolios, the analysis of the core indexes supports the selection/rejection of some safety measures. However, the definition of the optimal solution implies a detailed analysis of the alternative non-dominated portfolios according to case-specific criteria. For instance, in the case study the experts might be interested in selecting the portfolio that minimizes the expert disutility at the initial time step to prevent the ignition and allow people to escape the factory. On the other hand, if the experts set a safety target in terms of residual risk, the optimal solution could be the portfolio that maximizes the time to overcome the safety target. This criterion implies the longest time to intervene and limit the severity of the accident scenario.
One limitation of this methodology is the need of specify the possible safety measures in advance, including information about their costs and impacts on the reliability of the components. For a large system this can be a challenge so it would require a hierarchical approach.

5 Conclusion and future research

In this paper, we have extended the methodology [2] to dynamic accident scenarios through Dynamic Bayesian Network. The problem is framed within Portfolio Decision Analysis to support the selection of safety measures that are cost-efficient in improving the reliability of a dynamic system. Furthermore, we have computed the entire Pareto optimal frontier of portfolios over successive time steps and applied the methodology to the accident scenario of a vapour cloud ignition occurred at Universal Form Clamp in Bellwood, Illinois, U.S. on 14 June 2006.
The methodology can be employed in the design phase of process systems to identify the optimal combination of safety measures that minimizes the residual risk. Furthermore, the high availability of sensors for condition monitoring of industrial systems makes it possible to update the probability distributions of component states for future improvements of system safety. Thus, additional safety measures can be selected afterwards as a result of new observations on component reliability.
The methodology can potentially be extended by accounting for safety measures that can be

dynamically activated or deactivated depending on the specific states of the system. This extension requires investigations based on dynamic optimization and contingent portfolio programming [30].

Acknowledgements

The research has been supported by The Finnish Research Programme on Nuclear Power Plant Safety 2015-2018. The case study has been performed using SMILE, an inference engine, and GeNIe Modeler, a development environment for reasoning in graphical probabilistic models, developed by BayesFusion LCC and available at `http://www.bayesfusion.com/`.

References

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

[2] Mancuso A., Compare M., Salo A., Zio E., *Portfolio optimization of safety measures for reducing risks in nuclear systems*, Reliability Engineering and System Safety 167, pp. 20-29 (2017).

[3] 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).

[4] Pollino C. A., Woodberry O., Nicholson A., Korb K., Hart B.T., *Parametrisation and evaluation of a Bayesian network for use in an ecological risk assessment*, Environmental Modelling and Software 22, pp. 1140–1152 (2007).

[5] Marsh W., Bearfield G., *Using Bayesian networks to model accident causation in the UK railway industry*, Probabilistic Safety Assessment and Management, pp. 3597–3602, Springer London (2004).

[6] Kabir G., Tesfamariam S., Francisque A., Sadiq R., *Evaluating risk of water mains failure using a Bayesian belief network model*, European Journal of Operational Research 240, pp. 220-234 (2015).

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

[8] 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).

[9] Aldemir T., *A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants*, Annals of Nuclear Energy 52, pp. 113–124 (2013).

[10] Zio E., Di Maio F. *A data-driven fuzzy approach for predicting the remaining useful life in dynamic failure scenarios of a nuclear power plant*, Reliability Engineering and System Safety 95, pp.49-57 (2010).

[11] Zio E., Di Maio F., Stasi M., *A data-driven approach for predicting failure scenarios in nuclear systems*, Annals of Nuclear Energy 37, pp. 482–491 (2010).

[12] Murphy K.P., *Dynamic Bayesian Networks: Representation, Inference and Learning*, Doctoral dissertation, University of California, Berkeley (2002).

[13] Frigault M., Wang L., Singhal A., Jajodia S., *Measuring network security using dynamic Bayesian network*, Proceedings of the ACM Conference on Computer and Communications Security, pp. 23-29 (2008).

[14] Onisko A., Druzdzel M.J., Austin M., *Application of dynamic Bayesian networks to cervical cancer screening*, Proceedings of Artificial Intelligence Studies 6, pp. 5-14 (2009).

[15] Poropudas J., Virtanen K., *Simulation metamodeling with dynamic Bayesian networks*, European Journal of Operational Research 214, pp. 644-655 (2011).

[16] Boudali H., Dugan J.B., *A discrete-time Bayesian network reliability modeling and analysis framework*, Reliability Engineering and System Safety 87, pp. 337-349 (2005).

[17] Barua S., Gao X., Pasman H., Mannan M.S., *Bayesian network based dynamic operational risk assessment*, Journal of Loss Prevention in the Process Industries 41, pp. 399-410 (2016).

[18] Khakzad N., Khan F., Amyotte P., *Risk-based design of process systems using discrete-time Bayesian networks*, Reliability Engineering and System Safety 109, pp. 5-17 (2013).

[19] 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).

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

[21] Levitin G., Lisnianski A., Ushakov I., *Reliability of multi-state systems: A historical overview*, Mathematical and statistical methods in reliability, World Scientific, pp. 123-137 (2003).

[22] Pearl J., *Probabilistic Reasoning in Intelligent Systems*, Morgan Kaufmann, San Francisco, California (1988).

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

[24] 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).

[25] Liesiö J., Mild P., Salo A., *Preference programming for robust portfolio modeling and project selection*, European Journal of Operational Research 181, pp. 1488–1505 (2007).

[26] 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).

[27] Tervonen T., Liesiö J., Salo A., *Modeling project preferences in multiattribute portfolio decision analysis*, European Journal of Operational Research 263, pp. 225-239 (2017).

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

[29] U.S. Chemical Safety Board, *Mixing and heating a flammable liquid in an open top tank*, Investigation No. 2006-08-I-IL, Washington DC, April 2007, `http://www.csb.gov/assets/1/19/CSBUniversalFormClampCaseStudy.pdf`.

[30] Gustafsson J., Salo A. *Contingent portfolio programming for the management of risky projects*, Operations Research 53, pp. 943-953 (2005).

Figures

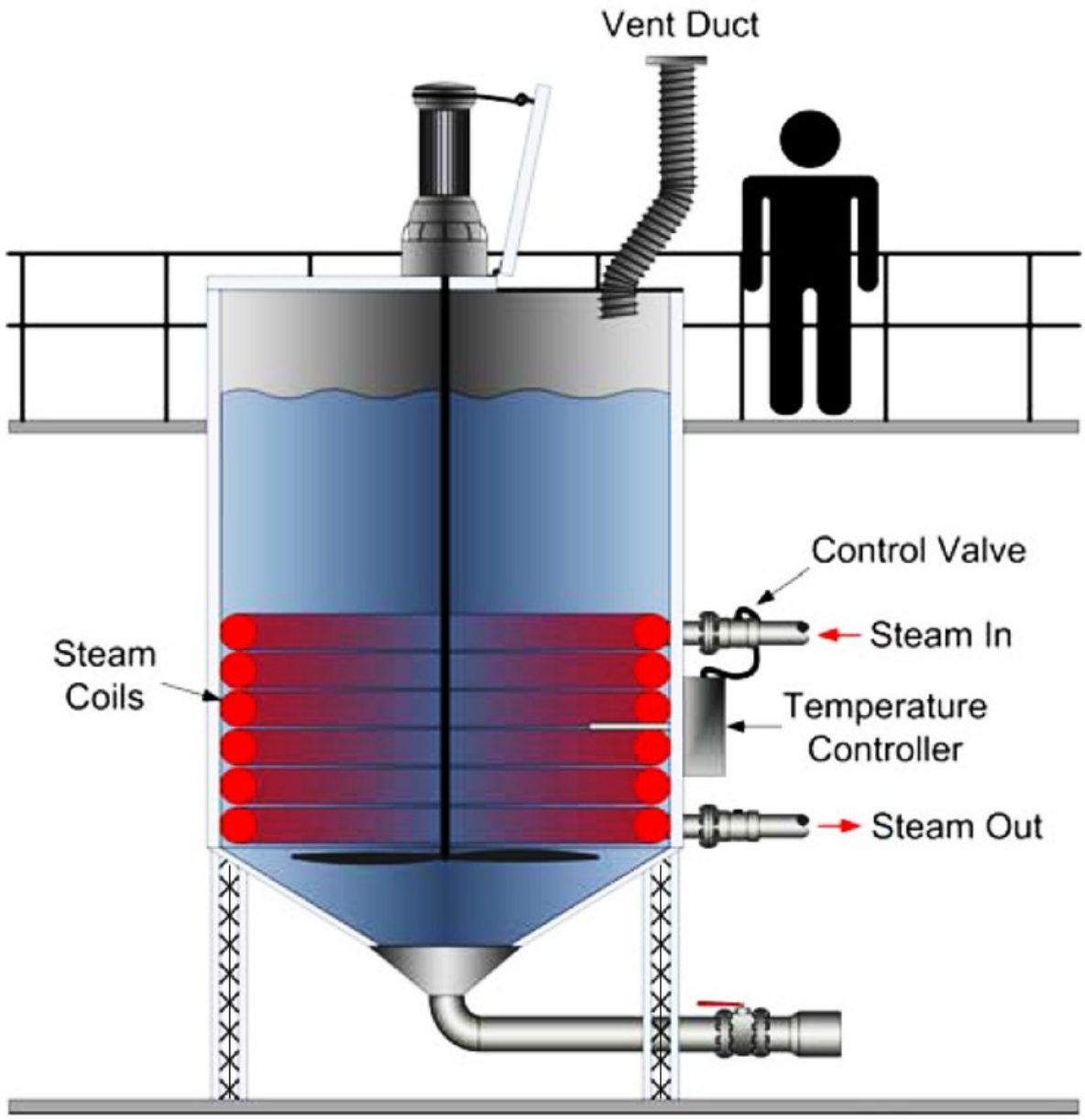

Figure 1: Mixing tank mechanical systems [29].

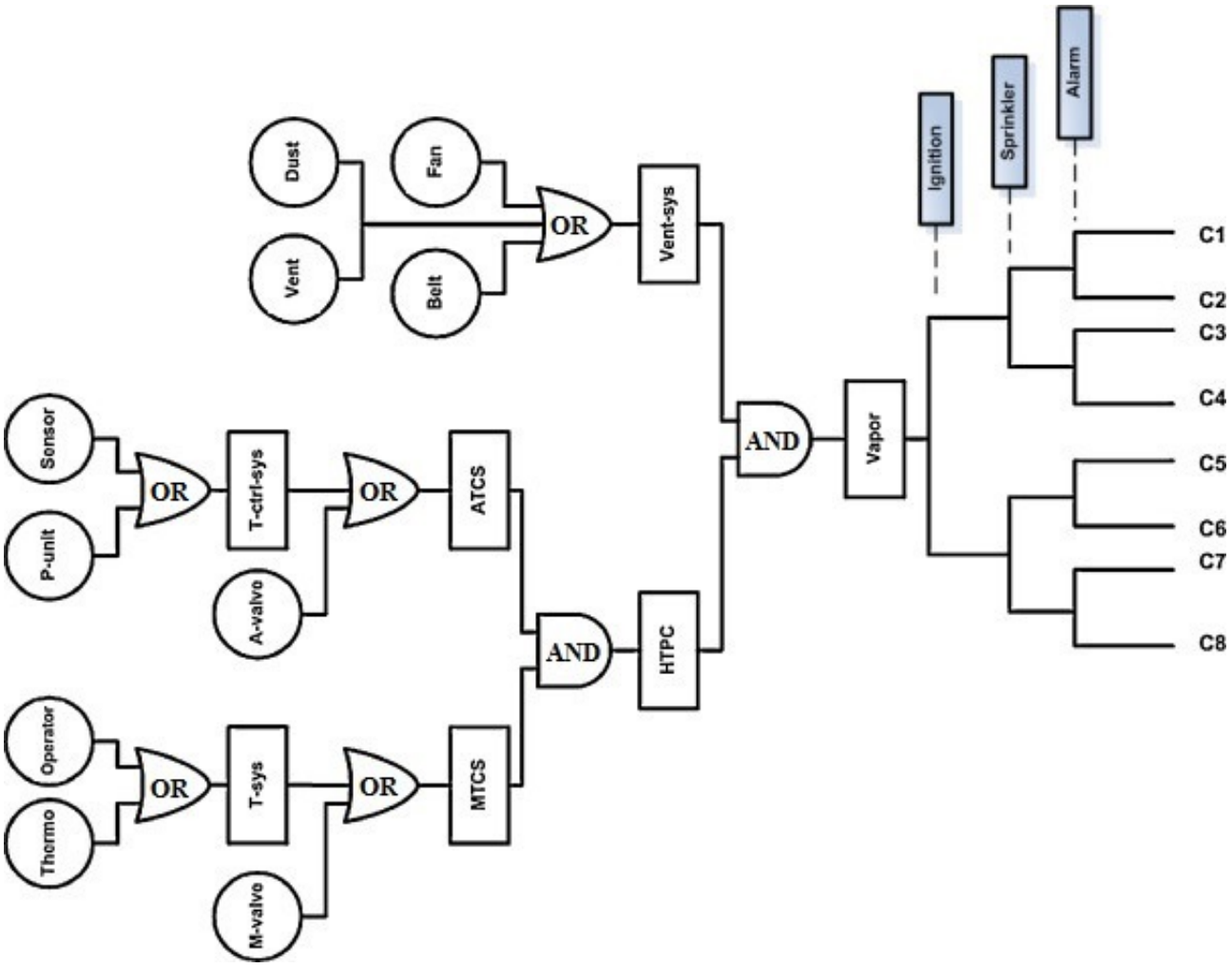

Figure 2: Fault Tree and Event Tree for the heat exchanger accident scenario [19].

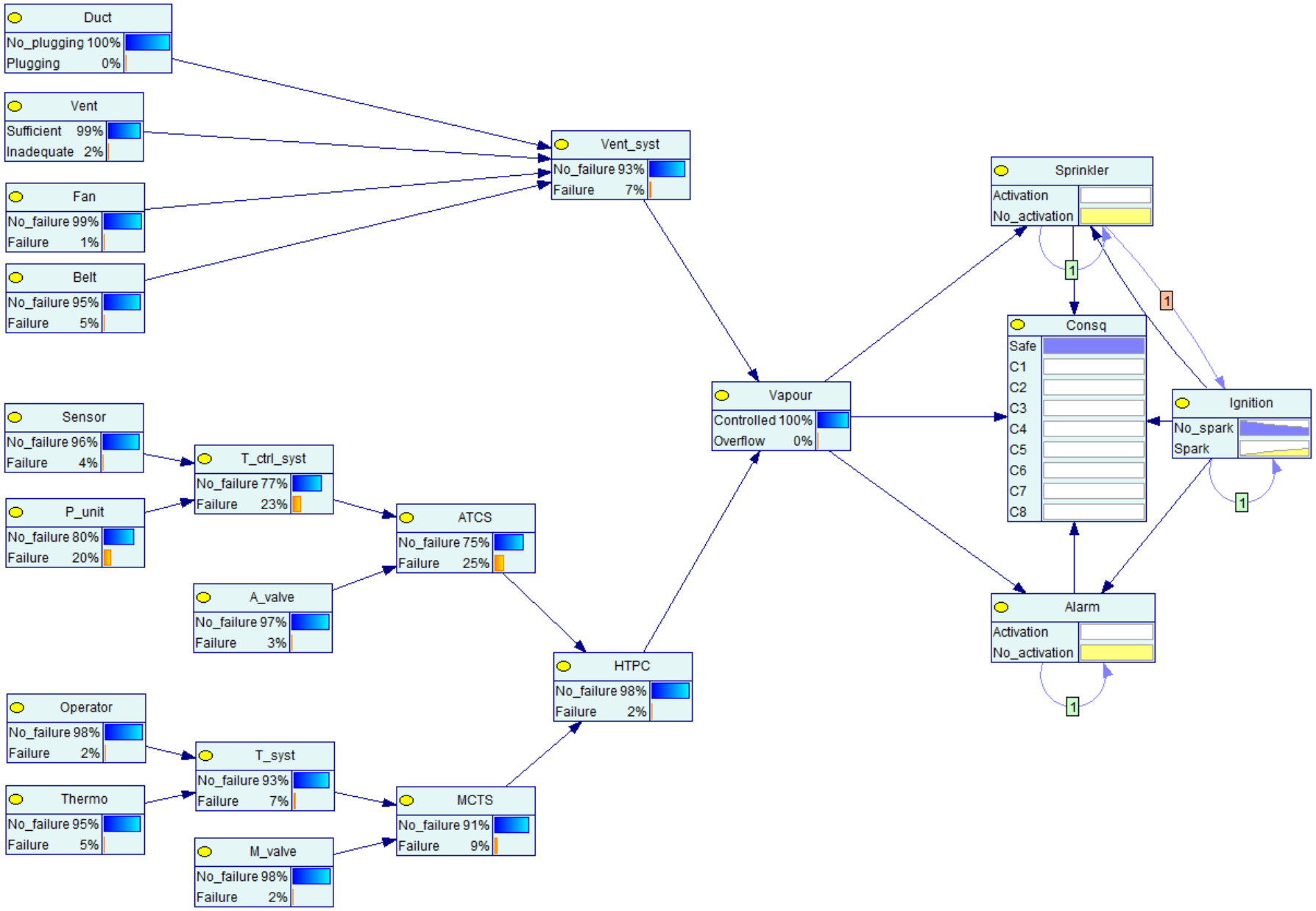

Figure 3: DBN for the heat exchanger accident scenario.

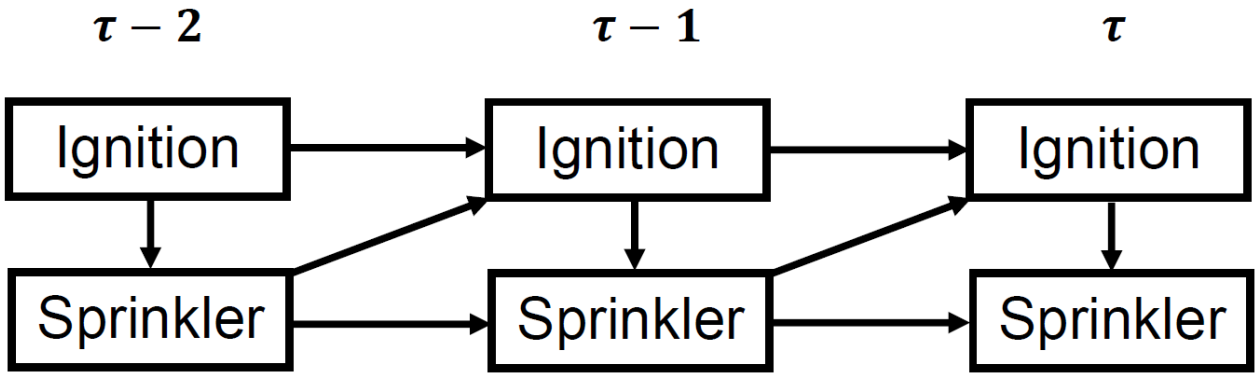

Figure 4: Causal dependence of *Ignition* to *Sprinkler*.

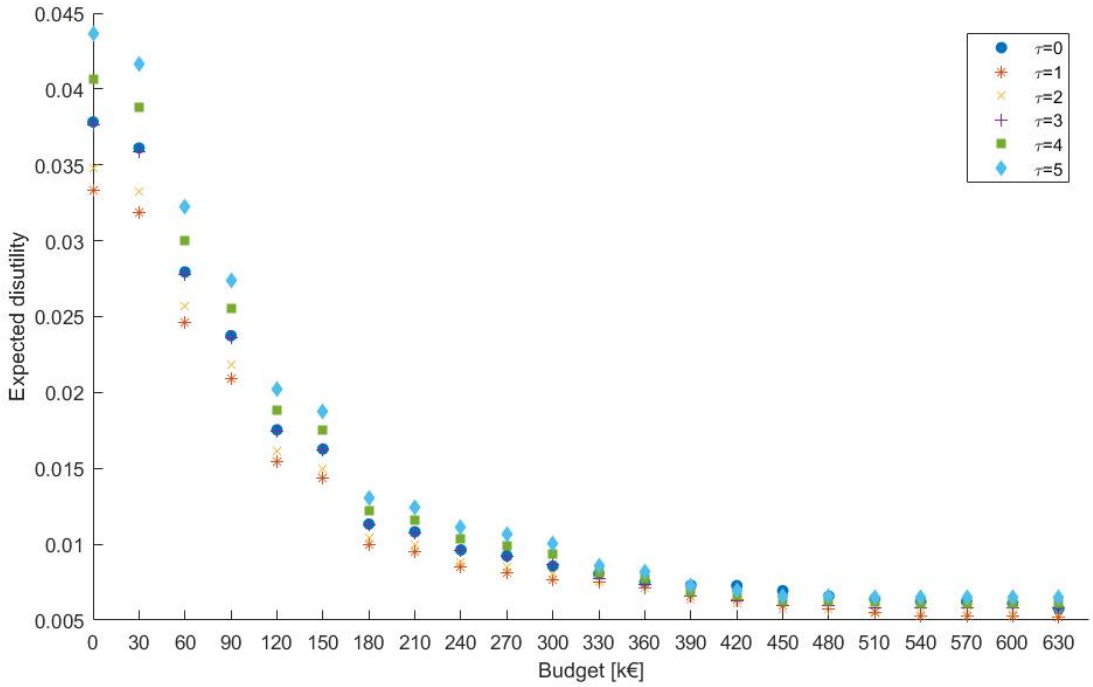

Figure 5: Minimum expected disutility of safety target *Consq*.

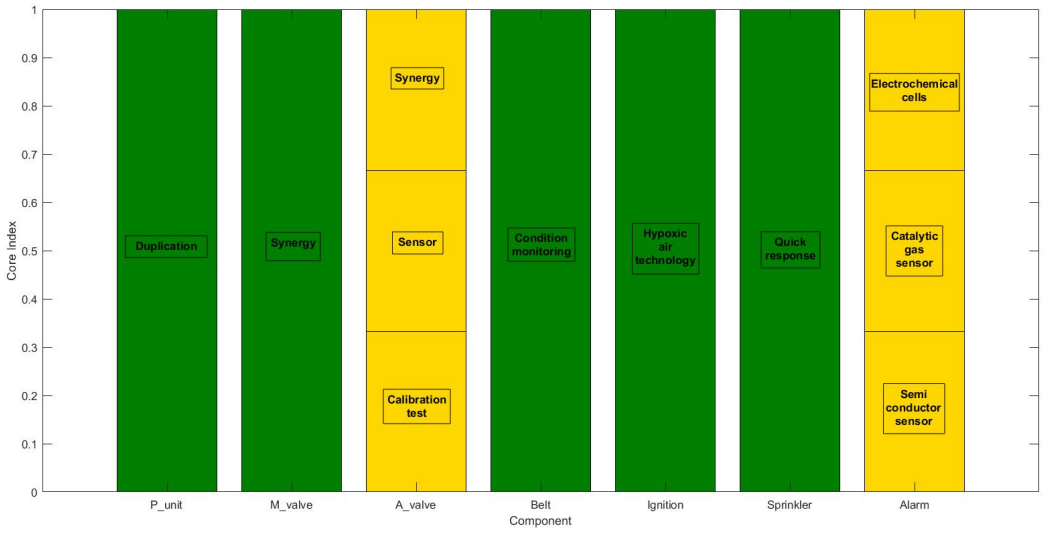

Figure 6: Core index analysis of safety measures.

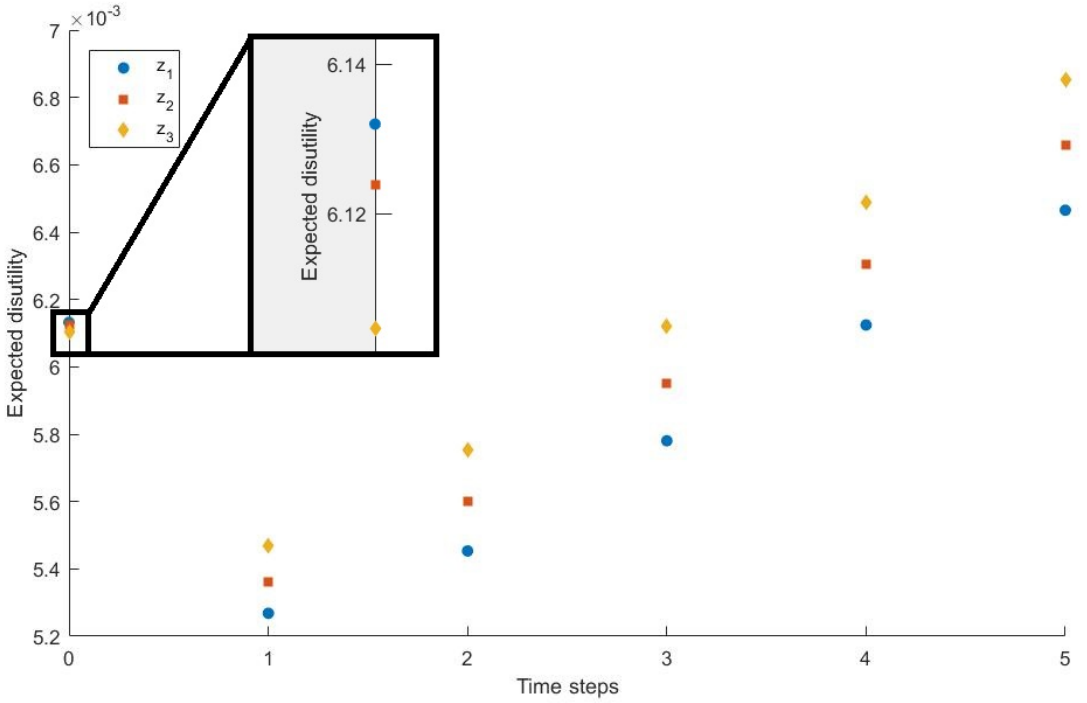

Figure 7: Expected disutility of non-dominated portfolios by setting $B = 600$ k€.

Tables

Table 1: Conditional probability tables of *Alarm* and *Sprinkler* at time step $\tau = 0$

	Vapour	*Controlled*		*Overflow*	
	Ignition	*No_spark*	*Spark*	*No_spark*	*Spark*
Alarm	*Activation*	0	0	0.7750	0.9987
	No_activation	1	1	0.2250	0.0013
Sprinkler	*Activation*	0	0	0.70	0.96
	No_activation	1	1	0.30	0.04

Table 2: List of components and their failure probabilities.

Component	**Symbol**	**Index**	**Failure probability**
Sensor	Sensor	1	0.0400
Pneumatic unit	P_unit	2	0.2015
Temperature control system	T_ctrl_sys	3	OR-gate
Operator	Operator	4	0.0200
Infrared thermometer	Thermo	5	0.0468
Temperature measurement system	T_sys	6	OR-gate
Manual steam valve	M_valve	7	0.0243
Automatic steam valve	A_valve	8	0.0276
Automatic temperature control system	ATCS	9	OR-gate
Manual temperature control system	MTCS	10	OR-gate
High temperature protection system	HTPS	11	AND-gate
Ventilation	Vent	12	0.0150
Fan	Fan	13	0.0100
Belt	Belt	14	0.0500
Duct	Duct	15	0.0010
Ventilation system	Vent_sys	16	OR-gate
Vapour overflow	Vapour	17	AND-gate
Ignition barrier	Ignition	18	0.1000
Water sprinkler system	Sprinkler	19	0.0400, 0.3000
Alarm system	Alarm	20	0.0013, 0.2250

Table 3: Conditional probability table of *Ignition* at time steps $\tau > 0$.

	$Ignition[\tau-1]$	No_spark		$Spark$	
	$Sprinkler[\tau-1]$	$Activation$	$No\_activation$	$Activation$	$No\_activation$
$Ignition[\tau]$	No_spark	0.95	0.9	0	0
	$Spark$	0.05	0.1	1	1

Table 4: List of consequences.

Outcome	**Symbol**	**Disutility**
Controlled vapour	$Safe$	0
Safe evacuation	C_1	10
Wet vapour cloud near the ground	C_2	15
Safe evacuation with possibility of delayed ignition	C_3	30
Vapour cloud with possibility of delayed ignition	C_4	40
Fire, moderate property damage, low death toll	C_5	60
Fire, high property damage, low death toll	C_6	80
Fire, moderate property damage, high death toll	C_7	90
Fire, high property damage, high death toll	C_8	100

Table 5: Probabilities of accident outcomes at each time step.

Outcome	$\tau = 0$	$\tau = 1$	$\tau = 2$	$\tau = 3$	$\tau = 4$	$\tau = 5$
$Safe$	0.998319	0.998319	0.998319	0.998319	0.998319	0.998319
C_1	0.000820	0.001226	0.001289	0.001256	0.001202	0.001144
C_2	0.000238	6.539242e-05	1.485681e-05	3.229053e-06	6.934547e-07	1.484231e-07
C_3	0.000352	0.000116	3.270228e-05	8.908458e-06	2.410073e-06	6.510108e-07
C_4	0.000102	6.202325e-06	3.767917e-07	2.289007e-08	1.390572e-09	8.447723e-11
C_5	0.000161	0.000264	0.000343	0.000411	0.000475	0.000536
C_6	6.713624e-06	2.083401e-06	5.733853e-07	1.552510e-07	4.193539e-08	1.132327e-08
C_7	2.097377e-07	2.850967e-08	5.062283e-09	1.019337e-09	2.140727e-10	4.552654e-11
C_8	8.739072e-09	5.313530e-10	3.227972e-11	1.960993e-12	1.191303e-13	7.237167e-15

Table 6: List of safety measures.

Component	**Safety measure**	**Symbol**	**Cost [k€]**	**Failure probability**
P_unit	Inspection plan	a_1^2	60	0.1500
	Duplication	a_2^2	80	0.1000
M_valve	Calibration test	a_1^7	30	0.0200
	Sensor	a_2^7	40	0.0150
	Synergy	a_3^7	60	0.0100
A_valve	Calibration test	a_1^8	30	0.0200
	Sensor	a_2^8	40	0.0150
	Synergy	a_3^8	60	0.0100
Belt	Periodic test	a_1^{14}	40	0.0300
	Condition monitoring	a_2^{14}	100	0.0100
Ignition	Tank blanketing	a_1^{18}	70	0.0800
	Inerting systems	a_2^{18}	100	0.0600
	Hypoxic air technology	a_3^{18}	150	0.0400
Sprinkler	Standard response	a_1^{19}	40	0.0300, 0.2000
	Quick response	a_2^{19}	80	0.0100, 0.1000
Alarm	Semi conductor sensor	a_1^{20}	60	0.0013, 0.2000
	Catalyic gas sensor	a_2^{20}	80	0.0013, 0.1500
	Electrochemical cells	a_3^{20}	100	0.0013, 0.1000