Mancuso, Alessandro; Compare, Michele; Salo, Ahti; Zio, Enrico

Portfolio optimization of safety measures for the prevention of time-dependent accident scenarios

Published in:
Reliability Engineering and System Safety

DOI:
10.1016/j.ress.2019.106500

Published: 01/10/2019

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Mancuso, A., Compare, M., Salo, A., & Zio, E. (2019). Portfolio optimization of safety measures for the prevention of time-dependent accident scenarios. *Reliability Engineering and System Safety*, *190*, Article 106500. https://doi.org/10.1016/j.ress.2019.106500

Portfolio optimization of safety measures for the prevention of time-dependent accident scenarios

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]Department of Energy Engineering, Politecnico di Milano, Italy
[3]Aramis s.r.l., Milano, Italy
[4]MINES ParisTech, PSL Research University, CRC, Sophia Antipolis, France

Abstract

This paper presents a methodology to support the selection of optimal portfolios of preventive safety measures for time-dependent accident scenarios. This methodology captures the dynamics of accident scenarios through Dynamic Bayesian Networks which represent the temporal evolution of component failures that can lead to system failure. An optimization model is presented to determine all Pareto optimal portfolios for which the residual risk of the system at different time stages is minimized, subject to budget and technical constraints on the set of feasible portfolios. The resulting portfolios are then analyzed to support the optimal selection of preventive safety measures. We also develop a computationally efficient algorithm for solving the multi-objective optimization model. The method is illustrated by revisiting the accident scenario of a vapor cloud ignition which occurred at Universal Form Clamp in Bellwood (Illinois, U.S.) on 14 June 2006. Results are presented for different cost levels of implementing the preventive safety measures, which provides additional management insights.

Keywords: Risk analysis, Preventive safety 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. Generally, this task is often addressed through an iterative procedure based on Risk Importance Measures [1] which provide information about how changes in the reliability of individual components impact the risk of the system. Preventive safety measures are then selected to mitigate the failure of those components whose impact on the risk of the system is greatest. The procedure is iterated until the budget for preventive safety measures is depleted or the risk is reduced to acceptable levels.

In a recent paper [2], we showed that this iterative procedure does not necessarily lead to the optimal selection of preventive safety measures; rather, Portfolio Decision Analysis (PDA) [3] is needed to optimize the allocation of resources to the system. We therefore proposed a PDA methodology which employs Bayesian Networks (BNs) [4] to represent sequences of events that can cause accidents. The resulting BN models help assess the residual risk of the system and can be used to identify the optimal portfolios of preventive safety measures that minimize such risk. Thus, this approach responds to the need for intuitive and computationally efficient methodologies for risk analysis [5, 6, 7]. Specifically, BNs make it possible (i) to circumvent the limitations of binary representation of failure processes by encoding multi-state events, (ii) to extend the concepts of AND/OR gates to gain more flexibility in modelling the accident scenarios and (iii) to combine expert judgments and quantitative knowledge for risk estimation. Yet, our earlier methodology does not account for the time-dependent interactions of failure events [8]. As a result, it is not applicable to the modelling of accident scenarios which depend on the *order*, *timing* and *magnitude* of component failures [9, 10, 11].

In this paper, we extend the PDA methodology to time-dependent accident scenarios by explicitly modeling the dynamic evolution of component failures in process systems. For this purpose we use Dynamic Bayesian Networks (DBNs), which generalize BNs by connecting nodes over multiple time stages [12]. DBNs have been successfully applied in various fields, including 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 process systems and illustrate their potential in the risk assessment and safety analysis of complex process systems. Barua et al. [17] propose a risk assessment methodology for process systems based on a DBN that captures the changes of the failure states over time. However, neither one of these approaches supports the selection of preventive safety measures.

Khakzad et al. [18] employ discrete-time BNs to allocate safety systems optimally in process facilities. Their approach targets the riskiness of individual accident scenarios by comparing the impacts of alternative measures before the most effective ones are selected. However, the analysis of individual accident scenarios can be very demanding in complex systems, because the number of such scenarios can be large. Furthermore, Khakzad et al. do not consider the impact of combinations of preventive safety measures on the system; instead, they identify the most critical failures for designing preventive safety measures. Still, the resulting sequential decisions may not lead to the optimal resource allocation. By contrast, we propose an optimization model for computing *all* optimal portfolios of preventive safety measures for time-dependent accident scenarios. Preventive safety measures are installed at the outset of the accident scenario, thus they are not selected dynamically based on the evolving states of the system components.

In the previous paper [2], the optimization model was built for static systems. In this paper, the methodology is extended to time-dependent accident scenarios by modelling Dynamic Bayesian Networks. Furthermore, the optimization algorithm is updated for the multi-objective optimization. In particular, Pareto-optimal portfolios are selected through the non-dominance condition. We also discuss several approaches to select the optimal solution among the set of non-dominated portfolios.

The rest of the paper is structured as follows. Section 2 presents the portfolio optimization model in the context of DBNs. It also presents the procedure for risk assessment through multiple time stages and the algorithm for computing the optimal allocation of preventive safety measures. Section 3 revisits an earlier case study on the accident scenario of a vapor cloud ignition [19] and analyzes the portfolios of preventive safety measures based on the dominance condition over multiple time stages. Section 4 discusses the potential and limitations 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 based on a detailed analysis of the accident scenarios, which often builds on the development of Fault Trees and Event Trees [20]. Formally, a DBN is a directed acyclic graph, which consists of a sequence of BNs for the time stages $\mathbb{T} = \{0, 1, ..., \mathcal{T}\}$. In this paper, DBNs are built to represent accident scenarios in time-dependent systems where failure events evolve over multiple time stages. Figure 1 shows an example of a DBN which consists of:

- *chance nodes* V^C, indicated by circles and representing random events occurring during the accident scenarios;

- *target nodes* V^T, indicated by hexagons and representing the outcomes of the accident scenarios;

- *arcs* E, indicated by directed edges and representing the causal dependencies among the nodes that define the accident scenarios.

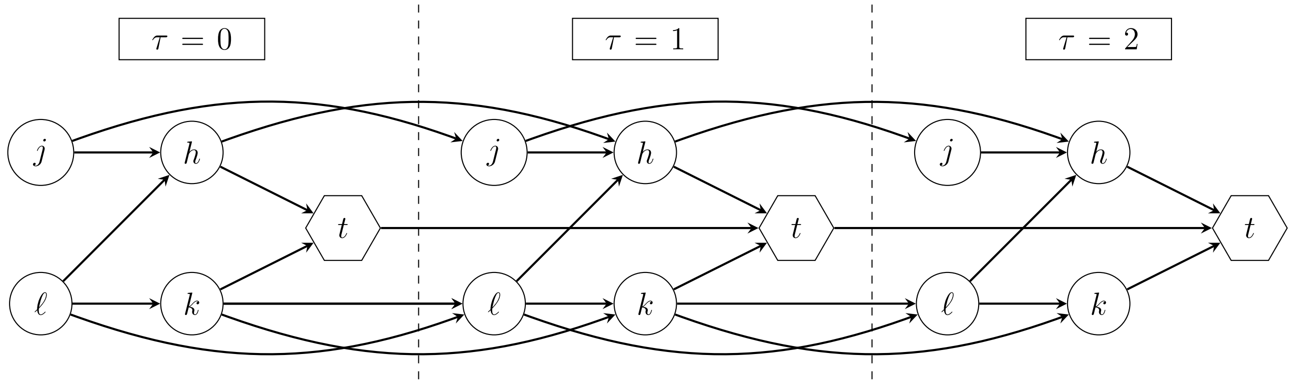

Figure 1: Example of a Dynamic Bayesian Network.

In particular, node $V^i(\tau)$ encodes the possible states of the failure event i at time $\tau \in \mathbb{T}$. In Figure 1, the sets of chance and target nodes are

$$V^C = \{V^j(\tau), V^\ell(\tau), V^h(\tau), V^k(\tau)\} \quad \forall \tau \in \mathbb{T} = \{0, 1, 2\}, \tag{1}$$

$$V^T = \{V^t(0), V^t(1), V^t(2)\}. \tag{2}$$

The directed arcs in the set $E(\tau)$ show causal dependencies among failure events, both at the same time stage τ and at previous time stages $\tau - \delta \in \mathbb{T}$ where $\delta \in \{0, 1, 2, ..., \tau\}$ indicates the temporal delay in the causal dependence. The set of nodes $V^i_-(\tau)$ that affect event i at time τ includes the immediate predecessors of node $V^i(\tau)$ such that

$$V^i_-(\tau) = \{V^j(\tau - \delta) | [V^j(\tau - \delta) \rightarrow V^i(\tau)] \in E(\tau),\, 0 \leq \delta \leq \tau\}\}. \tag{3}$$

where $[V^j(\tau - \delta) \rightarrow V^i(\tau)]$ shows that the state of event j at time $\tau - \delta$ affects the state of event i at time τ. It is not required that $i \neq j$, so the event i at time $\tau - \delta$ can affect the same event or other events at time τ. For instance, in Figure 1 the event k at time $\tau = 0$ affects the events k and ℓ at time $\tau = 1$, thus

$$V^\ell_-(1) = \{V^\ell(0), V^k(0)\}. \tag{4}$$

The set of all nodes V can be partitioned into the set of *leaf nodes* V^L and its complement set of *dependent nodes* V^D as

$$V^L = \{V^i(\tau) \in V | V^i_-(\tau) = \emptyset,\ \tau \in \mathbb{T}\}, \tag{5}$$

$$V^D = \{V^i(\tau) \in V | V^i_-(\tau) \neq \emptyset,\ \tau \in \mathbb{T}\}. \tag{6}$$

The residual risk of the system is evaluated at one or multiple safety target nodes which represent the final outcomes of the accident scenarios on safety, asset operation and environment. In Figure 1, the target node represents the event t through the time stages $\tau \in \mathbb{T}$.

2.1 Probability model

Each system component can be in different failure states, which possibly cause a sequence of cascading failures leading to system failure. The probability distribution of the random variable $X^i(\tau)$ describes the uncertainty in the state of the failure event i at time τ. The realization of the random variable $X^i(\tau)$ belongs to the discrete set of states $\mathbb{S}^i(\tau)$ with different contributions to the system risk [21]. Thus, it is possible to define a probability distribution $\mathbb{P}^s_{X^i(\tau)} = \mathbb{P}[X^i(\tau) = s]$ across the failure states $s \in \mathbb{S}^i(\tau)$ such that

$$\sum_{s \in \mathbb{S}^i(\tau)} \mathbb{P}^s_{X^i(\tau)} = 1, \quad \forall i \text{ such that } V^i(\tau) \in V^L. \tag{7}$$

The deployment of preventive safety measures on a subset of nodes $V^A \subseteq V$ can mitigate the system risk by affecting the occurrence probability of the failure events in the accident scenario. Formally, the set of alternative preventive safety measures is $\mathbb{A}^i = \{1, ..., |\mathbb{A}^i|\}$ for the event i, where the operator $|\cdot|$ indicates the cardinality of the set. The binary variable z^i_a represents the choice on preventive safety measure $a \in \mathbb{A}^i$ such that $z^i_a = 1$ if the measure is installed for all time stages $\tau \in \mathbb{T}$, and 0 otherwise. No preventive safety measures are available for nodes $V^i(\tau) \notin V^A$: this is modelled by $\mathbb{A}^i = \emptyset$ so that $|\mathbb{A}^i| = 0$. Thus, the binary vector $\mathbf{z}$ defines the portfolio of preventive safety measures as the concatenation of vectors $\mathbf{z}^i = [z^i_1, ..., z^i_{|\mathbb{A}^i|}]$ for all failure events. Without losing generality, we assume that the preventive safety measures for the failure event i are mutually exclusive. This implies that at most one preventive safety measure can be selected from set $\mathbb{A}^i$ so that

$$\sum_{a \in \mathbb{A}^i} z^i_a \leq 1, \quad \forall i \text{ such that } V^i(\tau) \in V^A. \tag{8}$$

Synergies between preventive safety measures can be modelled though logical constraints. Preventive safety measures are implemented at the outset of the accident scenarios, affecting the probability distributions at any later time stage. Specifically, the deployment of a preventive safety measure $a \in \mathbb{A}^i$ affects the probability distribution of event i at time τ by reducing the failure probability $\mathbb{P}^s_{X^i(\tau)}$ to $\mathbb{P}^s_{X^i_a(\tau)}$ for each time $\tau \in \mathbb{T}$. Then, the marginal probability of the realization $s \in \mathbb{S}^i(\tau)$ is

$$\mathbb{Q}^s_{X^i(\tau)}(\mathbf{z}) = \sum_{a \in \mathbb{A}^i} [\mathbb{P}^s_{X^i_a(\tau)} \, z^i_a] + \mathbb{P}^s_{X^i(\tau)} \prod_{a \in \mathbb{A}^i} [1 - z^i_a], \quad \forall i \text{ such that } V^i(\tau) \in V^L. \tag{9}$$

The Bayesian model computes the probabilities of cascading failure events through the *law of total probability*. Specifically, the total probability of the realization $s \in \mathbb{S}^i(\tau)$ at node $V^i(\tau) \in V^D$ depends on the states of its predecessors. To model this relationship, let $\mathbb{S}^i_-(\tau)$ be the Cartesian product of the sets of states of the predecessors such that

$$\mathbb{S}^i_-(\tau) = \bigtimes_{\substack{\{(j,\delta) | V^j(\tau-\delta) \in V^i_-(\tau)\} \\ 0 \leq \delta \leq \tau}} \mathbb{S}^j(\tau - \delta). \tag{10}$$

The notation $\mathbb{P}^s_{X^i(\tau)|\mathbf{x}^i_-(\tau)}$ refers to the probability of the state $s \in \mathbb{S}^i(\tau)$ of the event i, conditioned on the realization of states $\mathbf{x}^i_-(\tau) \in \mathbb{S}^i_-(\tau)$ of its predecessors. Similarly, the notation $\mathbb{P}^s_{X^i_a(\tau)|\mathbf{x}^i_-(\tau)}$ is the conditional probability of the state $s \in \mathbb{S}^i(\tau)$ for the realization $\mathbf{x}^i_-(\tau)$ and the deployment of the preventive safety measure $a \in \mathbb{A}^i$. Thus, the conditional probability of state $s \in \mathbb{S}^i(\tau)$ at dependent nodes $V^i(\tau) \in V^D$ is

$$\mathbb{Q}^s_{X^i(\tau)|\mathbf{x}^i_-(\tau)}(\mathbf{z}) = \sum_{a \in \mathbb{A}^i} [\mathbb{P}^s_{X^i_a(\tau)|\mathbf{x}^i_-(\tau)}\, z^i_a] + \mathbb{P}^s_{X^i(\tau)|\mathbf{x}^i_-(\tau)} \prod_{a \in \mathbb{A}^i} [1 - z^i_a]. \tag{11}$$

Based on the conditional independence of the predecessors [22], the total probability of the realization $s \in \mathbb{S}^i(\tau)$ can be expressed recursively as

$$\mathbb{Q}^s_{X^i(\tau)}(\mathbf{z}) = \sum_{\mathbf{x}^i_-(\tau) \in \mathbb{S}^i_-(\tau)} \mathbb{Q}^s_{X^i(\tau)|\mathbf{x}^i_-(\tau)}(\mathbf{z}) \prod_{\substack{\{(j,\delta)|V^j(\tau-\delta) \in V^i_-(\tau)\} \\ 0 \le \delta \le \tau}} \mathbb{Q}^{x^j(\tau-\delta)}_{X^j(\tau-\delta)}(\mathbf{z}). \tag{12}$$

The first summation is taken over all possible realizations $\mathbf{x}^i_-(\tau) \in \mathbb{S}^i_-(\tau)$ of the states of the predecessors, whereas $x^j(\tau - \delta)$ is the element of $\mathbf{x}^i_-(\tau)$ which corresponds to event j at time $\tau - \delta$. The total probability is a multiplicative function of the portfolio $\mathbf{z}$ of preventive safety measures that have been applied along the scenarios leading to the system failure.

The portfolio $\mathbf{z}$ of preventive safety measures is evaluated by the expected disutility at safety target nodes V^T over multiple time stages. The disutility $u^s_{X^t}$ represents the severity of the state $s \in \mathbb{S}^t(\tau)$ of the failure event t at target node V^T. Then, the expected disutility resulting from portfolio $\mathbf{z}$ is

$$\mathbb{U}_{X^t(\tau)}(\mathbf{z}) = \sum_{s \in \mathbb{S}^t(\tau)} \mathbb{Q}^s_{X^t(\tau)}(\mathbf{z}) \cdot u^s_{X^t}. \tag{13}$$

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

2.2 Dominance structure

Recommendations for selecting the optimal portfolio of preventive safety measures are generated by minimizing the expected disutility throughout the time stages $\tau \in \mathbb{T}$. In particular, the multi-objective optimization model limits the set of feasible portfolios through linear and non-linear constraints. Let M be the size of the binary vector $\mathbf{z}$, then the set $\mathbf{Z}_F$ of feasible portfolios can be defined by a set of L linear inequalities whose coefficients are in the matrix $H \in \mathbb{R}^{L \times M}$ and vector $\mathbf{b} \in \mathbb{R}^L$, so that

$$\mathbf{Z}_F = \{\mathbf{z} \in \{0,1\}^M | H\,\mathbf{z} \le \mathbf{b}\}, \tag{14}$$

where $\leq$ holds componentwise. Among the feasibility constraints, the overall cost (based on the cost c_a^i of deployment of the preventive safety measure $a \in \mathbb{A}^i$) of the portfolio must not exceed the budget constraint B, thus

$$\sum_{\{i|V^i(\tau)\in V^A\}} \sum_{a\in\mathbb{A}^i} z_a^i c_a^i \leq B. \tag{15}$$

It is possible to specify additional constraints to represent the properties of the system. For instance, if the preventive safety measures for mitigating the occurrence of the failure events i and j are mutually exclusive, then

$$\sum_{a\in\mathbb{A}^i} z_a^i + \sum_{a\in\mathbb{A}^j} z_a^j \leq 1. \tag{16}$$

Conversely, if at least one preventive safety measure must be applied, the corresponding constraint is

$$\sum_{a\in\mathbb{A}^i} z_a^i + \sum_{a\in\mathbb{A}^j} z_a^j \geq 1. \tag{17}$$

If there are components to which specific regulatory limits apply, it is possible to introduce additional constraints to ensure that the total probability of the failure states does not exceed an acceptable threshold $\epsilon_{X^t}^s$ so that

$$\mathbb{Q}_{X^t(\tau)}^s(\mathbf{z}) \leq \epsilon_{X^t}^s, \quad \forall \tau \in \mathbb{T}. \tag{18}$$

The values of $\epsilon_{X^t}^s$ are usually provided by regulatory offices: the constraints must be respected for the risk to be acceptable.

The set of non-dominated portfolios of preventive safety measures consists of those feasible portfolios for which there exists no other feasible portfolio which would decrease the residual risk of the system at some time stage without increasing it at any other time stage. This set includes all Pareto-optimal solutions defined by the dominance condition

$$\mathbf{z}^* \succ \mathbf{z} \Leftrightarrow \begin{cases} \mathbb{U}_{X^t(\tau)}(\mathbf{z}^*) \leq \mathbb{U}_{X^t(\tau)}(\mathbf{z}) & \text{for all } \tau \in \mathbb{T} \\ \mathbb{U}_{X^t(\tau)}(\mathbf{z}^*) < \mathbb{U}_{X^t(\tau)}(\mathbf{z}) & \text{for some } \tau \in \mathbb{T} \end{cases}, \tag{19}$$

for any pair of feasible portfolios. Thus, the multi-objective optimization model determines the set of non-dominated portfolios of preventive safety measures

$$\mathbf{Z}_{ND} = \{\mathbf{z}^* \in \mathbf{Z}_F | \nexists\ \mathbf{z} \in \mathbf{Z}_F \text{ such that } \mathbf{z} \succ \mathbf{z}^*\}. \tag{20}$$

Generally, the set of non-dominated portfolios can include multiple solutions of which one must be selected and deployed. For this purpose, we propose three possible procedures:

(i) The decision maker(s) can focus on Pareto-optimal solutions for specific time stages, depending on whether the accident scenarios have immediate or delayed impacts. For instance, the decision-maker(s) can disregard late time stages if the accident leads to harmful consequences very rapidly.

(ii) The decision maker(s) can select the Pareto-optimal solution $\mathbf{Z}_E$ that minimizes the overall cost of deployment such that

$$\mathbf{Z}_E = \arg \min_{\mathbf{z}^* \in \mathbf{Z}_{ND}} \sum_{\{i | V^i(\tau) \in V^A\}} z_a^i \, c_a^i \tag{21}$$

(iii) The decision-maker(s) can select specific preventive safety measures among the Pareto-optimal solutions by computing the core index of each measure. Based on Liesiö et al. [25, 26], the core index $CI(a)$ is the fraction of non-dominated portfolios that include the measure $a \in \mathbb{A}^i$. In these portfolios, the binary variable z_a^i is equal to 1 so that

$$CI(a) = \frac{|\{\mathbf{z}^* \in \mathbf{Z}_{ND} | z_a^i = 1\}|}{|\mathbf{Z}_{ND}|}. \tag{22}$$

The core index values help identify preventive safety measures that can be surely selected or rejected. If the core index of a preventive safety measure is 1, then that measure belongs to all non-dominated portfolios; on the other hand, if the core index is 0, the preventive safety measure is not included in any non-dominated portfolio. Decisions concerning safety measures whose core index values are in the open interval $(0, 1)$ can be taken based on further technical considerations, such as the installation time of these measures.

(iv) The definition of the optimal strategy can also be defined based on the minimum Euclidean distance of the expected disutilities from the origin of the axes, which represents an ideal point of the system risk through the time stages. Thus, the decision maker(s) can select the portfolio $\mathbf{Z}_L$ such that

$$\mathbf{Z}_L = \arg \min_{\mathbf{z}^* \in \mathbf{Z}_{ND}} \| [\mathbb{U}_{X^t(0)}(\mathbf{z}^*), \mathbb{U}_{X^t(1)}(\mathbf{z}^*), ..., \mathbb{U}_{X^t(\mathcal{T})}(\mathbf{z}^*)] \|. \tag{23}$$

However, this selection does not consider the time stages explicitly, thus it does not account for the variations of the risk over the time stages.

2.3 Optimization algorithm

We develop an implicit enumeration algorithm for computing the set of non-dominated portfolios of preventive safety measures that minimize the residual risk of the system throughout the time stages. The algorithm is an adaptation of the one proposed by Liesiö [28] for solving a multi-objective optimization problem.

The set $\mathbf{Z}^*$ includes potential non-dominated portfolios, which is initially empty. This set is updated at every iteration of the algorithm. If it is feasible not to deploy any preventive safety measure, the portfolio $\mathbf{z} = [0, ..., 0]$ is included in the set $\mathbf{Z}^*$ as a potential non-dominated solution.

The algorithm enumerates the portfolios starting from $\mathbf{z} = [0, ..., 0]$ through two main iterations: *Forward-loop* and *Backtrack step*. The *Forward-loop* sets $z_m = 1$ in an increasing order of the index m. If the resulting 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 portfolio $\mathbf{z}^* \in \mathbf{Z}^*$ that is dominated by $\mathbf{z}$.

The *Forward-loop* can only increment the values $z_{m+1}, ..., z_M$. If the portfolio $\mathbf{z}$ is unfeasible and cannot be made feasible by setting $z_r = 1$ for some indexes $r \in \{m+1, ..., M\}$, there is no need to continue the *Forward-loop* because it would generate unfeasible portfolios only. This fathoming condition avoids the enumeration of all 2^M possible portfolios. Alternatively, the *Forward-loop* terminates when m reaches M, whereafter the algorithm backtracks. The *Backtrack step* sets $z_M = 0$, detects the greatest index m such that $z_m = 1$ and sets $z_m = 0$. If such an index does not exist, the algorithm terminates; otherwise the *Forward-loop* is repeated. At termination, the set $\mathbf{Z}^*$ consists of the set of non-dominated portfolios $\mathbf{Z}_{ND}$. The pseudocode is presented in Algorithm 1. It has been coded in C++ programming language and linked to GeNIe Modeler, a development environment for reasoning in graphical probabilistic models.

```
Initialization: z = [0, ..., 0]; m ← 1; Z* ← ∅;
if z ∈ Z_F then
    Z* ← z;
end
while m > 0 do
    Forward-loop:
    while m ≤ M do
        z_m ← 1;
        if z ∈ Z_F and z* ⊁ z ∀z* ∈ Z* then
            Z* ← z ∪ {z* ∈ Z* | z ⊁ z*};
        end
        if Σ_{j=1}^{m} z_j H_j^ℓ + Σ_{j=m+1}^{M} min{0, H_j^ℓ} > b^ℓ for any ℓ = 1, ..., L then
            Break Forward-loop;
        end
        m ← m + 1;
    end
    Backtrack step:
    z_M ← 0;
    m ← max [{j | z_j = 1} ∪ {0}];
    if m > 0 then
        z_m ← 0;
        m ← m + 1;
    end
end
Z_ND ← Z*;
```

Algorithm 1: The implicit enumeration algorithm for multi-objective optimization.

3 Case study

We illustrate our methodology by revisiting the accident scenario of a vapor cloud ignition occurred at Universal Form Clamp in Bellwood (Illinois, U.S.) on 14 June 2006. In this accident, a flammable vapor cloud of heptane and mineral spirits overflowed from an open top mixing and heating tank. The vapor cloud ignited when it came into contact with unknown ignition sources. The accident led to one death, two injuries and a 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 checks the temperature with an infrared thermometer and is expected to intervene in case of emergency. Finally, the exhaust ventilation system is installed on top of the tank to control

possible vapor emissions. Figure 2 illustrates the process system.

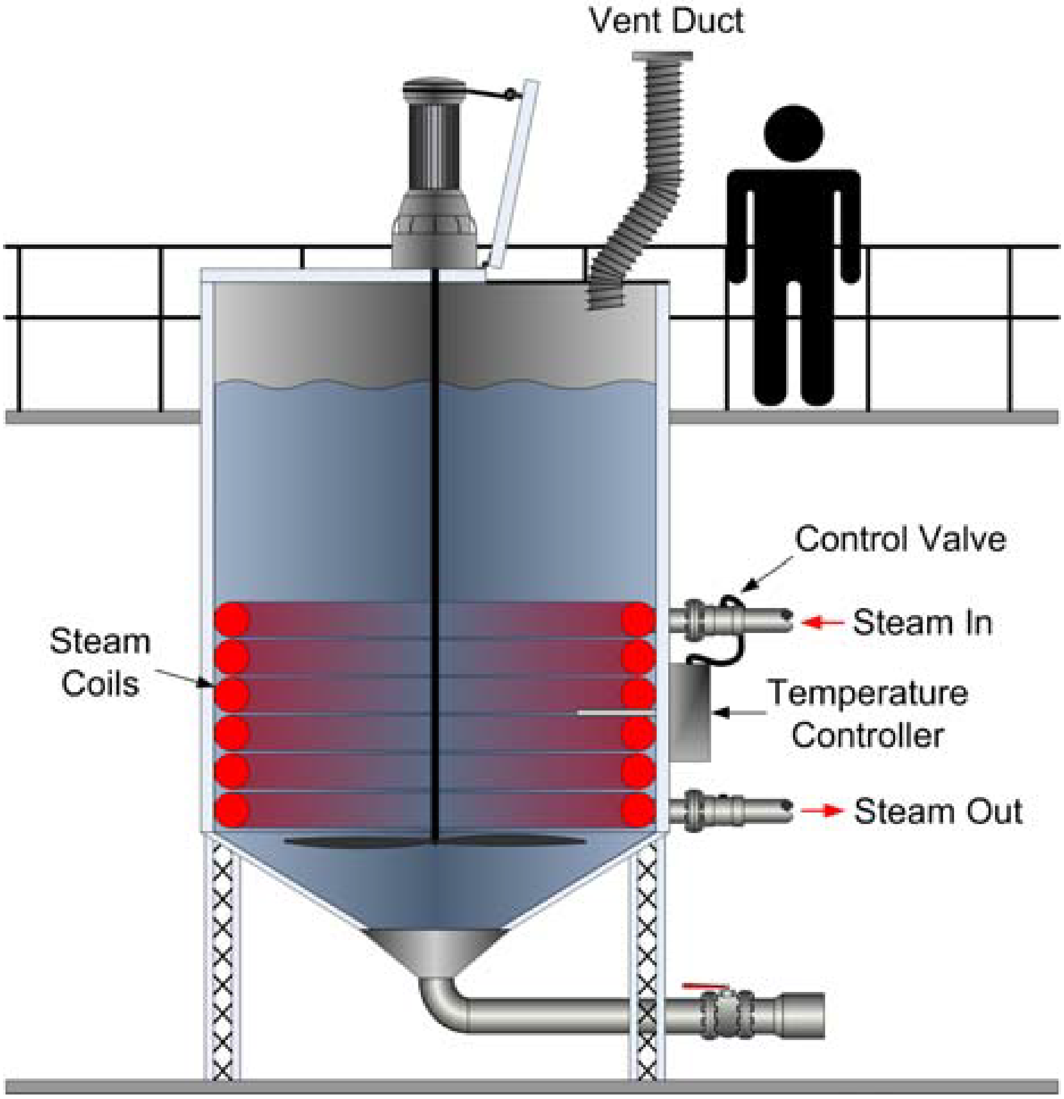

Figure 2: Mixing tank mechanical system [29].

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 so long that the mixture heated to its boiling point, thus generating a high volume of vapor. Because the local ventilation system failed due to a broken fan belt, the vapor cloud spilled from the tank and finally ignited when exposed to an unknown ignition source. It was also found that the ventilation system would not have had enough capacity to collect such a high volume of vapor, even if it had been working. Following the accident investigation, Khakzad et al. [19] developed the Fault Tree and Event Tree in Figure 3 to model the accident scenarios and investigate the effectiveness of the preventive safety measures. In addition, they converted the Fault Tree and

Event Tree to a Bayesian Network.

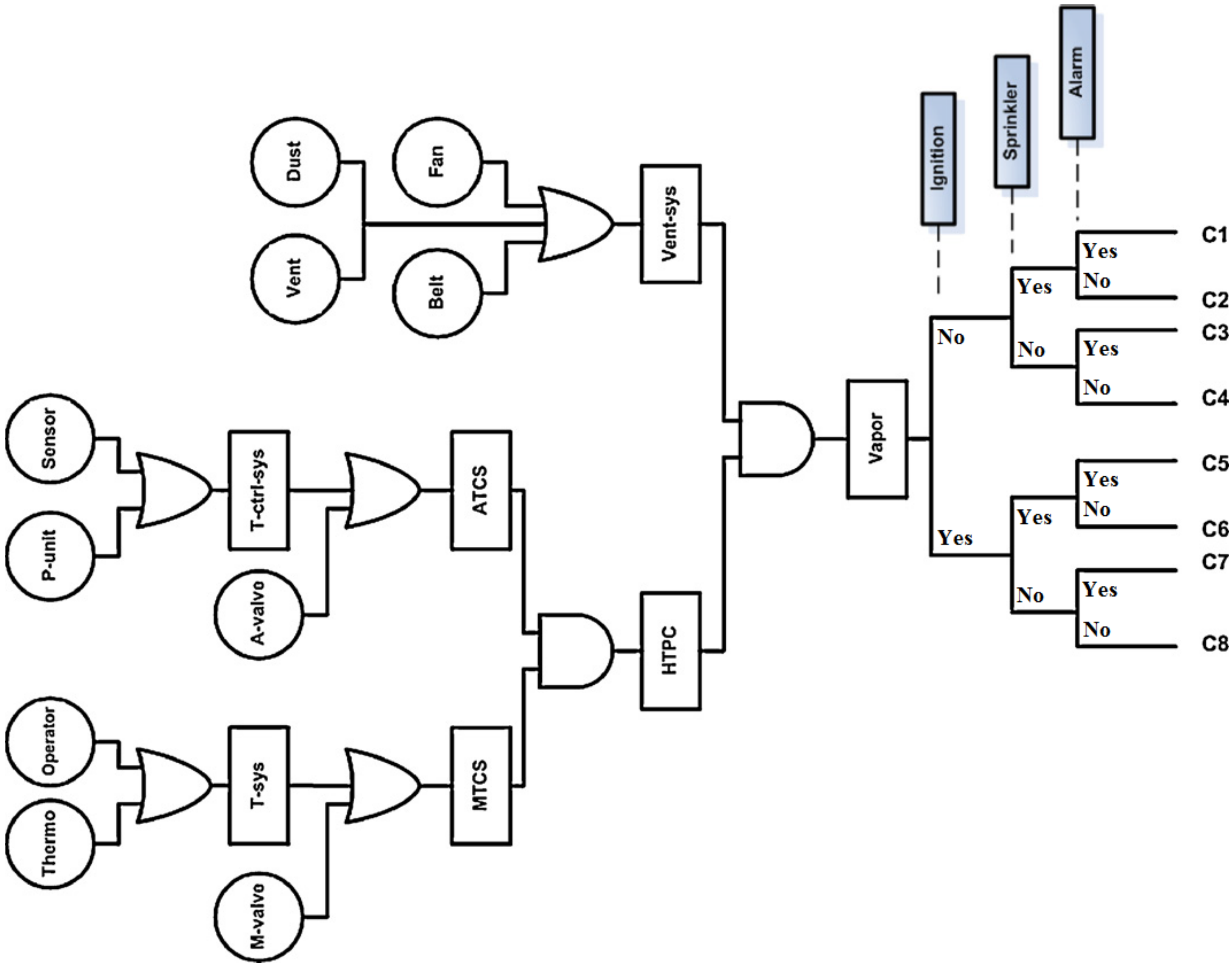

Figure 3: Fault Tree and Event Tree for the accident scenarios of a mixing tank mechanical system [19].

In this case study, we extend the Bayesian Network to a DBN in order to consider the temporal evolution of some events (immediate/delayed ignition) and the performance of the detection systems *Sprinkler* and *Alarm*. Figure 4 shows our probability model based on a DBN, where the node *Consq* represents the safety target. Depending on the success or failure of the preventive safety measures, the accident scenarios lead to nine possible outcomes of increasing severity. In particular, the state *Safe* represents the outcome following the non-occurrence of the system failure (*Vapor*=*Controlled*), while the other outcomes follow from malfunctions of some system components.

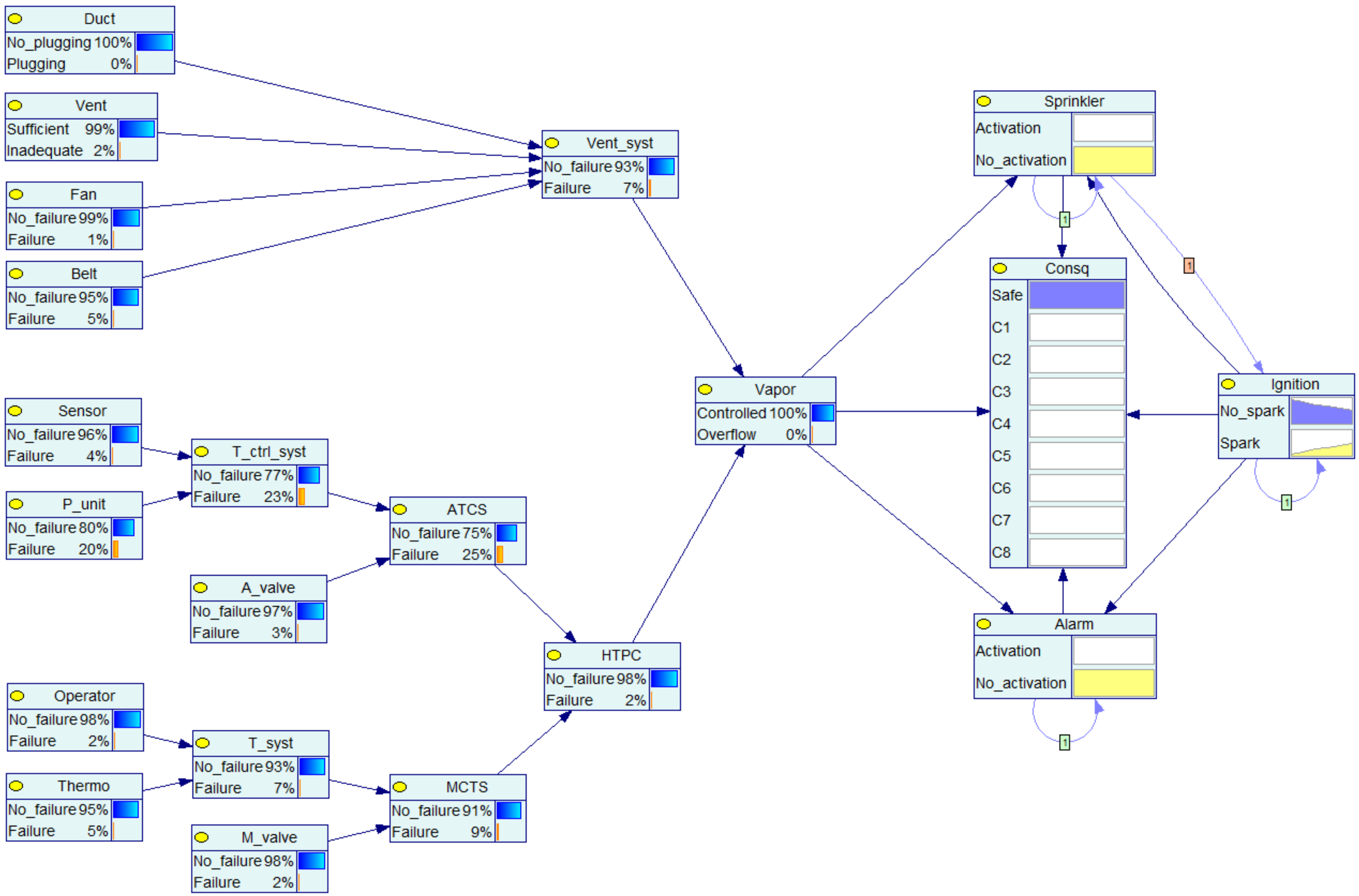

Figure 4: DBN for the accident scenarios of a mixing tank mechanical system.

Specifically, the Bayesian model considers $\mathcal{T} = 5$ time stages for the failure events following the Top Event *Vapor* due to the rapid dynamics of the accident scenario in case of vapor overflow. In Figure 4, the temporal delay δ is specified by the squared number over the respective arc. If no squared number is associated to the 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 5 shows the causal dependence of *Sprinkler* and *Ignition* throughout multiple time stages. Time dependence represents the possible occurrence of delayed ignitions, overcoming the limitations of the model of Khakzad et al. in which delayed ignitions are considered only as possible outcomes of accident scenarios.

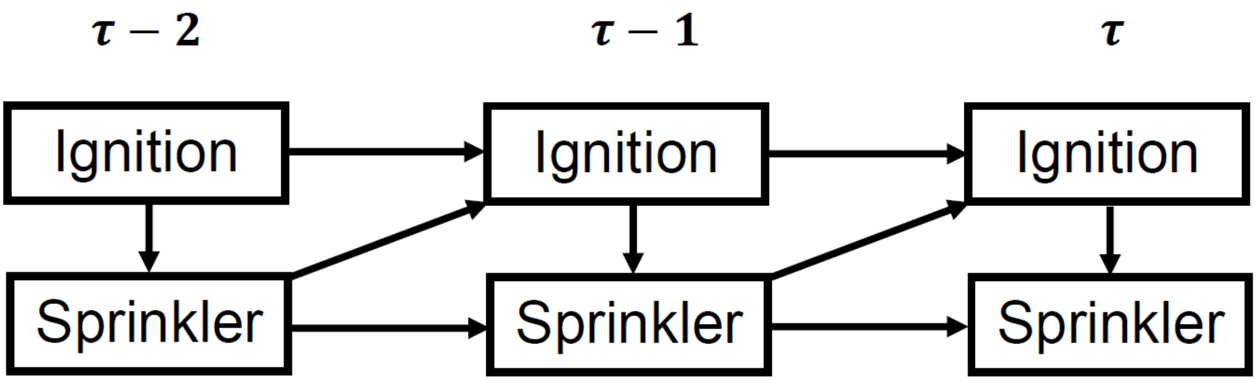

Figure 5: Causal dependence of *Ignition* to *Sprinkler* throughout multiple time stages.

Because the vapor cloud is not toxic, any fatalities or injuries can be attributed to the vapor ignition. The activation of *Sprinkler* and *Alarm* are influenced by *Ignition=Spark* or *Vapor=Overflow*, as shown by the causal dependence represented by the arcs. Specifically, the activation of *Sprinkler* and *Alarm* occur if vapor is ignited (*Vapor=Overflow* and *Ignition=Spark*) with failure probabilities equal to 0.04 and 0.0013, respectively. However, *Sprinkler* and *Alarm* can also be activated by a specific amount of vapor concentration in the air even if the vapor is not ignited (*Vapor=Overflow* and *Ignition=No_ spark*). The activation of *Sprinkler* and *Alarm* for a vapor concentration occur with failure probabilities equal to 0.3 and 0.225, respectively. For more details on the definition of the probabilistic model, please refer to our Data in Brief article [30].

Preventive safety measures reduce the expected disutility of the negative outcomes at the safety target *Consq*. Our Data in Brief article [30] reports the 18 preventive safety measures, including illustrative costs and updated failure probability of the components. The optimization model determines the entire set of non-dominated portfolios of preventive safety measures which minimize the expected disutility of the safety target *Consq* throughout multiple time stages. The optimization algorithm has been run for different budget constraints.

Figure 6 shows the minimum expected disutility of the accident scenarios for each time stage. For multiple non-dominated portfolios at a given budget level B (horizontal axis in Figure 6), 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 for no preventive safety measure to the system. By increasing the budget, the Pareto-optimal portfolios of preventive safety measures further reduce the residual risk of the system, as evaluated by the expected disutility of safety target *Consq*.

The possibility of immediate ignition is the underlying cause for the expected disutility at time $\tau = 0$. At time stage $\tau = 1$, the activation of *Sprinkler* decreases the probability of ignition and consequently the expected disutility. Finally, the expected disutility of the later time stages increases due to the possibility of delayed ignition. Figure 6 also provides additional risk management insights, for instance for defining the requisite budget to meet safety targets and for assessing how increases in the budget reduce the system risk [31].

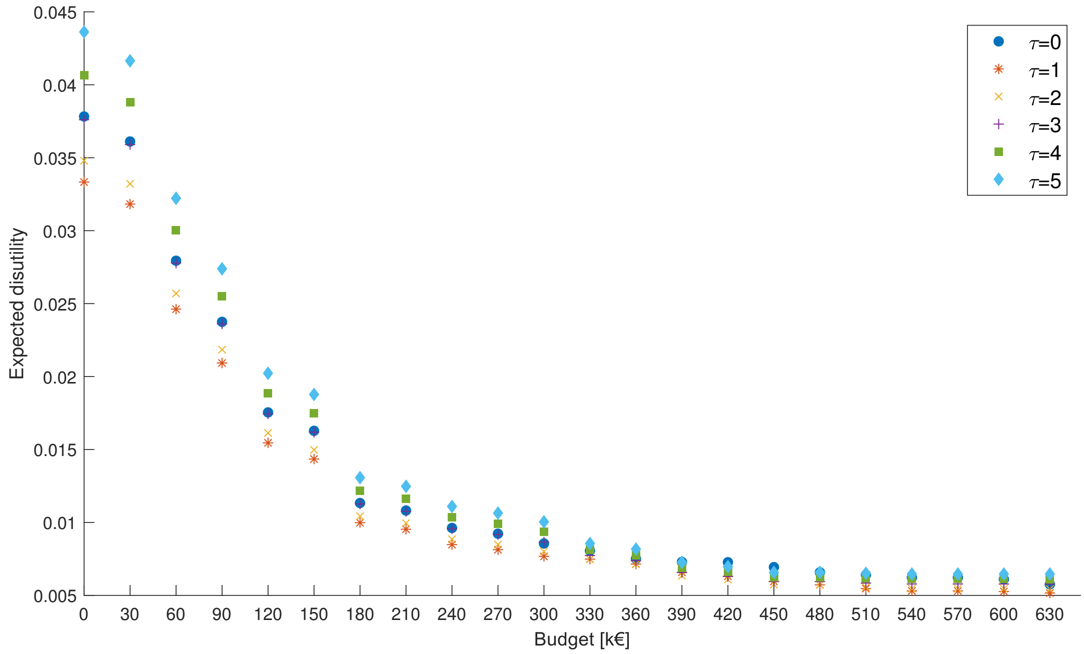

Figure 6: Minimum expected disutility of safety target *Consq*.

For the budget constraint at $B = 600$ k€, the optimization model provides the three non-dominated portfolios in Table 1.

Table 1: Non-dominated portfolios for budget constraint at $B = 600$ k€.

Component	$\mathbf{z}_1$	$\mathbf{z}_2$	$\mathbf{z}_3$
P_unit	Duplication	Duplication	Duplication
M_valve	Synergy	Synergy	Synergy
A_valve	Synergy	Sensor	Calibration test
Belt	Condition monitoring	Condition monitoring	Condition monitoring
Ignition	Hypoxic air technology	Hypoxic air technology	Hypoxic air technology
Sprinkler	Quick response	Quick response	Quick response
Alarm	Semi conductor sensor	Catalyic gas sensor	Electrochemical cells

The analysis of the core indexes in Figure 7 recommends to deploy the preventive safety measures *Duplication*, *Synergy*, *Condition monitoring*, *Hypoxic air technology* and *Quick response*, whereas the selection of preventive safety measures on *A_valve* and *Alarm* may require further analysis.

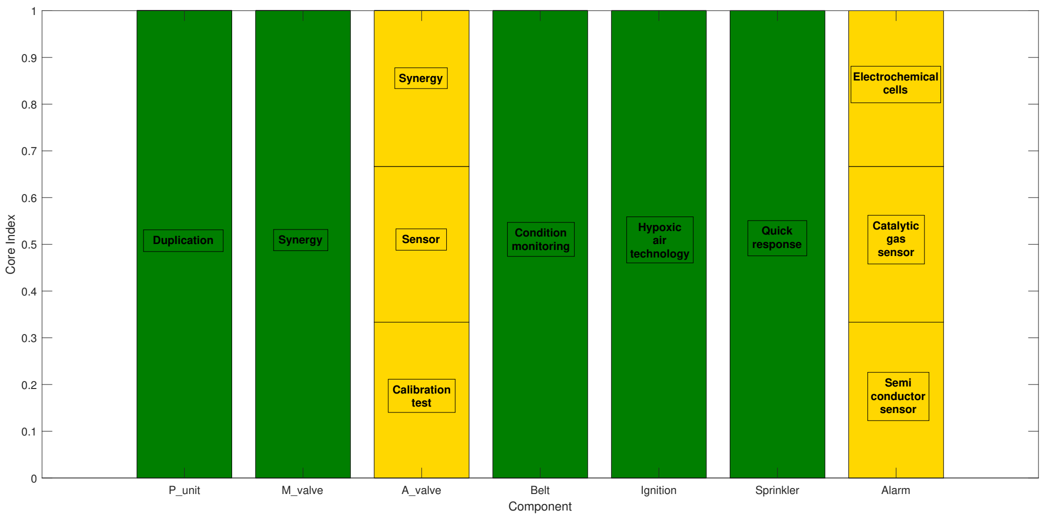

Figure 7: Core index analysis of preventive safety measures.

Because there are only few non-dominated portfolios, the solutions can be analyzed individually to select the optimal allocation of risk management resources. The overall cost of the first two non-dominated portfolios is 590 k€ and 600 k€ for the third one. Thus, portfolios $\mathbf{z}_1$ and $\mathbf{z}_2$ are the Pareto-optimal solutions that minimize the overall cost. In addition, Figure 8 shows that portfolio $\mathbf{z}_1$ dominates the other two solutions at time stages $\tau \geq 1$, but the zoomed frame at the initial time stage $\tau = 0$ highlights a higher expected disutility of 0.13% and 0.45% in comparison to portfolios $\mathbf{z}_2$ and $\mathbf{z}_3$, respectively. If such increases are significant, then portfolio $\mathbf{z}_1$ is recommended as the optimal allocation for the system.

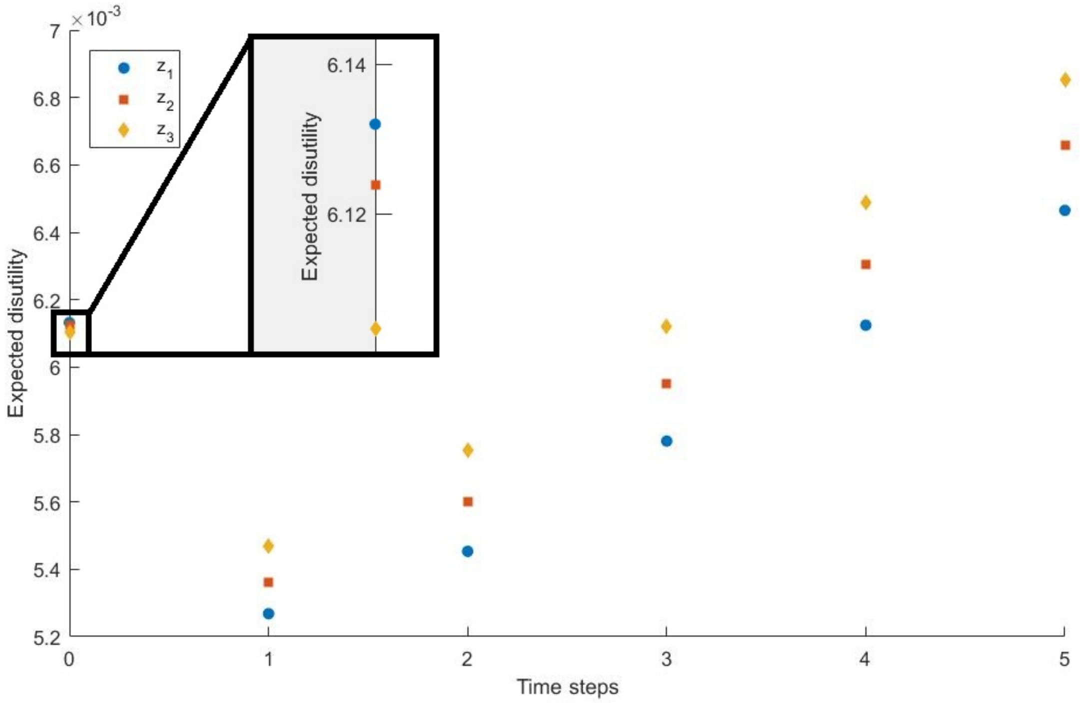

Figure 8: Expected disutility of non-dominated portfolios by setting $B = 600$ k€.

4 Discussion

330 The case study illustrates the main advantages of employing Portfolio Decision Analysis to select the optimal allocation of preventive safety measures for the system. The proposed methodology does not target the failure of the individual components; instead, it determines non-dominated portfolios that minimize the residual risk of the system throughout multiple time stages. This approach helps overcome the limitations of sequential decisions in the selection of preventive safety measures for the system, which could lead to suboptimal solutions.

The optimization algorithm is computationally efficient in generating Pareto-optimal solutions. Specifically, in the case study the computation of all non-dominated portfolios from the initial set of 2^{18} possible alternatives took approximately one minute on a regular laptop (Intel Core i5 CPU @ 2.3 GHz). Nonetheless, the algorithm may require a long computational time when the number of possible measures is large (over 40). In this case, it is possible to decompose the optimization problem into sub-problems for subsystems. The optimization algorithm has been linked to GeNIe Modeler to compute the occurrence probability of the safety targets at each time stage. The computational time depends on the constraints limiting the set of feasible portfolios. For instance, relaxing the budget constraint increases the computational time, because the set of feasible solutions is larger. However, the fathoming condition improves the algorithm efficiency by avoiding the enumeration of all 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 preventive 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. By contrast, changes in dependencies modify the dimensions and parameters of the conditional probability tables. Furthermore, the model can handle multiple states for each failure event. This representation makes the model more realistic, even if it increases the effort of eliciting the conditional probability tables.

Thanks to this comprehensive representation, the optimization model makes it possible to identify optimal choices between a single reliable component and a combination of less reliable ones. For multiple non-dominated portfolios, the core indexes support the selection/rejection of some preventive safety measures. However, the final selection calls for a detailed analysis of the alternative non-dominated portfolios according to case-specific criteria. For instance, in the case study the experts could be interested in the portfolio for minimizing the expected disutility at the initial time stages to prevent the ignition and allow people to escape the factory. In other situations, it could be optimal to choose the portfolio for which the safety target can be respected as long as possible to provide time for intervening and limiting the severity of the accident scenario.

One limitation of this methodology is the need to specify the preventive safety measures in advance, including information about their costs and impacts on the reliability of system components. Because this can be difficult in practice, future research will focus on extending this methodology to include incomplete information in the parameters of the preventive safety measures. In this respect, credal networks [33] can be employed to accommodate the imprecision through intervals of lower and upper bounds. Then, the optimization would provide solutions that are robust to changes in the model parameters.

5 Conclusions

In this paper, we have extended our earlier methodology for static systems [2] to time-dependent accident scenarios through Dynamic Bayesian Networks. The methodology employs Portfolio Decision Analysis to support the selection of preventive safety measures through multi-objective optimization. We have proposed several approaches for selecting the final decision from the set of non-dominated portfolio. We have also demonstrated the viability of the methodology by analyzing the accident scenarios of a vapor cloud ignition which occurred at Universal Form

Clamp in Bellwood (Illinois, U.S.) on 14 June 2006.

The PDA methodology can be employed especially in the design phase of process systems to choose the optimal combination of preventive safety measures that minimizes the residual risk at different time stages. Moreover, the improved availability of sensors for condition monitoring of industrial systems makes it is possible to update the required probability distributions of component states with the aim of gaining further improvements in system safety. In particular, additional preventive safety measures can then be selected based on new observations on component reliability.

One possible extension of the proposed methodology is to optimize the implementation and deployment of preventive safety measures which are activated or deactivated dynamically depending on the specific states of the system components. Such extensions can built through advances in dynamic optimization and contingent portfolio programming [34].

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 preventive 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] Nielsen, T.D. and Jensen, F.V., *Bayesian Networks and Decision Graphs*, Springer Science and Business Media (2009).

[5] 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).

[6] 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).

[7] 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).

[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] Oniśko A., Druzdzel M.J., *Impact of precision of Bayesian networks parameters on accuracy of medical diagnostic systems*, Artificial Intelligence in Medicine, pp. 197-206 (2013).

[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, https://www.csb.gov/universal-form-clamp-co-explosion-and-fire/.

[30] Mancuso A., Compare M., Salo A., Zio E., *Probabilistic model of time-dependent accident scenarios of a mixing tank mechanical system*, Data in Brief, submitted.

[31] Modarres M., Kaminskiy M.P., Krivtsov V., *Reliability Engineering and Risk Analysis: A Practical Guide*, CRC press, New York (2016).

[32] Coello C.A.C., Lamont G.B., Van Veldhuizen D.A., *Evolutionary Algorithms for Solving Multi-Objective Problems*, Springer, New York (2007).

[33] Cozman F.G., *Credal networks*, Artificial Intelligence 120(2), pp.199-233 (2000).

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