Aalto University publication series
DOCTORAL DISSERTATIONS /

Risk-informed optimization of mitigation strategies in safety-critical systems

Alessandro Mancuso

A doctoral dissertation completed for the degree of Doctor of Science (Technology) to be defended, with the permission of the Aalto University School of Science, at a public examination held at the lecture hall H304 of the school on 18 September 2020 at 12.

This doctoral thesis is conducted under a convention for the joint supervision of thesis at Aalto University (Finland) and Politecnico di Milano (Italy).

Aalto University
School of Science
Department of Mathematics and Systems Analysis
Systems Analysis Laboratory

Supervising professors
Professor Ahti Salo, Aalto University, Finland
Professor Enrico Zio, Politecnico di Milano, Italy

Thesis advisors
Doctor Michele Compare, Politecnico di Milano, Italy
Doctor Piotr Zebrowski, International Institute for Applied Systems Analysis, Austria

Preliminary examiners
Professor Genserik Reniers, Delft University, Netherlands
Professeur Vincent Mousseau, CentraleSupelec, France

Opponent
Professor Lesley Walls, University of Strathclyde, UK

Aalto University publication series
DOCTORAL DISSERTATIONS /

ISBN (printed)
ISBN (pdf)
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)
http://urn.fi/URN:ISBN:

Unigrafia Oy
Helsinki

Finland

Printed matter
4041-0619

Author
Alessandro Mancuso

Name of the doctoral dissertation
Risk-informed optimization of mitigation strategies in safety-critical systems

Publisher School of Science

Unit Department of Mathematics and Systems Analysis

Series Aalto University publication series DOCTORAL DISSERTATIONS /

Field of research Systems and Operations Research

Manuscript submitted 11 December 2019 **Date of the defence** 18 September 2020

Permission for public defence granted (date) 24 March 2020 **Language** English

☐ **Monograph** ☒ **Article dissertation** ☐ **Essay dissertation**

Abstract

Industrial organizations need to invest in the design and operations of their production systems to improve reliability, availability, maintainability and safety. Typically, these organizations have limited resources, therefore they can select only a subset of mitigation actions to protect the system from the risks associated with accident and threat scenarios. For this reason, optimization models for resource allocation are necessary to minimize the risks of such scenarios.

In current practices, resources are often allocated based on the failure risk of the individual components, which can lead to sub-optimal solutions. By contrast, this Dissertation proposes systemic analyses of accident and threat scenarios in order to determine the optimal mitigation strategy for the overall system. The optimal strategy is a combination (portfolio) of mitigation actions for system design and operations that minimize the systemic risks, while satisfying relevant budgetary and technical constraints.

For this purpose, the probabilistic analysis of the systemic risks is performed through Bayesian models to capture the uncertainties of the accident and threat scenarios. Then, the selection of the optimal resource allocation builds on Portfolio Decision Analysis to determine the optimal portfolios consisting of a set of discrete alternatives. In addition, the methodologies allow a range of sensitivity analyses on budget allocation and risk management of the accident and threat scenarios.

The methodologies are illustrated by revisiting real-life case studies and reported examples in the context of system design and operations, to demonstrate that systemic analyses integrate the current practices on component-based resource allocation. The methodologies are also generic in that they can be employed in other application areas with reasonable adaptations.

Keywords Risk Management, Safety-Critical Systems, Bayesian Networks, Portfolio Decision Analysis, Constrained Optimization.

ISBN (printed)	**ISBN (pdf)**
ISSN (printed) 1799-4934	**ISSN (pdf)** 1799-4942
Location of publisher Helsinki	**Location of printing** Helsinki **Year**
Pages 143	**urn** http://urn.fi/URN:ISBN:

Preface

This Dissertation is the final realization of challenging and fruitful years of personal and collaborative work. Luckily, I had my fair share of reliable, competent and trustworthy people standing with me. For this reason, I dedicate my doctoral Dissertation to each and every one of them.

I particularly wish to thank my supervisors, professors Ahti Salo and Enrico Zio, for the support to my personal development and my skills in critical thinking and problem solving. Together with my supervisors, my instructors, doctors Michele Compare and Piotr Żebrowski, contributed to this Dissertation through their close guidance on mathematical modelling and scientific writing. I deeply appreciated all the comments and suggestions provided by my supervisors and instructors, which have been essential for the development of this Dissertation. I also express my gratitude to the Strategic Research Council of the Academy of Finland and the Finnish Research Programme on Nuclear Power Plant Safety for the financial support to my doctoral studies.

I wish to thank my colleagues at Aalto University and Politecnico di Milano, who have been integral part of my experience in academia. I have spent the last five years surrounded by extraordinary people, who I admire for their competences and interests. It was a pleasure to discuss together as mutual exploration of our research topics. Such conversations have been essential to express and organize my thoughts towards the accomplishment of this Dissertation. Such support has proved invaluable to me, hopefully reciprocal. I particularly wish to thank Edoardo Tosoni and Matteo Brunelli who shared with me this experience in Finland, inside and outside the office. A special thanks also to the proud members of room Y224, past and present, for their friendship and warmth during these years.

I am extremely grateful to my girlfriend Kata for supporting my mental stability in these years together. Her thoughts and advises encouraged me through the challenging moments of this Dissertation. She also inspired me in the search for visual beauty, even in scientific publications.

During my doctoral studies, my dear family has always been right beside me. Isabella, Lillo and Eleonora have been strong pillars throughout the process towards my graduation by paying careful attention and supporting me in the

organization of my thoughts and actions. Such attention also includes the careful preparation of food by my grandmas, Marina and Lucia, to feed my creativity and slow my productivity down. I also wish to remember my grandfathers, Gianni and Filippo.

Last but not least, I wish to thank my friends, Alberto, Maurizio, Andrea, Stefano and Francesco, for the invaluable moments we spent together throughout these years. This Dissertation finally proves them that I have *actually* delivered some results during the last five years.

Helsinki, June 17, 2020,

Alessandro Mancuso

Contents

List of Publications

This Dissertation is an overview of the following Publications, which are presented as Roman numerals throughout the thesis.

I Alessandro Mancuso, Michele Compare, Ahti Salo and Enrico Zio. Portfolio optimization of safety measures for reducing risks in nuclear systems. *Reliability Engineering and System Safety*, 167:20-29, November 2017.

II Alessandro Mancuso, Piotr Żebrowski and Aitor Couce Vieira. Risk-based selection of mitigation strategies for cybersecurity of electric power systems. *Manuscript*, 25 pages, May 2019.

III Alessandro Mancuso, Michele Compare, Ahti Salo and Enrico Zio. Portfolio optimization of safety measures for the prevention of time-dependent accident scenarios. *Reliability Engineering and System Safety*, 190(106500):1-9, October 2019.

IV Alessandro Mancuso, Michele Compare, Ahti Salo and Enrico Zio. Probabilistic model data of time-dependent accident scenarios for a mixing tank mechanical system. *Data in Brief*, 25(104243):1-5, August 2019.

V Alessandro Mancuso, Michele Compare, Ahti Salo, Enrico Zio and Tuija Laakso. Risk-based optimization of pipe inspections in large underground networks with imprecise information. *Reliability Engineering and System Safety*, 152:228-238, August 2016.

VI Alessandro Mancuso, Michele Compare, Ahti Salo and Enrico Zio. Optimal Prognostics and Health Management-driven inspection and maintenance strategies for industrial systems. *Manuscript*, 24 pages, December 2019.

Author's Contribution

Publication I: "Portfolio optimization of safety measures for reducing risks in nuclear systems"

Mancuso is the primary author. Salo and Zio proposed the research topic. Mancuso and Compare formulated the model under the guidance of Salo. Mancuso performed numerical analyses and computations for the case study. Mancuso and Compare wrote the paper under the guidance of Salo and Zio.

Publication II: "Risk-based selection of mitigation strategies for cybersecurity of electric power systems"

Mancuso is the primary author. Mancuso and Żebrowski proposed the research topic. Mancuso formulated the model under the guidance of Żebrowski. Couce Vieira provided expertise on cybersecurity. Mancuso performed numerical analyses and computations for the case study. Mancuso wrote the paper under the guidance of Żebrowski.

Publication III: "Portfolio optimization of safety measures for the prevention of time-dependent accident scenarios"

Mancuso is the primary author. Salo and Zio proposed the research topic. Mancuso and Compare formulated the model under the guidance of Salo. Mancuso performed numerical analyses and computations for the case study. Mancuso and Compare wrote the paper under the guidance of Salo and Zio.

Publication IV: "Probabilistic model data of time-dependent accident scenarios for a mixing tank mechanical system"

Mancuso is the primary author. Mancuso and Salo proposed the research topic. Mancuso performed numerical analyses and computations for the case study. Mancuso and Compare wrote the paper under the guidance of Salo and Zio.

Publication V: "Risk-based optimization of pipe inspections in large underground networks with imprecise information"

Mancuso is the primary author. Salo and Laakso proposed the research topic. Mancuso and Compare formulated the model under the guidance of Salo. Laakso provided data and expertise on the water network system. Mancuso performed numerical analyses and computations for the case study. Mancuso and Compare wrote the paper under the guidance of Salo and Zio.

Publication VI: "Optimal Prognostics and Health Management-driven inspection and maintenance strategies for industrial systems"

Mancuso is the primary author. Mancuso and Salo proposed the research topic. Salo formulated the model, which has been extended by Mancuso and Compare for applications to Prognostics and Health Management. Mancuso performed numerical analyses and computations for the case study. Mancuso and Compare wrote the paper under the guidance of Salo and Zio.

Abbreviations

BN	Bayesian Network
BT	Bow Tie
CVaR	Conditional Value at Risk
DBN	Dynamic Bayesian Network
ET	Event Tree
ETA	Event Tree Analysis
FT	Fault Tree
FTA	Fault Tree Analysis
IIoT	Industrial Internet of Things
MAUT	Multi Attribute Utility Theory
MAVT	Multi Attribute Value Theory
MCDA	Multi Criteria Decision Analysis
PDA	Portfolio Decision Analysis
PHM	Prognostics and Health Management
PRA	Probabilistic Risk Assessment
RIM	Risk Importance Measure
RPM	Robust Portfolio Modeling
VaR	Value at Risk
VoPI	Value of Perfect Information
VTA	Value Tree Analysis

1. Introduction

In industrial practice, Probabilistic Risk Assessment (PRA) is employed to quantitatively assess the failure risk of systems and components [1, 2, 3]. Risk importance measures, such as Risk Reduction Worth, Fussel-Vesely and Risk Achievement Worth, define the importance ranking of the components, based on the impact of component failures on the system. Thus, the resource allocation for system improvements often relies on such ranking [4].

This iterative practice involves (i) the identification of components with the highest impact on systemic risk and (ii) the deployment of preventive mitigation actions to reduce their failure probabilities. The procedure is iterated until the budget for system improvements is depleted or the risk becomes acceptable with respect to regulatory criteria [5]. However, the resulting portfolio of preventive mitigation actions may be sub-optimal due to the lack of systemic perspective [6], whereby budget and technical constraints are considered only afterwards. In addition, the many different risk importance measures in the literature can lead to different rankings of critical components, therefore experts need to interpret the results to prioritize the resource allocation. Table 1.1 summarizes the advantages of systemic analysis in the selection of preventive mitigation strategies for safety-critical systems.

This Dissertation shows that a systemic approach overcomes the limitations of selecting mitigation actions based on the failure risk of individual components.

Table 1.1. Comparison of practices for reliability analysis.

Individual components	**Systemic analysis**
Analysis of the failure risk of *single components*	Analysis of the accident/threat scenarios for the *overall system*
Interpretation of importance measures to prioritize mitigation actions	Selection of the optimal strategies for system reliability and safety
Costs and feasibility of mitigation actions are considered only afterwards	The optimization model accounts for financial and technical constraints

1.1 Objectives and scope

This Dissertation presents methodological advances to improve reliability, availability, maintainability and safety of complex technological systems [7]. Specifically, the methodologies support decisions on *system design* and *system operations* to mitigate the failure risk.

The applications of the methodologies to various technical systems show the potential of systemic analysis in the optimization of risk mitigation strategies. The contributions in this Dissertation indicate that a comprehensive analysis of the technical system can lead to relevant improvements in risk mitigation, compared to current practices.

The optimization models of this Dissertation consider single or multiple objectives, concerning reliability, availability, maintainability and safety of the system. Information sources are logical structures from traditional practices (such as binary gates from Fault Tree analysis), statistical analyses and expert elicitation. The optimization solutions are robust to imperfect information by accommodating aleatory and epistemic uncertainties [8].

Table 1.2 summarizes the scope of the Publications in terms of methodological differences in the model objectives, information sources and uncertainty quantification. Publication II and Publication III consider multiple objectives, in particular the risks on multiple accident outcomes and the risks on multiple time stages, respectively. Publication IV is not included in Table 1.2 because it is a data article, which does not constitute an independent research contribution.

Table 1.2. Scope of the Publications.

Publication	Focus	Objectives	Information	Uncertainty
Publication I	Design	Single	Statistical analyses	Aleatory
Publication II	Design	Multiple	Statistical analyses	Aleatory
Publication III	Design	Multiple	Statistical analyses	Aleatory
Publication V	Operations	Multiple	Expert	Epistemic
Publication VI	Operations	Single	Sensors	Aleatory

1.2 Dissertation structure

The Dissertation proposes several contributions both to *system design* and *system operations* in the field of risk-informed optimization of mitigation strategies. Figure 1.1 outlines the Dissertation structure, where squares represent the main models, circles indicate model variants and double circles refer to the information sources.

For system design, the Dissertation presents an optimization model to select the mitigation strategies that minimize the risk of system failure. Specifically, the accident scenarios are represented through a Bayesian Network to assess the consequences of the component failures. The Bayesian model is presented in Publication I and Publication II with applications to accident scenarios and threat scenarios, respectively. Then, Publication III extends the Bayesian model to time-dependent accident scenarios. Publication IV describes a case study on the time-dependent accident scenarios of a mechanical system.

For system operations, the Dissertation includes Publication V and Publication VI. The former provides a framework to optimize inspection strategies of a pipe network. The latter presents an optimization model to select the inspection and maintenance strategies for maximizing the utility of an industrial system [9]. Specifically, the first model is based on expert judgment about the impact of pipe features on the risk of system failure, whereas the second model is based on system monitoring through sensors.

In the rest of this introductory summary chapter, Section 2 presents the methodological foundations of the Dissertation, Section 3 summarizes the contributions of the Publications. Finally, Section 4 discusses potential implications and outlines extensions for future research.

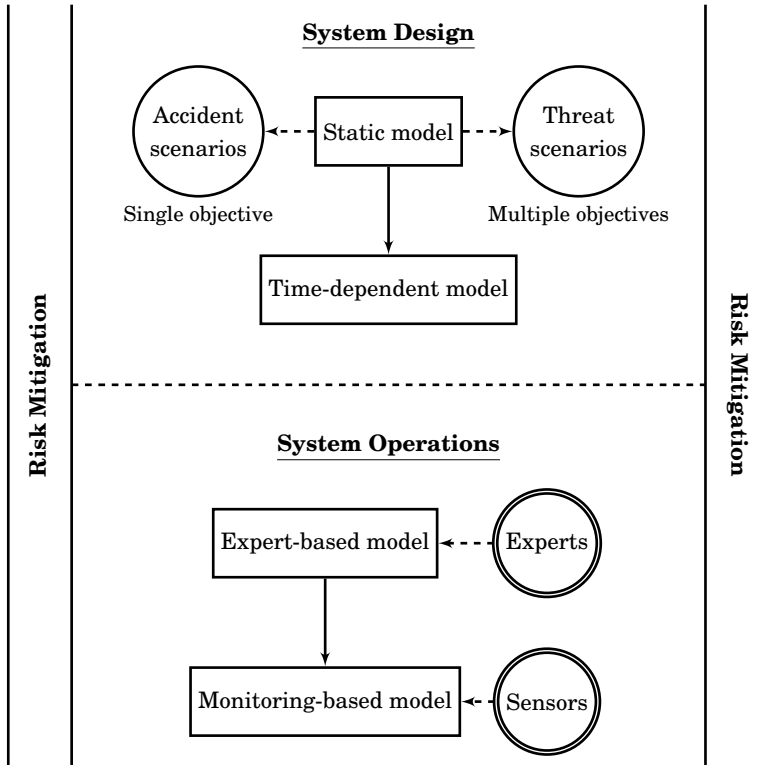


Figure 1.1. Dissertation structure.

2. Methodological Foundations

This Section presents the methodological foundations of the Dissertation. Specifically, Bayesian models represent the consequences of the component failures, whereas risk assessment is based on Multi-Attribute Value Theory and Multi-Attribute Utility Theory. The selection of the optimal mitigation strategies builds on Portfolio Decision Analysis (PDA).

2.1 Bayesian models for reliability analysis

The analysis of safety-critical systems typically relies on traditional frameworks, like Fault Trees (FT) and Event Trees (ET). Fault Tree Analysis (FTA) is based on the identification of an undesired event, called Top Event. Then, the formulation of the FT proceeds from the failure events to their causes, until the failure of the basic components. In FTA, failure events are binary and statistically independent, while their dependencies are represented by means of logic gates. Event Tree Analysis (ETA) is based on the identification of an initiating event, which is followed by a sequence of hazardous events. Each hazardous event leads to a finite set of outcomes which occur with a given probability. Finally, the ET represents the possible consequences of the accident scenarios [10, 11].

Bow-Tie (BT) combines the scenario modeling and quantification of FT and ET. Among the various techniques for the analysis of safety-critical systems, Bow-Tie analysis is a popular technique as it represents an accident scenario from causes to effects [12]. The application of BT in reliability analysis is limited due to: (i) the static nature of FT and ET, (ii) the inability to represent conditional dependencies and (iii) difficulties in handling imprecise information [13]. In cybersecurity management, the analysis of individual cyber threat scenarios is based on attack graphs, multi-leveled diagrams describing threats to cyber-physical systems and possible attacks to realize such threats [14]. Attack graphs have largely the same limitations as Bow Ties.

To overcome these limitations, the BT can be mapped into a Bayesian Network (BN) which makes it possible to employ Bayesian inference and prediction for

reliability models [15]. Formally, a BN is a directed acyclic graph consisting of

chance nodes representing random events of the accident/threat scenarios, leading to system failure;

arcs indicating causal dependencies among nodes.

The main feature of BNs is the possibility to include local conditional dependencies by directly specifying the causes that influence a specific effect, based on expert judgment and quantitative knowledge [16]. Moreover, BNs allow a multi-state representation of the component failures by combining BT events into the same chance node [17].

Bayesian Networks are also capable to model time-dependent accident scenarios by explicitly representing the dynamic evolution of component failures in process systems [18]. For this purpose, Dynamic Bayesian Networks (DBNs) generalize BNs by connecting nodes over multiple time stages [19].

One limitation of BNs in reliability analysis is the need to elicit the conditional probability tables for all component failures. Because this task can be difficult in practice, Bayesian models can be extended to include incomplete information. In this respect, credal networks accommodate imprecision through probability intervals, in order to provide robust assessments on the failure risk of the system [20].

The impact of risk mitigation strategies on system reliability can be evaluated through influence diagrams [21, 22]. Specifically, decision nodes represent the choice of mitigation actions, as illustrated in Figure 2.1. Each arc directed from a decision node (square) to a chance node (circle) indicates that the deployment of the mitigation action affects the occurrence probability of the event represented by the chance node. Utility nodes (diamonds) represent the (dis)utility of possible outcomes of the accident/threat scenarios.

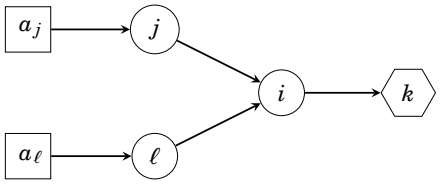


Figure 2.1. Example of influence diagram.

Let mitigation actions be numbered $a \in \{1,2,...,N\}$ so that the binary variable z_a indicates the deployment of the mitigation action a. Specifically, the binary variable is $z_a = 1$ for the deployment of the mitigation action a and $z_a = 0$ otherwise. Thus, a portfolio is defined by the binary vector $\mathbf{z}$ as a combination of binary variables z_a for all the possible mitigation actions. With no loss of generality, the vector $\mathbf{z}$ lists binary variables such that

$$\mathbf{z} = [z_1, z_2, \dots, z_N]. \tag{2.1}$$

In influence diagrams, the probability of the cascading events throughout the accident/threat scenarios is computed through the *law of total probability* [23]. Thus, the expected impacts of the accidents/threats quantify the risks of the system, which depend on the deployment of the portfolio of mitigation actions $\mathbf{z}$. This framework aims to compute the risk of accident/threats for all impact criteria, making it possible to select mitigation strategies based on the minimization of the expected impacts. The selection of mitigation strategies may depend on the states of random events of the accident/threat scenarios, if chance nodes affect decisions in the influence diagram.

2.2 Multi-criteria decision analysis

Multi-Criteria Decision Analysis (MCDA) aims to structure and solve decision problems by explicitly evaluating alternatives with regard to multiple conflicting criteria [24]. Typically, such problems may not have a unique optimal solution, therefore it is necessary to use decision-maker's preferences to differentiate between solutions [25]. Several methods for multi-criteria decision analysis are available in literature, however this Dissertation focuses on Multi-Attribute Value Theory [26] and Multi-Attribute Utility Theory [27].

In Value Tree Analysis (VTA), a value tree consists of: a *fundamental objective*, possible *lower-level objectives*, *attributes* that measure the achievement of the objectives and *alternatives* whose attribute specific performance are being measured. The attributes $a_1, a_2, ..., a_n$ have *measurement scales* $X_i, i = 1, 2, ..., n$. Alternatives $x = (x_1, x_2, ..., x_n)$ are characterized by their performance with regard to the attributes. Multi-Attribute Value Theory (MAVT) supports decision recommendations when attribute-specific values are certain.

A value function v maps the attribute-specific measurement scale onto a numerical scale in accordance with the decision maker's preferences. Attribute-specific value functions are assessed by (i) defining measurement scales $[x_i^0, x_i^*]$ and (ii) specifying equally preferred differences in attribute levels. Value functions can be normalized such that $v_i(x_i^0) = 0$ and $v_i(x_i^*) = 1$.

If the attributes are mutually preferentially independent and difference independent [28], the overall value of the alternative $x = (x_1, x_2, ..., x_n)$ is a function that aggregates attribute-specific values such that

$$V(x_1, x_2, ..., x_n) = f(v_1(x_1), v_2(x_2), ..., v_n(x_n)). \tag{2.2}$$

By defining the attribute *weights* w_i, the overall value function is a weighted sum of the attribute-specific values

$$V(x, w, v) = \sum_{i=1}^{n} w_i \, v_i(x_i). \tag{2.3}$$

The attribute weight w_i reflects the increase in overall value when the performance level on attribute a_i is changed from its worst level to its best, relative

to similar changes in other attributes. Thus, weights reflect trade-offs between attributes, not their absolute importance. Several procedures for weight elicitation are available in literature, such as trade-off weighing approaches SMART [29], SWING [30] or SMARTS [31].

Incomplete information about attribute weights can be modelled as set of feasible weights that are consistent with the decision maker's preference statements

$$S_w \subseteq S_w^0 = \{w \in \mathbb{R}^n | \sum_{i=1}^{n} w_i = 1, w_i \geq 0 \; \forall i\}. \tag{2.4}$$

Incomplete preference statements can be modelled as linear inequalities between the weights. When the weights are incompletely specified, the alternatives' overall values are intervals. For this reason, preference over interval-valued alternatives can be established based on a *dominance* relation. Specifically, alternative x^j dominates x^k in S if

$$x^j \succ_S x^k \Leftrightarrow \begin{cases} V(x^j, w, v) \geq V(x^k, w, v) & \text{for all } w \in S_w \\ V(x^j, w, v) > V(x^k, w, v) & \text{for some } w \in S_w \end{cases}. \tag{2.5}$$

The set of non-dominated alternatives is

$$X_{ND}(S_w) = \{x^k \in X | \nexists j \text{ such that } x^j \succ_{S_w} x^k\}, \tag{2.6}$$

which includes the alternatives for which there is no other alternative that has at least as high value for all feasible weights and strictly higher for some [32].

Multi-Attribute Utility Theory (MAUT) supports decision recommendations when attribute-specific performance are uncertain [33]. Specifically, alternatives are evaluated in view of a set of outcomes $t \in T$, each associated with an occurrence probability p_t. A utility function u maps the attribute-specific measurement scale onto a numerical scale in accordance with the decision maker's preferences. Attribute-specific utility functions are assessed by (i) defining measurement scales $[x_i^0, x_i^*]$ and (ii) specifying equally preferred lotteries. Utility functions can be normalized such that $u_i(x_i^0) = 0$ and $u_i(x_i^*) = 1$.

If the attributes are mutually preferentially independent and additive independent, the overall utility function in a specific outcome $t \in T$ can be expressed as

$$U_t(x_1, x_2, ..., x_n) = \sum_{i=1}^{n} w_i \, u_i(x_i). \tag{2.7}$$

Attribute weights are elicited similarly in MAVT and MAUT. Decision recommendations can be expressed by ranking the alternatives based on their expected utility

$$\mathbb{E}[U(x)] = \sum_{t \in T} p_t \, U_t(x) = \sum_{t \in T} p_t \sum_{i=1}^{n} w_i \, u_i(x_i). \tag{2.8}$$

Incomplete information about attribute weights can be also modelled in MAUT, thus preference over interval-valued alternatives can be established through a dominance relation on expected utilities.

2.3 Portfolio models for resource allocation

Portfolio decisions involve the selection of a combination (portfolio) of items from a large set of alternatives [34]. These decision problems are often characterized by multiple conflicting objectives. In this Dissertation, the optimal mitigation strategies are cost-efficient solutions that minimize the risks of system failure.

Typically, the resource allocation builds on the selection of a portfolio of projects, subject to resource constraints. Thus, portfolio selection is fundamental for strategic decisions in public administration [35, 36, 37] and industrial investments [38, 39, 40]. In this framework, the optimization of resource allocation relies on Portfolio Decision Analysis (PDA, [41]).

Based on the problem formulation by Liesiö et al. [42, 43], the set $X = \{x^1, ..., x^m\}$ includes m projects which are evaluated on n criteria. The score matrix $v \in \mathbb{R}^{m \times n}$ is composed of score vectors $v^j = [v_1^j, ..., v_n^j]$, which specify the evaluation scores of project x^j with regard to criteria $i = 1, ..., n$.

A project portfolio $p \subseteq X$ is a subset of available projects, thus the set of all possible portfolios is the power set $P := 2^X$. Each portfolio p can be represented by a binary vector $z(p) \in \{0,1\}^{1 \times m}$ such that

$$z_j(p) = \begin{cases} 1 & \text{if } x^j \in p \\ 0 & \text{if } x^j \notin p \end{cases}. \tag{2.9}$$

The overall value of portfolio p is captured through an additive value function

$$V(p, w, v) = \sum_{x^j \in p} \sum_{i=1}^{n} w_i \, v_i^j = z(p) \, v \, w, \tag{2.10}$$

where the vector $w \in \mathbb{R}^{n \times 1}$ specifies the criteria weights.

The portfolio selection may have to fulfill various *budget*, *logical*, *positioning* and *threshold* constraints. Typically, the set of feasible portfolios can be characterized by a set of linear inequalities such that the coefficients are recorded in matrix $A \in \mathbb{R}^{q \times m}$ and vector $B \in \mathbb{R}^q$. Thus, the set of feasible portfolios is

$$P_F = \{p \in P | A \, z(p) \leq B\}, \tag{2.11}$$

where $\leq$ holds componentwise.

The optimal feasible portfolio maximizes the overall value through the integer linear problem

$$\max_{p \in P_F} V(p, w, v) = \max_{z(p)} \{z(p) \, v \, w | A \, z(p) \leq B, \, z(p) \in \{0,1\}^m\}. \tag{2.12}$$

Because the elicitation of exact weights and scores can be difficult, Robust Portfolio Modeling (RPM, [42, 43]) supports the selection of portfolios in the presence of multiple criteria and incomplete information. Specifically, the decision maker's preference statements are converted into a set of feasible criteria

weights $S_w \subseteq S_w^0$, whereas the set of feasible scores is

$$S_v = \{v \in \mathbb{R}^{m \times n} | \underline{v} \leq v \leq \overline{v}\}. \tag{2.13}$$

The information set of feasible weights and scores is the Cartesian product

$$S = S_w \times S_v. \tag{2.14}$$

For this reason, preference over interval-valued portfolios can be established through a *dominance* relation. Specifically, portfolio p^* dominates p in S if

$$p^* \succ_S p \Leftrightarrow \begin{cases} V(p^*, w, v) \geq V(p, w, v) & \text{for all } (w, v) \in S \\ V(p^*, w, v) > V(p, w, v) & \text{for some } (w, v) \in S \end{cases}. \tag{2.15}$$

The set of non-dominated portfolios is

$$P_N(S) = \{p \in P_F | \nexists p^* \text{ such that } p^* \succ_S p\}. \tag{2.16}$$

To facilitate the analysis of the set of non-dominated portfolios, Liesiö et al. [42, 43] introduce the notion of *core index*. The core index of a project x^j is the share of non-dominated portfolios that include the project such that

$$CI(x^j, S) = \frac{|\{p \in P_N | x^j \in p\}|}{|P_N|}. \tag{2.17}$$

The core index values support the selection and rejection of projects. Specifically, if the core index of a project is one, the project can be selected because it belongs to all non-dominated portfolios; on the other hand, if the core index of a project is zero, the project can be rejected because it is not included in any non-dominated portfolio. Decisions concerning projects whose core index values are in the open interval $(0, 1)$ can be taken based on the elicitation of additional information about the decision maker's preferences [44, 45, 46].

The selection of project portfolios can also account for exogenous uncertainties, which may affect the project performance. For this purpose, it is necessary to analyze the project performance across several scenarios and select the portfolio that maximizes the expected utility [47]. Because the elicitation of scenario probabilities can be difficult, scenario-based portfolio models capture incomplete information about scenario probabilities and utility functions through set inclusion in order to identify all non-dominated portfolios [48]. The non-dominated portfolios are (i) robust to incomplete information about scenarios and (ii) proactive by steering the course of change towards the desired scenario [49].

3. Contributions of the Dissertation

Table 3.1 summarizes the contributions of the Publications in this Dissertation. Generally, the Publications present (i) the risk model of the analyzed system and (ii) the optimization model to select portfolios of risk mitigation actions.

The risk models are represented by various techniques, specifically Bayesian Networks in Publication I and Publication II, Dynamic Bayesian Networks in Publication III, Value Tree Analysis in Publication V and influence diagrams in Publication VI. The choice of the modelling techniques mainly derives from the information sources for the specific decision problem.

The optimization models build on Portfolio Decision Analysis to minimize the systemic risk by deploying preventive mitigation actions to the individual components. In particular, the optimization algorithms rely on implicit portfolio enumeration in Publication I, Publication II and Publication III, Robust Portfolio Modelling in Publication V and mixed integer linear programming in Publication VI.

Each of the Publications presents a case study to show the viability of the methodology and additional insights on the optimization results. Following the presentation order of the Publications, the Dissertation shows applications to the airlock system of a CANDU nuclear power plant, the advanced metering infrastructure of an electric power system, the mixing tank mechanical system of a concrete production industry, the underground pipe network of Espoo water system and a gas turbine with sensor monitoring capabilities. The applications are illustrative case studies that have been previously analyzed in literature or real-life case studies based on statistical data and expert elicitation.

Publication I and Publication II also review the current practices to choose preventive mitigation strategies for industrial systems and cyber-physical systems, respectively. These analyses compare the current practice with the methodologies presented in the Publications in order to discuss the potential and limitations of both approaches.

The following Sections summarize the main contributions and results of each Publication.

Table 3.1. Summary of the Publications.

Publication	Research objectives	Methodology	Main results
Publication I	Development of an optimization model to select the portfolio of preventive mitigation strategies that minimizes the failure risk of industrial systems.	Bayesian Networks, Portfolio Decision Analysis, Risk Importance Measures.	Formulation of a probabilistic model of the accident scenarios; Development of an optimization algorithm; Model validation on a nuclear safety system.
Publication II	Development of an optimization model to select the Pareto-optimal mitigation strategies that minimize the risks of cyber threats.	Bayesian Networks, Portfolio Decision Analysis, Multi-objective optimization.	Analysis of the current practice; Formulation of a Bayesian framework to model the cyber threat scenarios; Model validation on an electric power system.
Publication III	Development of an optimization model to select the Pareto-optimal portfolios of preventive mitigation strategies that minimize the failure risk of time-dependent accident scenarios.	Dynamic Bayesian Networks, Portfolio Decision Analysis, Multi-objective optimization.	Formulation of a probabilistic model that captures the temporal evolution of component failures; Extension of the optimization algorithm to multi-objective optimization.
Publication IV	Presentation of the case study on time-dependent accident scenarios of the vapour cloud ignition of a mechanical system.	Probability theory, Data analysis.	Benchmark data for future research; Model of time-dependent accident scenarios through conditional probability tables.
Publication V	Development of a methodology to optimize the inspection strategies of large underground infrastructure networks, based on imprecise expert information.	Multi-Attribute Value Theory, Robust Portfolio Modelling, Cost benefit analysis.	Definition of pipe features that affect likelihood and impact of network ruptures; Selection of the optimal inspection strategy for the Espoo water system.
Publication VI	Development of a methodology to optimize inspection and maintenance strategies of industrial systems with PHM capabilities, based on imperfect monitoring information.	Influence diagrams, Decision Programming, Mixed-Integer Linear Programming.	Definition of causal dependencies between system state and mitigation strategies; Selection of the optimal inspection and maintenance strategies; Computation of Value of Information.

3.1 Publication I

The selection of mitigation strategies to limit the risk of accidents is a crucial decision in safety management. In the framework of Probabilistic Risk Assessment [50], this Publication develops a methodology to support the selection of cost-efficient portfolios of preventive mitigation actions. This methodology provides a systemic approach to define the portfolio of mitigation actions that minimizes the risk of the system failure. Thus, it provides an alternative to risk importance measures for guiding the selection of preventive mitigation actions [51].

Bayesian Networks [52] are employed to represent the alternative scenarios leading to system failure, by deriving the accident scenarios from traditional Fault Trees. Unlike Fault Trees, Bayesian Networks are capable of encoding event dependencies and multi-state failure behaviours. Nodes represent random events of the accident scenarios whereas arcs indicate causal dependencies among the component failures.

The optimization model considers a single objective so that the optimal strategy is the one that minimizes the residual risk of system failure. The model includes regulatory, budget and technical constraints. In addition, we developed an implicit enumeration algorithm [53] to determine the optimal portfolio of preventive mitigation actions on the system components. By running the optimization model for different budget levels, the analysis of the risk profile supports decisions on safety investments based on the convergence of the systemic risk or the definition of a target risk.

Publication I demonstrates the viability of the methodology by revisiting the Design Basis Accident that occurred in the airlock system of a CANDU nuclear power plant in 2011 [54]. The results of the case study indicate that the systemic risk can be reduced by 21% in comparison to the choice of mitigation actions based on risk importance measures. The illustrative example proves that risk importance measures do not necessarily lead to optimal decisions, because the computation of the risk importance measures depends on the previous decisions at each iteration. Furthermore, RIM-based decisions involves assumptions and expert judgment, which can affect the decisions at the following iterations and the resulting portfolio of preventive mitigation actions.

3.2 Publication II

As cyber-physical systems, electric power systems are highly vulnerable to cyber threats which have led to frequent and costly impacts worldwide [55]. Among the most relevant episodes, a cyber-attack to an electric grid caused a power outage in Ukraine in 2015 [56]. These episodes call for the efficient allocation of resources to minimize the risks of cyber threats. Standard approaches guide the selection of mitigation strategies by prioritizing the cyber threat scenarios

through a qualitative assessment [57]. These approaches consider cyber threat scenarios separately, thus they possibly result in sub-optimal resource allocations for the system [58]. In this context, Publication II proposes a systemic analysis based on Bayesian Networks to quantify the risks of cyber threats to electric power systems. In the Bayesian model, nodes represent the random events in cyber threat scenarios and arcs show the causal dependencies among these random events. Mitigation actions reduce the likelihood of potentially threatening events thus mitigate the risks of cyber threats, evaluated as the expected impacts on multiple criteria, such as safety, economy and customer service. Thus, a mitigation strategy is Pareto optimal if no other feasible strategy further reduces the risks of cyber threats for any impact criterion without increasing the risk for any other criteria. The selection of Pareto optimal strategies is based on an implicit enumeration algorithm that considers budget and technical constraints.

Publication II illustrates the methodology by analyzing the cyber threat scenarios concerning the advanced metering infrastructure of an electric power grid. The model provides additional insights on risk management when performed for different budget levels. In particular, increasing the budget level leads to the implementation of mitigation strategies that are increasingly effective, thus reducing the risks of cyber threats. In case of multiple Pareto optimal portfolios, further analyses support the selection of cost-efficient solutions from the set of Pareto optimal portfolios.

The choice of the optimal mitigation strategy relies on a systemic analysis of multiple cyber threat scenarios. This framework can be introduced as a novel practice for assessing the risks of cyber threats and for supporting risk-based decisions on resource allocation to cyber-physical systems.

3.3 Publication III

The final outcome of accident scenarios can depend on the *order*, *timing* and *magnitude* of the component failures. If the risk analysis does not account for the dynamic evolution of failures, it may fail to consider severe accident scenarios [59]. For this reason, Publication III extends the methodology in Publication I to support the selection of cost-efficient portfolios for time-dependent accident scenarios. Dynamic Bayesian Networks are capable of representing alternative scenarios leading to system failure, by capturing the accident dynamics as temporal evolution of component failures.

The optimization model in Publication I has been extended to solve multi-objective optimization over the time stages. Specifically, the optimization model selects all Pareto optimal portfolios of preventive mitigation actions to minimize the residual risk of the system throughout the time stages. A feasible portfolio is Pareto optimal if no other feasible portfolio decreases the residual risk of the system at some time stages without increasing the risk at any other time stage.

The implicit enumeration algorithm in Publication I has been extended to compute the set of Pareto optimal portfolios of preventive mitigation actions. In addition, we discuss several approaches to select the optimal solution among the set of Pareto optimal portfolios, for instance supporting the selection/rejection of mitigation actions through the computation of the core index [43].

Publication III demonstrates the viability of the 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 [60]. The model represents the causal dependencies of the component failures of a mixing tank mechanical system throughout multiple time stages. The results show a sharp reduction of the residual risk of the system by increasing the budget level. The computation of the core index facilitates the selection of the optimal portfolio. The analysis of the risk profile provides additional insights on risk management.

3.4 Publication IV

This article presents the probabilistic model data of the case study presented in Publication III. Specifically, data refers to the time-dependent accident scenarios of a mixing tank mechanical system in concrete production industry. The risk assessment of the accident scenarios is based on the failure probabilities of the system components.

Possible component failures can cause accidents, which evolve over multiple time stages and can lead to system failure. Publication IV provides an example of time-dependent probabilistic model by representing the causal dependence of *Ignition* and *Sprinkler* activation over multiple time stages.

The consequences of these accident scenarios are analyzed by quantifying the failure probabilities and severity of their outcomes. Finally, the data article presents a list of preventive mitigation actions for the mixing tank mechanical system, including illustrative costs and updated failure probabilities.

3.5 Publication V

The correct operation of large infrastructure networks depends on condition inspections and preventive maintenance actions, which significantly affect the network operating costs [61]. Therefore, the efficient management of these complex networks requires the optimization of the inspection strategies.

This article presents a risk-based methodology to prioritize the inspections of a large underground infrastructure networks by (i) performing the risk assessment of the network components and (ii) optimizing the inspection strategies of the critical components. The identification of the high-risk components out of the large number of network components is driven by the definition of a portfolio optimization model which is computationally tractable.

Based on Value Tree Analysis [62], the risk assessment of each component builds on the failure likelihood and severity on the network disruption. Risk assessment of large underground networks is typically based on incomplete information about the network components. For this reason, the quantification of likelihood and severity relies on the imprecise information provided by expert judgment. Thus, the dominance relation on likelihood and severity defines the ranking of the network components based on the risk of network disruption.

The optimization model selects the cost-efficient inspection strategies that maximize the inspection benefit, achieved through the reduction of expected disruption costs as a result of pipe renovations. An inspection strategy is cost-efficient if no other feasible strategy provides a higher benefit at a lower cost. Specifically, costs and benefits are defined as interval values to consider the variability on the component degradation and the uncertainty on renovations.

Due to the large number of critical components, the approximate algorithm of Robust Portfolio Modelling [63] determines a subset of the Pareto optimal inspection strategies. The optimization model accommodates imprecise information about costs and benefits, as well as logic constraints on inspection activities. Appropriate decision rules support the selection among the set of Pareto optimal solutions, such as *maximin* or *minimax regret* rules.

Publication V demonstrates the viability of the methodology on the inspection optimization of the sewerage network system of Espoo in the Finnish Capital Region. In this case study, *likelihood* depends on pipe features, past events and local circumstances, whereas *severity* quantifies the effect of a pipe failure on the network and the surroundings [64]. The risk assessment shows that the critical pipes represent 34% of the initial data set. The optimization of the inspection strategies is performed through the RPM algorithm, where the termination condition is the convergence of the core index of the pipes.

Publication V also inspired a novel application on the risk-based maintenance of gas networks [65].

3.6 Publication VI

Digitalization is a fundamental driver of Industry 4.0 [66], which enables the development of predictive maintenance for industrial systems [67]. Predictive maintenance employs condition monitoring data recorded by Industrial Internet of Things (IIoT) devices to monitor the health of the system. This information is employed for Prognostics and Health Management (PHM, [68]) to perform

detection by identifying deviations from normal operating conditions in production processes, manufacturing equipment and products;

diagnostics by classifying abnormal states;

prognostics by predicting the evolution of abnormal states up to failure.

However, IIoT devices may provide imprecise measurements of the monitored physical parameters, which affect the performance of the PHM algorithms by conveying inaccurate or misleading information about the actual system state. Thus, these failures can cause missing alarms or unnecessary system downtimes, resulting in large financial losses.

For this reason, the definition of inspection and maintenance strategies must consider the state of the industrial system and the state of the monitoring sensors. The causal dependencies between the monitored system and the PHM capabilities are represented through influence diagrams [22]. In particular, the decisions on inspection and maintenance activities are based on the sensor data and inspection results. Information sources for the conditional probability tables are statistical analyses of equipment history, simulations and expert judgement.

This article presents a novel methodology to support inspection and maintenance decisions for industrial systems with PHM capabilities. Specifically, the optimal strategy maximizes the utility of system operations, discounted by the costs of inspection and maintenance activities. The solution to this multi-stage decision problem derives from Decision Programming [69]. Specifically, the influence diagram is first converted into a sequence of decision and chance nodes while preserving their information dependencies. Then, this sequence is transformed into an equivalent mixed-integer linear programming formulation of the multi-stage decision problem. This optimization problem can include budget and technical constraints, as well as chance constraints, for instance to curtail the Value at Risk (VaR) and the Conditional Value at Risk (CVaR) of system operations.

Publication VI demonstrates the viability of the methodology on the optimization of inspection and maintenance strategy for a gas turbine with PHM capabilities. The case study shows the computation of the Value of Perfect Information (VoPI) deriving from monitoring sensors and inspections [70]. Formally, the VoPI is the difference between the optimal expected value for two situations: (i) when the system state is correctly observed and (ii) when the system state is observed with possible errors. The computation of VoPI provides insights into the value of investments in the renovation of the PHM capabilities, based on a comparison between the VoPI and the renovation costs.

4. Discussion

4.1 Theoretical and practical implications

The Publications of this Dissertation demonstrate the importance of systemic analysis in risk prevention, which arises from resilient design and optimal operations management. The comparison with traditional approaches shows a significant reduction of systemic risks due to a comprehensive analysis of the scenario accidents [71].

The methodologies and results of this Dissertation provide relevant contributions to academia and industry. Specifically, novel practices can be introduced in industry for a systemic analysis of the possible hazards, both accidental and malicious. As demonstrated by the Publications, this analysis leads to the selection of optimal mitigation strategies to minimize the systemic risk. For instance, the risk minimization can be achieved by increasing the reliability of an individual component or by installing a system of parallel components. This choice can make a relevant difference on the reliability, availability, maintainability and safety of the industrial system, as well as on the company profitability.

In recent years, maintenance business is rapidly evolving due to the high availability of Industrial Internet of Things (IIoT) devices to monitor the condition of the system components [72]. As a consequence, this monitoring information facilitates the systemic analysis of safety-critical system to define the need for inspection and maintenance activities. These late developments are enabling new models for maintenance business by combining standard maintenance visits and predictive maintenance [73]. For instance, the TotalCare maintenance model by Rolls-Royce strongly relies on the monitoring information of the engine performance through Engine Health Monitoring [74]. In addition, companies are responsible for the reliability, availability and safety of their assets for the entire life cycle. For this reason, operational excellence drives company profitability by optimizing maintenance decisions based on systemic failure risks.

In this framework, component-based analyses (such as Risk Importance Measures) are not excluded from the risk analysis of the system, instead they are

complementary to systemic approaches. This synergy provides a comprehensive analysis, enhancing the risk management through clear representations of the possible accident/threat scenarios and detailed measures on the risk of the individual components. The analysis of the accident/threat scenarios makes also possible to evaluate the Value at Risk (VaR) and Conditional Value at Risk (CVaR) to improve the risk management of the system [75].

4.2 Prospective research directions

The models of this Dissertation show some limitations that need to be addressed in future research, for this reason here I suggest some prospective research directions. In particular, risk models need to account for the imprecision and uncertainty stemming from incomplete datasets or the qualitative statements provided by the experts. For example, the expert may provide imprecise values about costs and impacts of mitigation actions. Such imprecision and uncertainty must be properly represented and propagated throughout the optimization model to obtain robust solutions. Credal networks can be employed to accommodate the imprecision through intervals of lower and upper bounds on the occurrence probabilities [76]. Then, the optimization would provide solutions that are robust to variations in the model parameters.

Furthermore, methods to facilitate the elicitation of parameters need to be developed so that experts need not to answer many and/or complex questions on the model parameters, which could introduce biases as well. A possible solution to limit the need for expert judgement is the extension of the Bayesian models to continuous and discrete variables, which is feasible under specific conditions [77]. Another possible solution is to introduce machine learning models by developing software that implements the scientific principle: (i) formulate a hypothesis (choose a model) about the failure events, (ii) collect data to test the hypothesis (validate the model) and (iii) refine the hypothesis (iterate) [78].

An additional challenge for future research in portfolio optimization is the improvement of the computational viability of the optimization algorithms. The algorithms presented in this Dissertation are computationally efficient, thus they can solve meaningful problems for real-life industrial systems. However, they may require a long computational time for a large number of mitigation actions due to the curse of dimensionality. Decomposition of large problems into a hierarchic pyramid of sub-problems has been proposed in the literature to optimize large problems for engineering systems [79]. Furthermore, the recent advances in quantum computing prove that certain computational tasks can be executed exponentially faster on a quantum processor than on a classical processor. By relying on quantum algorithms, the methodologies in this Dissertation may be capable in future to solve portfolio optimization problems in an exponentially large computational space [80]. The dramatic increase in computational speed is due to the quality of *superposition* of qubits (quantum bits), which they

do not necessarily represent binary bits but they can take all intermediary values in the interval $[0,1]$. Although the final readout of each qubit is 0 or 1, this quality of superposition allows each qubit to perform more than one calculation at a time, reducing the computational time of the optimization algorithm [81].

A relevant application area for risk analysis is cybersecurity, discussed in Publication II. Unlike accident scenarios in industry, cyber threat scenarios do not only include random events, but also intentional attacks. For this reason, the risk model needs to consider the objectives of the threat agent(s) in order to provide one-sided decision support [82]. In this regard, Adversarial Risk Analysis supports decisions for risks in which probabilities and outcomes depend on the decisions of other self-interested agents [83].

Future research on this topic also includes the comparison of the criticality of cyber threat scenarios. Criticality could be quantified through a topological analysis of the network to quantify the in-coming and out-coming nodes or ranking the scenarios based on risk measures of the cyber threats, meaning the ratio between the current expected impact and the expected impact when the occurrence probability of that cyber threat scenario is null.

Finally, research should properly address cyber resilience, meaning the ability to continuously deliver the service despite adverse cyber events [84]. In this regard, Dynamic Bayesian Networks are capable to represent the time-dependent evolution of the outcome of cyber attacks in order to (i) compare the resilience of different systems and (ii) optimize the capacity of energy storage for electric power systems [85]. For this purpose, it is necessary to introduce temporal variables to model the system recovery over time stages: the analysis of cyber threat scenarios requires the ability to anticipate not only an unprecedented event but also the ripple effects that it could cause [86].

References

[1] George E Apostolakis. How useful is quantitative risk assessment? *Risk Analysis*, 24(3):515–520, 2004.

[2] Terje Aven, Piero Baraldi, Roger Flage, and Enrico Zio. *Uncertainty in Risk Assessment: The Representation and Treatment of Uncertainties by Probabilistic and Non-Probabilistic Methods*. John Wiley & Sons, 2013.

[3] Louis Anthony Cox Jr. *Risk Analysis of Complex and Uncertain Systems*, volume 129. Springer Science & Business Media, 2009.

[4] Way Kuo and Xiaoyan Zhu. *Importance Measures in Reliability, Risk, and Optimization: Principles and Applications*. John Wiley & Sons, 2012.

[5] Michael C Cheok, Gareth W Parry, and Richard R Sherry. Use of importance measures in risk-informed regulatory applications. *Reliability Engineering & System Safety*, 60(3):213–226, 1998.

[6] Björn Wahlström. Systemic thinking in support of safety management in nuclear power plants. *Safety Science*, 109:201–218, 2018.

[7] Enrico Zio. Integrated deterministic and probabilistic safety assessment: concepts, challenges, research directions. *Nuclear Engineering and Design*, 280:413–419, 2014.

[8] Armen Der Kiureghian and Ove Ditlevsen. Aleatory or epistemic? Does it matter? *Structural Safety*, 31(2):105–112, 2009.

[9] Geert Waeyenbergh and Liliane Pintelon. Maintenance concept development: a case study. *International Journal of Production Economics*, 89(3):395–405, 2004.

[10] Tim Bedford and Roger Cooke. *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, 2001.

[11] Enrico Zio. *An Introduction to the Basics of Reliability and Risk Analysis*, volume 13. World scientific, 2007.

[12] Nima Khakzad, Faisal Khan, and Paul Amyotte. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. *Reliability Engineering & System Safety*, 96(8):925–932, 2011.

[13] Philippe Weber, Gabriela Medina-Oliva, Christophe Simon, and Benoît Iung. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. *Engineering Applications of Artificial Intelligence*, 25(4):671–682, 2012.

[14] Nayot Poolsappasit, Rinku Dewri, and Indrajit Ray. Dynamic security risk management using Bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 9(1):61–74, 2012.

[15] David-Rios Insua, Fabrizio Ruggeri, Refik Soyer, and Simon Wilson. Advances in Bayesian decision making in reliability. *European Journal of Operational Research*, 282(1):1–18, 2020.

[16] Andrea Bobbio, Luigi Portinale, Michele Minichino, and Ester Ciancamerla. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. *Reliability Engineering & System Safety*, 71(3):249–260, 2001.

[17] Helge Langseth and Luigi Portinale. Bayesian networks in reliability. *Reliability Engineering & System Safety*, 92(1):92–108, 2007.

[18] Pierre-Etienne Labeau, Carol Smidts, and Sanjay Swaminathan. Dynamic reliability: towards an integrated platform for probabilistic risk assessment. *Reliability Engineering & System Safety*, 68(3):219–254, 2000.

[19] Kevin P Murphy and Stuart Russell. *Dynamic Bayesian Networks: Representation, Inference and Learning*. University of California, Berkeley Dissertation, 2002.

[20] Fabio G Cozman. Credal networks. *Artificial Intelligence*, 120(2):199–233, 2000.

[21] Ross D Shachter. Evaluating influence diagrams. *Operations Research*, 34(6):871–882, 1986.

[22] Ronald A Howard and James E Matheson. Influence diagrams. *Decision Analysis*, 2(3):127–143, 2005.

[23] Judea Pearl. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Elsevier, 2014.

[24] José Figueira, Salvatore Greco, and Matthias Ehrgott. *Multiple Criteria Decision Analysis: State of the Art Surveys*, volume 78. Springer Science & Business Media, 2005.

[25] Murat Köksalan, Jyrki Wallenius, and Stanley Zionts. *Multiple Criteria Decision Making: From Early History to the 21st Century*. World Scientific, 2011.

[26] James S Dyer and Rakesh K Sarin. Measurable multiattribute value functions. *Operations Research*, 27(4):810–822, 1979.

[27] Gordon B Hazen. Partial information, dominance, and potential optimality in multiattribute utility theory. *Operations Research*, 34(2):296–310, 1986.

[28] Simon French. *Decision Theory: An Introduction to the Mathematics of Rationality*. Halsted Press, 1986.

[29] Ward Edwards. How to use multiattribute utility measurement for social decision making. *IEEE Transactions on Systems, Man, and Cybernetics*, 7(5):326–340, 1977.

[30] Ward Edwards and Detloff von Winterfeldt. Decision analysis and behavioral research. *Cambridge University Press*, 604:6–8, 1986.

[31] Ward Edwards and Hutton Barron. SMARTS and SMARTER: Improved simple methods for multiattribute utility measurement. *Organizational Behavior and Human Decision Processes*, 60(3):306–325, 1994.

[32] Ahti Salo and Raimo P Hämäläinen. Preference assessment by imprecise ratio statements. *Operations Research*, 40(6):1053–1061, 1992.

[33] Ralph L Keeney. Utility independence and preferences for multiattributed consequences. *Operations Research*, 19(4):875–893, 1971.

[34] Alec Morton, Jeffrey M Keisler, and Ahti Salo. Multicriteria portfolio decision analysis for project selection. In *Multiple Criteria Decision Analysis*, pages 1269–1298. Springer, 2016.

[35] Kamal Golabi, Craig W Kirkwood, and Alan Sicherman. Selecting a portfolio of solar energy projects using multiattribute preference theory. *Management Science*, 27(2):174–189, 1981.

[36] Paul L Ewing Jr, William Tarantino, and Gregory S Parnell. Use of decision analysis in the army base realignment and closure (brac) 2005 military value analysis. *Decision Analysis*, 3(1):33–49, 2006.

[37] Yael Grushka-Cockayne, Bert De Reyck, and Zeger Degraeve. An integrated decision-making approach for improving european air traffic management. *Management Science*, 54(8):1395–1409, 2008.

[38] Christian Stummer and Kurt Heidenberger. Interactive R&D portfolio analysis with project interdependencies and time profiles of multiple objectives. *IEEE Transactions on Engineering Management*, 50(2):175–183, 2003.

[39] Mats Lindstedt, Juuso Liesio, and Ahti Salo. Participatory development of a strategic product portfolio in a telecommunication company. *International Journal of Technology Management*, 42(3):250–266, 2008.

[40] Walter J Gutjahr, Stefan Katzensteiner, Peter Reiter, Christian Stummer, and Michaela Denk. Multi-objective decision analysis for competence-oriented project portfolio selection. *European Journal of Operational Research*, 205(3):670–679, 2010.

[41] Ahti Salo, Jeffrey Keisler, and Alec Morton. *Portfolio Decision Analysis: Improved Methods for Resource Allocation*, volume 162. Springer Science & Business Media, 2011.

[42] Juuso Liesiö, Pekka Mild, and Ahti Salo. Preference programming for robust portfolio modeling and project selection. *European Journal of Operational Research*, 181(3):1488–1505, 2007.

[43] Juuso Liesiö, Pekka Mild, and Ahti Salo. Robust portfolio modeling with incomplete cost information and project interdependencies. *European Journal of Operational Research*, 190(3):679–695, 2008.

[44] Juuso Liesiö and Antti Punkka. Baseline value specification and sensitivity analysis in multiattribute project portfolio selection. *European Journal of Operational Research*, 237(3):946–956, 2014.

[45] Thomas Fliedner and Juuso Liesiö. Adjustable robustness for multi-attribute project portfolio selection. *European Journal of Operational Research*, 252(3):931–946, 2016.

[46] Tommi Tervonen, Juuso Liesiö, and Ahti Salo. Modeling project preferences in multiattribute portfolio decision analysis. *European Journal of Operational Research*, 263(1):225–239, 2017.

[47] Derek Bunn and Ahti Salo. Forecasting with scenarios. *European Journal of Operational Research*, 68(3):291–303, 1993.

[48] Juuso Liesiö and Ahti Salo. Scenario-based portfolio selection of investment projects with incomplete probability and utility information. *European Journal of Operational Research*, 217(1):162–172, 2012.

[49] Eeva Vilkkumaa, Juuso Liesiö, Ahti Salo, and Leena Ilmola-Sheppard. Scenario-based portfolio model for building robust and proactive strategies. *European Journal of Operational Research*, 266(1):205–220, 2018.

[50] Enrico Zio. *Computational Methods for Reliability and Risk Analysis*, volume 14. World Scientific Publishing Company, 2009.

[51] Michele Compare, Enrico Zio, Emilio Moroni, Gianni E Portinari, and Tiziano Zanini. Development of a methodology for systematic analysis of risk reduction by protective measures in tyre production machinery. *Safety Science*, 110:13–28, 2018.

[52] Thomas D Nielsen and Finn V Jensen. *Bayesian Networks and Decision Graphs*. Springer Science & Business Media, 2009.

[53] Juuso Liesiö. Measurable multiattribute value functions for portfolio decision analysis. *Decision Analysis*, 11(1):1–20, 2014.

[54] Francesco Di Maio, Samuele Baronchelli, and Enrico Zio. Hierarchical differential evolution for minimal cut sets identification: Application to nuclear safety systems. *European Journal of Operational Research*, 238(2):645–652, 2014.

[55] Nir Kshetri. *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives*. Springer Science & Business Media, 2010.

[56] David E Whitehead, Kevin Owens, Dennis Gammel, and Jess Smith. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, pages 1–8. IEEE, 2017.

[57] Electric Power Research Institute. *Electric Sector Failure Scenarios and Impact Analyses*. National Electric Sector Cybersecurity Organization Resource (NESCOR), 2015.

[58] Arash Nourian and Stuart Madnick. A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet. *IEEE Transactions on Dependable and Secure Computing*, 15(1):2–13, 2018.

[59] Tunc Aldemir. A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. *Annals of Nuclear Energy*, 52:113–124, 2013.

[60] Nima Khakzad, Faisal Khan, and Paul Amyotte. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. *Process Safety and Environmental Protection*, 91(1-2):46–53, 2013.

[61] Enrico Zio and Michele Compare. Evaluating maintenance policies by quantitative modeling and analysis. *Reliability Engineering & System Safety*, 109:53–65, 2013.

[62] Ralph L Keeney and Howard Raiffa. *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. Cambridge University Press, 1993.

[63] Pekka Mild, Juuso Liesiö, and Ahti Salo. Selecting infrastructure maintenance projects with robust portfolio modeling. *Decision Support Systems*, 77:21–30, 2015.

[64] Margaret A Hahn, Richard N Palmer, Steve M Merrill, and Andrew B Lukas. Expert system for prioritizing the inspection of sewers: Knowledge base formulation and evaluation. *Journal of Water Resources Planning and Management*, 128(2):121–129, 2002.

[65] Tommaso Sacco, Michele Compare, Enrico Zio, and Giovanni Sansavini. Portfolio decision analysis for risk-based maintenance of gas networks. *Journal of Loss Prevention in the Process Industries*, 60:269–281, 2019.

[66] Heiner Lasi, Peter Fettke, Hans-Georg Kemper, Thomas Feld, and Michael Hoffmann. Industry 4.0. *Business and Information Systems Engineering*, 6(4):239–242, 2014.

[67] Enrico Zio. Some challenges and opportunities in reliability engineering. *IEEE Transactions on Reliability*, 65(4):1769–1782, 2016.

[68] Daeil Kwon, Melinda R Hodkiewicz, Jiajie Fan, Tadahiro Shibutani, and Michael G Pecht. IoT-based prognostics and systems health management for industrial applications. *IEEE Access*, 4:3659–3670, 2016.

[69] Ahti Salo, Juho Andelmin, and Fabricio Oliveira. Decision programming for multi-stage optimization under uncertainty. https://arxiv.org/pdf/1910.09196.pdf, 2019. [Online: accessed 21-February-2020].

[70] Milad Memarzadeh and Matteo Pozzi. Value of information in sequential decision making: Component inspection, permanent monitoring and system-level scheduling. *Reliability Engineering & System Safety*, 154:137–151, 2016.

[71] Edoardo Tosoni, Ahti Salo, Joan Govaerts, and Enrico Zio. Comprehensiveness of scenarios in the safety assessment of nuclear waste repositories. *Reliability Engineering & System Safety*, 188:561–573, 2019.

[72] Matthias M Herterich, Falk Uebernickel, and Walter Brenner. The impact of cyber-physical systems on industrial services in manufacturing. *Procedia CIRP*, 30:323–328, 2015.

[73] Marcello Colledani, Maria Chiara Magnanini, and Tullio Tolio. Impact of opportunistic maintenance on manufacturing system performance. *CIRP Annals*, 67(1):499–502, 2018.

[74] Aleyn Smith-Gillespie, Ana Muñoz, Doug Morwood, and Tiphaine Aries. Rolls-Royce: A Circular Economy Business Model Case. http://www.r2piproject.eu/wp-content/uploads/2018/08/Rolls-Royce-Case-Study.pdf, 2019. [Online: accessed 21-February-2020].

[75] Tyrrell Rockafellar and Stanislav Uryasev. Conditional Value-at-Risk for general loss distributions. *Journal of Banking & Finance*, 26(7):1443–1471, 2002.

[76] Alessandro Antonucci and Marco Zaffalon. Decision-theoretic specification of credal networks: A unified language for uncertain modeling with sets of Bayesian networks. *International Journal of Approximate Reasoning*, 49(2):345–361, 2008.

[77] Laura Uusitalo. Advantages and challenges of Bayesian networks in environmental modelling. *Ecological Modelling*, 203(3-4):312–318, 2007.

[78] Alex Jung. Machine Learning: Basic Principles. https://arxiv.org/abs/1805.05052, 2019. [Online: accessed 21-February-2020].

[79] Jaroslaw Sobieszczanski-Sobieski. Overcoming the Bellman's curse of dimensionality in large optimization problems. https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19900014075.pdf, 1990. [Online: accessed 21-February-2020].

[80] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[81] Mika Hirvensalo. *Quantum Computing*. Springer, 2013.

[82] David Rios Insua, Aitor Couce-Vieira, Jose A Rubio, Wolter Pieters, Katsiaryna Labunets, and Daniel G Rasines. An adversarial risk analysis framework for cybersecurity. *Risk Analysis*, In press, 2019.

[83] Wei Wang, Francesco Di Maio, and Enrico Zio. Adversarial risk analysis to allocate optimal defense resources for protecting cyber-physical systems from cyber attacks. *Risk Analysis*, 39(12):2766–2785, 2019.

[84] Viktoria Gisladottir, Alexander A Ganin, Jeffrey M Keisler, Jeremy Kepner, and Igor Linkov. Resilience of cyber systems with over- and underregulation. *Risk Analysis*, 37(9):1644–1651, 2017.

[85] Vilma Virasjoki, Paula Rocha, Afzal S Siddiqui, and Ahti Salo. Market impacts of energy storage in a transmission-constrained power system. *IEEE Transactions on Power Systems*, 31(5):4108–4117, 2015.

[86] Stuart Madnick. Preparing for the cyberattack that will knock out US power grids. https://hbr.org/2017/05/preparing-for-the-cyberattack-that-will-knock-out-u-s-power-grids, 2017. [Online: accessed 21-February-2020].

Publication I

Alessandro Mancuso, Michele Compare, Ahti Salo and Enrico Zio. Portfolio optimization of safety measures for reducing risks in nuclear systems. *Reliability Engineering and System Safety*, 167:20-29, November 2017.

Reliability Engineering and System Safety 167 (2017) 20–29

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Portfolio optimization of safety measures for reducing risks in nuclear systems

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

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

ARTICLE INFO

Keywords:
Bayesian Belief Networks
Portfolio optimization
Risk analysis
Safety barriers
Risk importance measures

ABSTRACT

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

1. Introduction

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

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

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

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

As pointed out also by Toppila and Salo [8], using FTs for risk analysis has some limitations. Indeed, in spite of the clear visual representation of the analysed combinations of events leading to system failure [11,12], they are not suitable for describing multi-state

* Corresponding author at: Department of Mathematics and Systems Analysis, Aalto University, Finland.
E-mail address: alessandro.mancuso@aalto.fi (A. Mancuso).

http://dx.doi.org/10.1016/j.ress.2017.05.005
Received 16 September 2016; Accepted 3 May 2017
Available online 9 May 2017
0951-8320/

Nomenclature

V	set of nodes
N	number of nodes
$V^L \subset V$	set of leaf nodes
$V^D \subset V$	set of dependent nodes
$V^T \subset V$	set of target nodes
$V^A \subseteq V$	set of nodes at which safety measures can be applied
E	set of arcs
V_-^i	set of predecessors of node $i \in V$
d^i	depth of node $i \in V$
$\mathbb{A}^i$	set of possible safety measures at node $i \in V^A$
$z_a^i \in \{0,1\}$	binary decision variable for indicating safety measure $a \in \mathbb{A}^i$
$\mathbf{X}^i$	random variable representing the uncertainty in the state of the event at node $i \in V$
$\mathbb{S}^i$	set of states of the event at node $i \in V$
$\mathbb{P}_{X^i}(s)$	probability of the event that node $i \in V^L$ is in state $s \in \mathbb{S}^i$
$\mathbb{P}_{X_a^i}(s)$	probability of the event that node $i \in V^L$ is in state $s \in \mathbb{S}^i$ given that the safety measure $a \in \mathbb{A}^i$ is applied
$\mathbb{Q}_{X^i}(s)$	total probability of the event that node $i \in V$ is in state $s \in \mathbb{S}^i$
$u^t(s)$	disutility function of state $s \in \mathbb{S}^t$ at node $t \in V$
$\mathbb{U}^t(s)$	expected disutility of state $s \in \mathbb{S}^t$ at node $t \in V$
$R_a(s)$	Risk Reduction Rate of safety measure $a \in \mathbb{A}^i$ in state $s \in \mathbb{S}^i$
c_a	cost of safety measure $a \in \mathbb{A}^i$
Λ	time periods
r	annualized discount rate

component behaviours (e.g., “No leakage”, “Minor leakage” and “Major leakage” for a component leakage failure, [13,14]).

In this paper, we propose a PRA-based decision support methodology to identify the optimal portfolio of safety measures that minimizes the residual system risk while accounting for feasibility and budget constraints. The methodology represents the combinations of events leading to system failure as BBNs [15,16], which overcome the limitations of FTs by offering the possibility of modelling multi-state events and extending the concepts of AND/OR gates.

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

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

2. Problem formulation

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

- Nodes $V = \{1, \dots, N\}$, shown as circles, represent the FT random events whose combinations can lead to system failure. More specifically, when the FT is converted into the BBN, some FT events can be merged to the same node; in general, there is no one-to-one correspondence between FT events and BBN nodes [17]. The target nodes for the risk analysis are indicated by the set $V^T \subset V$ and are shown as rounded squares. The set V^T includes the node associated with the top event of the FT [9], but it can contain other nodes which represent possible failures that deserve attention in risk analysis.
- Directed arcs $E \subseteq \{(i,j) | i,j \in V, i \neq j\}$ indicate conditional dependencies among nodes. Specifically, the arc $(j,i) \in E$ which connects node $j \in V$ to node $i \in V$ indicates that the event at node i is conditionally dependent on the event at node j.

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

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

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

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

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

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

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

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

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

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

$$z_k = \begin{cases} z_k^{i^*}, & i^* = \min\{j | j \in V^A\}, \ k = 1,2,\dots,|\mathbb{A}^{i^*}| \\ z_{k-q}^{j^*}, & k = |\mathbb{A}^{i^*}| + 1, \dots, \sum_{i \in V^A} |\mathbb{A}^i|, \end{cases} \quad (2)$$

where

$$j^* = \min \left\{ j \in V^A \middle| \sum_{i=1}^{j} |\mathbb{A}^i| \geq k \right\}, \quad (3)$$

$$q = \sum_{i=1}^{j^*-1} |\mathbb{A}^i|. \quad (4)$$

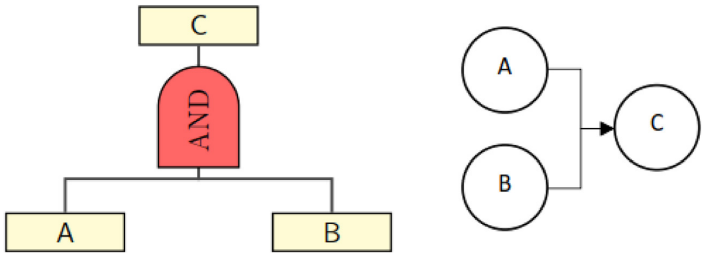


Fig. 1. Correspondence between FT (left) and BBN (right).

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

$\mathbb{P}_{X^C}$		C	$\overline{C}$	$\mathbb{P}_{X^C}$		C	$\overline{C}$
A	B	1	0	A	B	0.98	0.02
	$\overline{B}$	0	1		$\overline{B}$	0.03	0.97
$\overline{A}$	B	0	1	$\overline{A}$	B	0.03	0.97
	$\overline{B}$	0	1		$\overline{B}$	0.01	0.99

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

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

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

2.1. Characterization of conditional probability tables

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

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

Conditional probabilities can be derived from expert judgements and statistical analyses. When the conditional probability tables are elicited from experts, systematic approaches can be adopted to reduce the number of statements needed. For instance, the noisy-OR model [19,20] or the β-factor model [21,22] can be used for this purpose.

2.2. Optimization model

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

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

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

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

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

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

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

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

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

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

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

Let $\mathbb{S}^i_-$ be the set of the Cartesian product of all the sets of states $\mathbb{S}^j$, $j \in V^j_-$. Then, a possible realization of $\mathbf{X}^i_-$ is indicated by the vector $\mathbf{x}^i \in \mathbb{S}^i_-$, whose jth entry x^i_j represents the realization of the corresponding random variable $\mathbf{X}^j$, $j \in V^i_-$. Then, the conditional probability of state $s \in \mathbb{S}^i$ of the event at node $i \in V^D \cap V^A$, given $\mathbf{x}^i \in \mathbb{S}^i_-$, is

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

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

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

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

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

As mentioned in Section 1, the objective of the analysis is to evaluate the risk at the target nodes $t \in V^T$ for different impacts of the portfolio

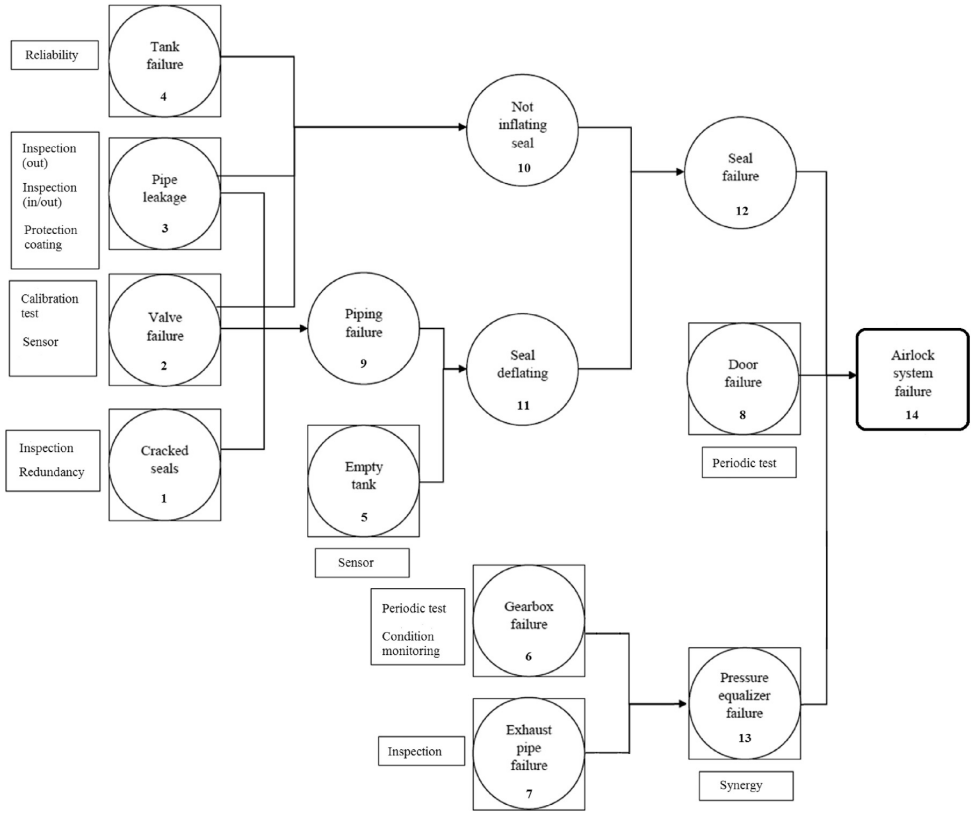


Fig. 2. BBN for the airlock system failure.

of safety measures. The risk at node $t \in V^T$ is not acceptable if the probability $\mathbb{P}_{X^t}(s)$ is greater than the accepted threshold for at least one state $s \in \{1, \dots, \mathbb{S}^t\}$. We assume that the larger the value of the realized state $\mathbf{X}^i = s$, the larger the magnitude of failure, then the smaller the probability threshold.

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

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

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

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

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

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

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

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

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

subject to the constraints

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.3. Optimization algorithm

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

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

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

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

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

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

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

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

3. CANDU NPP airlock system case study

We illustrate our methodology by revisiting the Design Basis Accident (DBA) that occurred in the airlock system of a CANDU NPP in 2011 [18,28]. The Airlock System (AS) is a safety system which keeps the pressure of the inner side of the reactor vault lower than the outer side. This pressure difference prevents the dispersion of contaminants from the reactor bay in case of failure. Specifically, the AS consists of a vessel in the containment wall of the reactor vault and its doors allow the operators to access the vault for inspection. One door opens towards the inside, the other towards the outside.

Table 2
Parameters of the safety measures.

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

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

The target node represents the event that the single door cannot be tightened so that the airlock system fails to maintain the pressure boundary (Appendix A.2, [18]). For simplicity, we do not replicate the same FT for the second door of the airlock system.

Possible causes for the occurrence of this target node are:

- Failure of the pressure equalizer system: This event is due to the combination of the gear box failure (which does not allow vents to open and close on-demand) and the failure to close the exhaust pipe (which prevents the equalizer from reaching the desired pressure level).
- Door failure: The door fails to close because the latches are not locked.
- Sealing system failure: This event can be caused by either (i) a failure in inflating the seals (which is due to a failure to open the valve controlling the inflation, a major pipe leakage spreading out the inflating air or a failure to engage the back-up tank) or (ii) continuous air deflating (which requires that (i) the back-up tank is already empty and can no longer compensate the air deflating and that (ii) there is a failure in the inflating air piping system). The piping failure can be caused by a crack in the seal, a pipe leakage or a valve failure.

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

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

Table 2 lists the safety measures $a_j^i, i \in V^A = \{1, 2, 3, 4, 5, 6, 7, 8, 13\}, j \in \{1, 2, \ldots, |\mathbb{A}^i|\}$ that can be applied to the events at

nodes $i \in V^A$ to mitigate the event at the target node $t = 14$. Although most safety measures apply to leaf nodes, our approach can accommodate situations in which safety measures are applied at nodes whose depth is $d^i > 1$.

Specifically, we consider the safety measure "Synergy" ($a_1^{13} \in \mathbb{A}^{13}$) applied to mitigate the event "Pressure equalizer failure" ($i = 13$) at the second level $d^{13} = 2$. This safety measure represents the combination of safety measures "Periodic test" ($a_1^6 \in \mathbb{A}^6$) and "Inspection plan" ($a_1^7 \in \mathbb{A}^7$), such that

$$\begin{aligned} 2z_{a_1^{13}} &\leq z_{a_1^6} + z_{a_1^7} \\ z_{a_1^{13}} &\geq z_{a_1^6} + z_{a_1^7} - 1. \end{aligned} \tag{24}$$

The synergy does not reduce risks, but saves costs by $c_1^{13} = -30$ k€ for joined inspections at the gearbox and the exhaust pipe. We define the cost of the safety measure $a_j^i \in \mathbb{A}^i$ as $c_j^i = c_{a_j^i}$ (fourth column in Table 2).

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

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

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

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

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

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

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

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

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

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

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

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

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

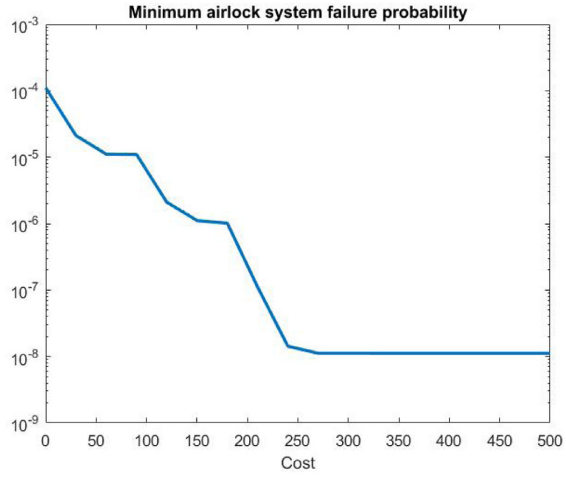


Fig. 3. Probability of airlock system failure.

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

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

From Fig. 3, we see that the minimum probability of airlock system failure remains practically the same for $B \geq 230$ k€ whereafter the risk reduction due to additional safety measures becomes negligible. As shown in Fig. 4, if the budget is at least 230 k€, the optimal portfolio already contains the inspection of the door, the joined actions on the valve and the reliability improvement of the tank. These events are directly linked to the target node by OR gates; thus, reducing their failure probabilities significantly reduces the probability of the airlock system failure. In contrast, the effects of other safety measures become negligible.

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

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

3.1. Comparison with a Risk Reduction Worth-based procedure

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

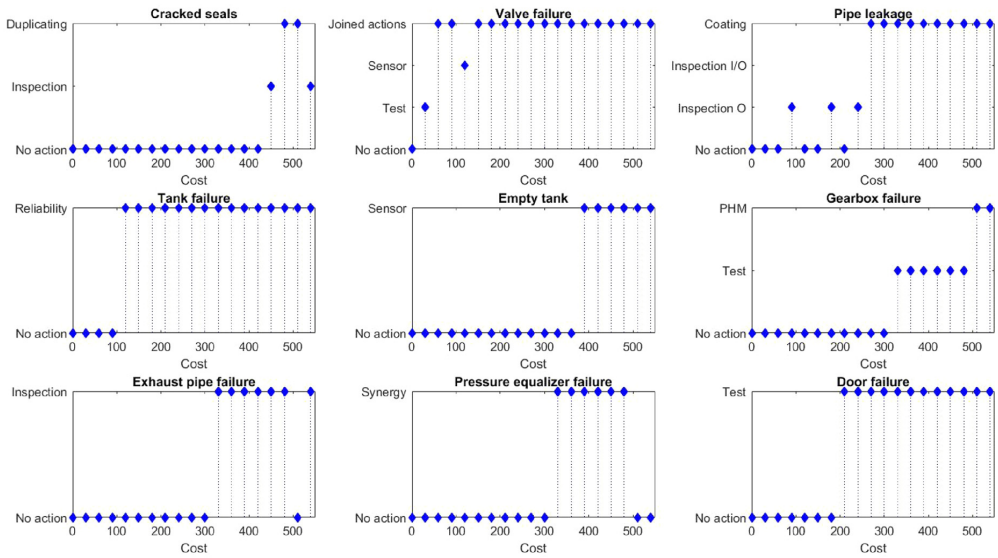


Fig. 4. Optimal safety measure per event.

in our framework. Thus, it is necessary to apply small changes to the example in Section 3.

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

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

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

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

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

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

We illustrate this approach by analysing the airlock system. At each iteration τ, we calculate the values of RRW for nodes $i \in V^A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ of which safety measures can be applied (Fig. 2). We do not consider the safety measure "Synergy" ($a_1^{13} \in \mathbb{A}^{13}$), because $R_{a_1^{13}}(1) = 1$, i.e. it does not have any additional impact on risk with respect to the two safety measures a_1^6 and a_1^7 that lead to this synergy.

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

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

At node "Valve failure" ($i = 2$), two possible safety measures can reduce the risk of the target node. If the safety measure "Sensor" ($a_2^2 \in \mathbb{A}^2$) is chosen to prevent "Valve failure", the RRW values at iteration $\tau = 2$ are

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

Continuing, after the safety measure "Sensor" to reduce the probability of "Valve failure" ($i = 2$) has been applied, the event "Tank failure" ($i = 4$) has the most potential for risk reduction. At this node, the only safety measure "Improving reliability" ($a_1^4 \in \mathbb{A}^4$) is also one of the most expensive, meaning that most of the available budget will be used, so that less expensive safety measures cannot be applied.

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

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

The events "Valve failure" ($i = 2$) and "Door failure" ($i = 8$) have the highest RRW values, in particular $RRW_3^2 = RRW_3^8$.

If the safety measure "Sensor" ($a_2^2 \in \mathbb{A}^2$) is applied to mitigate the event "Valve failure", the safety measure "Periodic test" ($a_1^8 \in \mathbb{A}^8$) is applied to prevent the event "Door failure". This way, at iteration $\tau = 4$, this approach would lead again to safety measures on the event "Valve failure" ($i = 2$), given that

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

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

$$R_{a_3^2}(1) \neq R_{a_1^2}(1) \cdot R_{a_2^2}(1) \tag{36}$$

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

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

4. Discussion

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

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

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

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

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

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

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

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

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

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

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

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

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

The PDA approach can be utilized in several ways for large systems. For instance, the experts can first employ RIMs to select computationally manageable portfolios consisting of the most risky components and then apply the PDA approach to make cost-effective decisions on the components within these pre-selected portfolios. The experts can also analyse portfolios consisting of similar or comparable components to generate guidelines as to what kinds of safety measures are most cost-efficient for these components. Furthermore, complex PSA models are typically hierarchically structured and can be decomposed into several indenture levels. Then, the PDA approach can be used iteratively to first select the optimal portfolios of systems at the highest indenture levels and to determine corresponding risk reduction rates and costs. These solutions can be converted into requirements for the portfolio selection at the following lower indenture levels. Future research will focus on the computational and modelling issues arising from the application of the PDA approach to large-scale complex systems.

5. Conclusion and future research

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

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

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

Acknowledgement

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

A1. Algorithm for selecting the optimal portfolio of safety measures

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

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

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

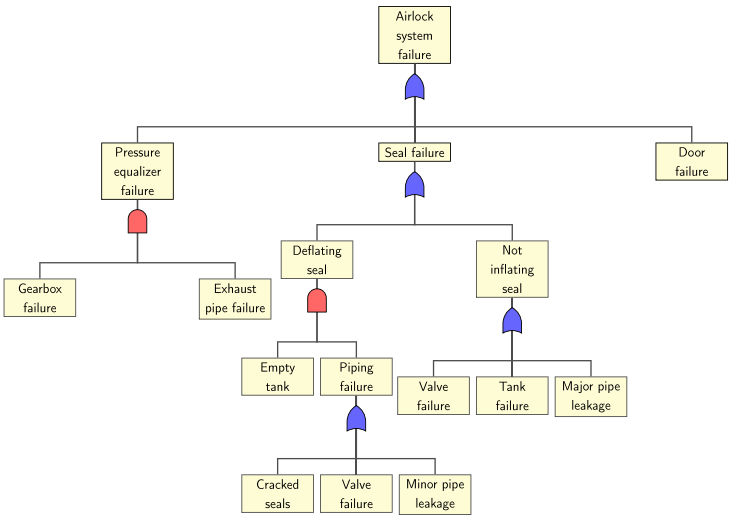
where $\leq$ holds component-wise.

In addition to the constraints which ensure the uniqueness of the safety measure at each node in (15), the set Z_F accounts for feasibility and budget constraints in (16).

Algorithm 1: The implicit enumeration algorithm.

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

A2. Airlock system Fault Tree



References

[1] Aven T, Baraldi P, Flage R, Zio E. Uncertainty in risk assessment: the representation and treatment of uncertainties by probabilistic and non-probabilistic methods. New York: John Wiley & Sons; 2014.

[2] Kuo W, Zhu X. Importance measures in reliability, risk and optimization: principles and applications. New York: John Wiley & Sons; 2012.

[3] Zio E. Computational methods for reliability and risk analysis. Singapore: World Scientific Publishing; 2011.

[4] Cheok MC, Parry GW, Sherry RR. Use of importance measures in risk-informed regulatory applications. Reliab Eng Syst Safety 1998;60:213–26.

[5] Zio E, Podofillini L. Importance measures and genetic algorithms for designing a risk-informed optimally balanced system. Reliab Eng Syst Safety 2007;92:1435–47.

[6] Vesely WE. Principles of resource-effectiveness and regulatory-effectiveness for risk-informed applications: reducing burdens by improving effectiveness. Reliab Eng Syst Safety 1999;63:283–92.

[7] Salo A, Keisler J, Morton A. Portfolio decision analysis improved methods for resource allocation. International Series in Operations Research & Management Science. vol. 162, Springer-Verlag, 2011.

[8] Toppila A, Salo A. Selection of risk reduction portfolios under interval-valued probabilities. Reliab Eng Syst Safety 2017;163:69–78.

[9] Zio E. An introduction to the basics of reliability and risk analysis. Singapore: World Scientific Publishing; 2007.

[10] Prasad VR, Kuo W. Reliability optimization of coherent systems. IEEE Trans Reliab 2000;49:323–30.

[11] Couronneau JC, Tripathi A. Implementation of the new approach of risk analysis in france. In: Proceedings of the 41st International Petroleum Conference, Bratislava, Slovakia; 2003.

[12] Markowski AS, Kotynia A. "bow-tie" model in layer of protection analysis. Process Safety Environ Prot 2011;89:205–13.

[13] Baraldi P, Compare M, Despujols A, Lair W, Zio E. A practical analysis of the degradation of a nuclear component with field data. In: Safety, Reliability and Risk Analysis: Beyond the Horizon - Proceedings of the European Safety and Reliability Conference, ESREL 2013; 2014. p. 1009–14.

[14] Veeramany A, Pandey MD. Reliability analysis of nuclear piping system using semi–markov process model. Ann Nucl Energy 2011;38:1133–9.

[15] Jensen F. Bayesian networks and decision graphs. New York: Springer-Verlag; 2001.

[16] Weber P, Median-Oliva G, Iung B. Overview on bayesian networks application for dependability, risk analysis and maintenance areas. Eng Appl Artif Intell 2012;25:671–82.

[17] Khakzad N, Khan F, Amyotte P. Dynamic safety analysis of process systems by mapping bow-tie into bayesian network. Process Safety Environmental Prot 2013;91:46–53.

[18] Di Maio F, Baronchelli S, Zio E. Hierarchical differential evolution for minimal cut sets identification: application to nuclear safety systems. Eur J Oper Res 2014;238:645–52.

[19] Käki A, Salo A, Talluri S. Disruptions in supply networks: a proababilistic risk assessment approach. J Bus Logist 2015;36:273–87.

[20] Pearl J. Probabilistic reasoning in intelligent systems: networks of plausible inference. San Mateo: Morgan Kaufmann Publishers; 1988.

[21] Fleming KN. A reliability model for common mode failures in redundant safety systems. In: Proceedings of the Sixth Annual Pittsburgh Conference On Modeling and Simulations, Instrument Society of America, Pittsburgh; 1975.

[22] Modarres M. Risk analysis in engineering: techniques, tools and trends. Boca Raton: CRC Press; 2006.

[23] Edwards W. How to use multiattribute utility measurement for social decision making. IEEE Trans Syst Man Cybern 1977;7:326–40.

[24] Von Winterfeldt D, Edwards W. Decision analysis and behavioural research. Cambridge: UK: Cambridge University Press; 1986.

[25] Edwards W, Barron FH. SMARTS and SMARTER: improved simple methods for multiattribute utility measurement. Org Behav Hum. Decis Processes 1994;60:306–25.

[26] Liesiö J. Measurable multiattribute value functions for portfolio decision analysis. Decis Anal 2014;11:1–20.

[27] Liesiö J, Mild P, Salo A. Robust portfolio modeling with incomplete cost information and project interdependencies. Eur J Oper Res 2008;190:679–95.

[28] Lee A, Lu L. Petri net modeling for probabilistic safety assessment and its application in the air lock system of a CANDU nuclear power plant. Procedia engineering, 2012 international symposium on safety science and technology 2012;vol. 25:11–20.

[29] Luenberger DG. Investment science. Oxford: Oxford University Press; 1997.

[30] Lennon T, Moore D. The natural fire safety concept - full scale tests at cardington. Fire Safety J 2003;38:623–43.

[31] Zio E. Integrated deterministic and probabilistic safety analysis: concepts, challenges, research directions. Nucl Eng Des 2014;280:413–19.

Publication II

Alessandro Mancuso, Piotr Żebrowski and Aitor Couce Vieira. Risk-based selection of mitigation strategies for cybersecurity of electric power systems. *Manuscript*, 25 pages, May 2019.

Risk-based selection of mitigation strategies for cybersecurity of electric power systems

A. Mancuso [*1,2], P. Żebrowski[3] and A. Couce-Vieira[4]

[1]Department of Mathematics and Systems Analysis, Aalto University, Finland

[2]Department of Energy Engineering, Politecnico di Milano, Italy

[3]International Institute for Applied Systems Analysis (IIASA), Austria

[4]Instituto de Ciencias Matematicas, Consejo Superior de Investigaciones Cientficas, Madrid, Spain

Abstract

Electric power systems extensively rely on cyber physical systems to control physical components through cyber-based commands. Thus, the vulnerability to cyber threats requires an efficient allocation of resources to mitigate the risk of attacks. Common practices guide the selection of mitigation actions by prioritizing the cyber threat scenarios through a qualitative assessment. These practices can result in sub-optimal allocations of resources to protect the system. To overcome these drawbacks, we quantify the risk of cyber threats to the system through a comprehensive analysis of the system vulnerabilities. This analysis relies on Bayesian networks, which provide a solid framework for probabilistic risk assessment by representing cyber threat scenarios as combinations of cascading events. In addition, we develop an optimization model to determine the non-dominated mitigation strategies to protect the system from cyber threats. Specifically, the minimization of the risk of cyber threats supports the selection of mitigation actions, considering budget and technical constraints. The optimization model provides additional insight into risk management at different budget levels.

Keywords: Cyber Physical Systems, Cybersecurity, Electric Power Grids, Risk Management, Multi-Objective Optimization.

*Corresponding author. Tel.: +358 504084419. E-mail address: alessandro.mancuso@aalto.fi (A. Mancuso)

1 Introduction

Cyber physical systems are physical systems in which operations are integrated, monitored and controlled through multi-core processors [1]. Such systems are increasingly employed in a wide range of industries, including electric power industry. Despite the substantial benefits to our society, the rapid proliferation of cyber physical systems also provides potential attackers with new opportunities to disrupt critical infrastructures [2].

Costly impacts can result from such attacks, for instance a cyber attack in 2015 caused the power outage of 225000 customers in Ukraine that lasted up to six hours. In that occasion, the operators at the three operations centers were unable to regain remote control of more than 50 substations affected by the incident. After the loss of over 130MW of load, the operators restored power by sending technicians to the substations and manually controlling the power system [3]. Besides critical infrastructures, cyber threats may affect all kind of institutions with potentially severe and costly impacts worldwide. For instance, the Petya and WannaCry cyber-attacks hit thousands of companies across the globe in 2017 [4]. Other relevant cases include the Stuxnet attack in 2010 to target an uranium enrichment centrifuge in Iran [5] and the attack on a German steel mill in 2014 to take over the plant control systems [6]. In recent years, cyber attacks have increased dramatically in terms of quantity, diversity and sophistication with significant economic losses [7].

These episodes prove the need for an effective deployment of security measures to mitigate the risk of cyber threats. Poolsappasit et al. [8] develop a mitigation strategy based on the likelihood of cyber attacks. A genetic algorithm supports the selection of a subset of mitigation actions by minimizing the cost of deployment and the expected damage to the system. Shameli-Sendi et al. [9] propose a dynamic framework for selecting optimal countermeasures to mitigate attacks. The selection is based on minimizing the cost of deployment and the impact on users and services. However, these optimization models do not consider the multiple impacts deriving from the cyber threat scenarios. Instead, mitigation strategies are selected on the cost and performance of individual actions. The resulting resource allocation could be sub-optimal for the cyber physical systems due to the lack of modeling the multiple impacts of cyber attacks [10]. Thus, the efficient allocation of resources to secure cyber physical systems involves challenges that we address in this paper.

Specifically, this paper fits into the first two functions of the National Institute of Standards and Technology (NIST) cybersecurity framework [11] in *detecting* system vulnerabilities and *protecting* the system from cybersecurity incidents. The NIST cybersecurity framework sets broadly accepted guidelines to improve the security of cyber physical systems. In this framework, we propose a methodology for the risk assessment of cyber threats based on a comprehensive analysis of the system vulnerabilities. This

methodology relies on Bayesian networks that model a probabilistic representation of combinations of events, possibly leading to severe outcomes. This model responds to the need for intuitive and computationally efficient methods for risk analysis, combining expert judgment and statistical analyses for the quantitative assessment of risks [12].

The proposed methodology leads to select the optimal portfolios of mitigation actions, based on the minimization of the risk of multiple impacts of cyber attacks. In particular, this paper focuses on mitigation strategies for protecting electric power systems, yet the framework has broader applications on cyber physical systems. Recently, the Electric Power Research Institute (EPRI) analyzed the cybersecurity failure scenarios and impacts for the electric sector [13]. The report provides insights on cybersecurity risks and potential mitigation actions to support risk assessment and resource allocation. Among applications on electric power systems, Ciapessoni et al. [14] propose a methodology to assess the security of such systems by analyzing the vulnerabilities to natural and human threats. On the other hand, Shelar and Amin [15] formulate a game theoretic framework to assess the security of an electricity distribution network, based on which the defender optimizes the security strategy of the network nodes.

In this paper, Section 2 reviews the practice proposed by the EPRI to select appropriate mitigation actions for the electric power system. Specifically, we present a critical analysis of the ranking procedure of individual cyber threats, which could lead to inefficient or unfeasible allocations for the system. This problem is addressed in Section 3, which provides an alternative to the EPRI practice by evaluating portfolios of mitigation actions to protect the cyber physical system against multiple cyber threat scenarios. In addition, an optimization model supports the selection of the mitigation strategies that minimize the expected impacts of cyber attacks, based on financial and technical constraints. Section 4 illustrates the methodology by analyzing the cyber threat scenarios concerning the Advanced Metering Infrastructure (AMI) of an electric power system. Section 5 discusses the potential and limits of the proposed framework, suggesting possible ways to overcome some inconveniences. Finally, Section 6 concludes the paper and outlines extensions for future research.

2 Analysis of the EPRI practice

Cybersecurity management calls for an extensive analysis of the system vulnerabilities, which leads to an efficient allocation of resources to protect the electric power system. In particular, the EPRI proposes the analysis of individual cyber threat scenarios based on attack graphs, multi-leveled diagrams describing threats on cyber physical systems and possible attacks to realize such threats [16]. Attack graphs are increasingly being applied to computer control systems, especially related to electric power systems, but they have also been used to analyze threats to physical systems [17]. Figure 1 illustrates the graphical

notation of two attack graphs, where a cyber threat scenario is represented through sequences of events (shown as diamonds) leading to the possible impacts of the cyber attack (shown as ellipses). The impacts of the cyber attack occur if a combination of events of the cyber threat scenario has proven to be successful, based on the binary representation of AND and OR gates (shown as solid and dashed lines, respectively).

Attack graphs represents cyber threat scenarios, which are evaluated based on the *likelihood* of occurrence and *impact*. According to the EPRI analyses, the likelihood depends on 5 criteria whereas the impact depends on 15 criteria which are reported in Tables 3 and 4, respectively. These tables also report the EPRI scoring system for quantifying the likelihood and impact of cyber threat scenarios. Each score is an integer value in the range $0-9$, thus the likelihood and impact are computed by summing the scores over the respective criteria. However, this scoring system can be questioned on the meaningfulness of the $0-9$ scale. For instance, is a public accessible asset three times more accessible than a fenced asset with standard locks and nine times more accessible than a guarded/monitored asset? Furthermore, the additive model can be questioned on the sum of scores across different criteria. For instance, is "Public safety concern" comparable to "Long term economic damage"?

Mapping the likelihood and impact of all cyber threat scenarios in a risk matrix [18] makes it possible to rank the priority of individual cyber threats. This procedure clusters each cyber threat into *High*, *Medium* or *Low* likelihood and *High*, *Medium* or *Low* impact in order to prioritize the selection of mitigation actions. Specifically, cyber threats with *High* likelihood and *High* impact deserve the highest priority in the choice of mitigation actions, whereas priority decreases for cyber threats with lower likelihood and/or impact until the budget is depleted.

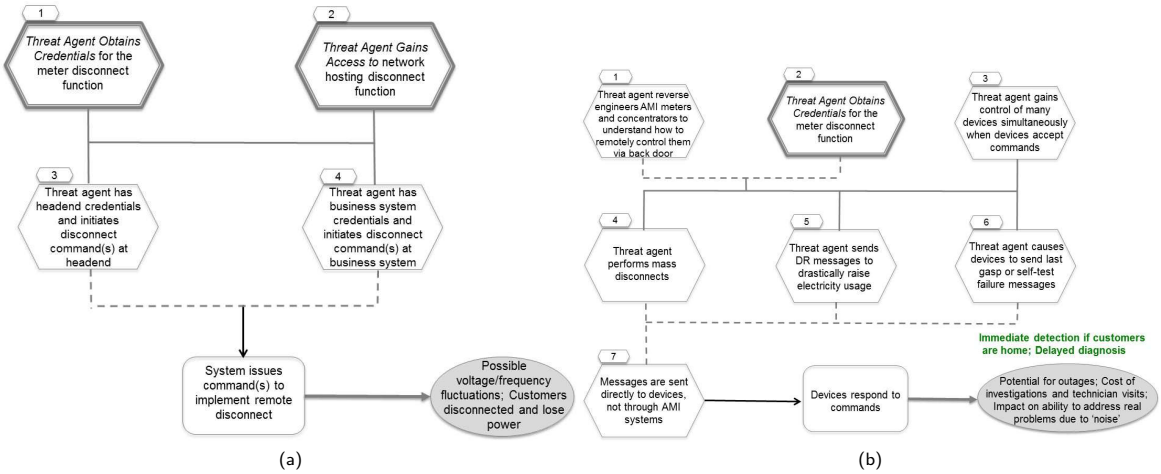


Figure 1: Attack graphs for (a) "Invalid disconnect messages to meters impact customers and utility" and (b) "Reverse engineering of AMI equipment allows unauthorized mass control" [13].

Despite the intuitive appeal and simplicity, risk matrices do not necessarily recommend effective risk management decisions, instead they may lead to incorrect risk prioritization [19,20]. Thus, the sequential choices of mitigation actions may result in a sub-optimal resource allocation because they are based on an incorrect prioritization of cyber threats [21]. Furthermore, this procedure does not consider technical and budget constraints across different scenarios. In conclusion, the EPRI practice presents several inconsistencies in assessing the risk of cyber threats and supporting the selection of mitigation actions.

3 Bayesian framework

We propose a Bayesian framework, which provides an alternative to the EPRI practice for the risk assessment of cyber threats and the risk-based selection of mitigation strategies. In particular, the proposed risk assessment is based on a comprehensive analysis of multiple cyber threats that can affect the cyber physical system [22]. The framework also includes an optimization model for determining non-dominated mitigation strategies in order to protect the system from cyber threats. Specifically, an optimization algorithm computes the portfolios of mitigation actions that minimize the expected impacts of cyber attacks, considering budget and technical constraints.

3.1 From attack graphs to Bayesian network

In contrast to the EPRI analysis of individual cyber threat scenarios, the Bayesian framework relies on a comprehensive analysis of multiple attack graphs [23]. Each attack graph represents a single cyber threat scenario, however some events could be equivalent among different attack graphs. For instance, in Figures 1a and 1b the event "Threat agent obtains credentials for the meter disconnect function" is equivalent among both attack graphs. For this reason, multiple attack graphs can be integrated into a directed acyclic graph by combining the corresponding events into single nodes. This integration leads to a comprehensive representation of cyber threat scenarios that overviews the alternative opportunities to attack the system [24].

This directed acyclic graph can be converted into a Bayesian network [25], a probabilistic graphical model that consists of:

- *chance nodes* (shown as circles) representing the random events of cyber threat scenarios;
- *value nodes* (shown as diamonds) representing the possible impacts of the cyber attacks;
- *arcs* (shown as directed edges) indicating causal dependencies between nodes.

Specifically, chance nodes are connected by arcs to represent combinations of events leading to the respective final impacts [26]. In this framework, the combinations of events indicate the stages of cyber

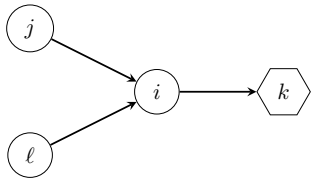


Figure 2: Example of a Bayesian network.

threat scenarios, whereas the final impacts indicate the possible outcomes of the cyber attacks. Arcs connects the nodes to represent the causal dependencies between the events of the attack graph. Figure 2 illustrates a Bayesian network, where each chance node represents a random event that encodes a finite set of discrete states, including a state of *No occurrence* of the event. Bayesian networks typically consider discrete states, nevertheless it is possible to include continuous variables under specific conditions [25].

Statistical analyses and expert judgment provide information to define the probability distributions of events that do not depend on any other chance node (nodes j and ℓ in Figure 2). For events that show causal dependencies on other chance nodes through directed arcs (node i in Figure 2), the probabilistic representation is based on the state of the events they are depending on. Thus, it is necessary to define conditional probability tables for such nodes. Following the binary representation of attack graphs, conditional probability tables are derived from the information provided by AND and OR gates. Specifically, if the event i depends on the events j and ℓ through AND(OR) gates, then the occurrence probability of the event i is 1 if the events j and(or) ℓ occur as well, and 0 otherwise. For illustrative purposes, we consider the event "Threat agent performs mass disconnects" in Figure 1b as an example throughout the paper. Table 1 displays the conditional probability table of the event, based on the binary representation of *Occurrence* and *No occurrence* of the dependent events. The conditional probability table is derived from the information provided by AND and OR gates of the attack graph in Figure 1b.

Bayesian networks represent the events such that the occurrence probability is not necessarily limited to 0 and 1, but it is a real value in the set $[0, 1]$. This model leads to a more realistic representation of the stages of cyber threat scenarios, in contrast to the binary representation. Table 2 displays the conditional probability table of the event "Threat agent performs mass disconnects", based on the multiple states of the events. This conditional probability table is not meant to represent any actual electric power system. According to the EPRI analyses, the occurrence probability of each event depends on (i) skill required, (ii) physical accessibility, (iii) logical accessibility and (iv) attack vector. In particular, the occurrence probability increases by enhancing the accessibility to equipment and information, while it decreases by requiring specialized knowledge and technical means to pursue the cyber threat.

The cascading events of the cyber threat scenarios finally lead to the possible impacts, assessed according to a set of criteria represented by the set K of value nodes [27]. The EPRI lists 14 possible

Table 1: Conditional Probability Table Based on Binary States.

			Threat agent performs mass disconnects	
Threat agent reverse engineers AMI equipment	Threat agent obtains credentials	Threat agent gains control of devices	*Occurrence*	*No occurrence*
Occurrence	*Occurrence*	*Occurrence*	1	0
		No occurrence	0	1
	No occurrence	*Occurrence*	1	0
		No occurrence	0	1
No occurrence	*Occurrence*	*Occurrence*	1	0
		No occurrence	0	1
	No occurrence	*Occurrence*	0	1
		No occurrence	0	1

Table 2: Conditional Probability Table Based on Multiple States.

			Threat agent performs mass disconnects [MW]			
Threat agent reverse engineers AMI equipment	Threat agent obtains credentials	Threat agent gains control of devices	*No occurrence*	(0 50]	(50 100]	> 100
Occurrence	*Occurrence*	*None*	1	0	0	0
		Few	0.6	0.4	0	0
		Moderate	0.4	0.2	0.4	0
		High	0.3	0.1	0.2	0.4
	No occurrence	*None*	1	0	0	0
		Few	0.6	0.4	0	0
		Moderate	0.4	0.2	0.4	0
		High	0.3	0.1	0.2	0.4
No occurrence	*Occurrence*	*None*	1	0	0	0
		Few	0.6	0.4	0	0
		Moderate	0.4	0.2	0.4	0
		High	0.3	0.1	0.2	0.4
	No occurrence	*None*	1	0	0	0
		Few	1	0	0	0
		Moderate	1	0	0	0
		High	1	0	0	0

impact criteria of cyber attacks on electric power systems, including financial, safety and service impacts. As a result, each value node of the Bayesian network represents a single impact criterion k, whose score depends on the state of events leading to that specific outcome. Ideally, the scores should be evaluated by a specific scale that reflects its unit of measure.

3.2 Probabilistic risk assessment

The probabilistic risk assessment of cyber threats is based on the computation of the expected impact for every impact criteria. Each chance node i represents a random event that encodes a finite set $\mathbb{S}_i$ of discrete states, including a state of *No occurrence* of the event. In particular, the occurrence probability of events that show causal dependencies relies on the occurrence probability of the events they depend on. For this reason, we define Δ_i as the set of all possible combinations of states of the chance nodes

affecting the event i, such that

$$\Delta_i = \prod_{j|(j,i)\in E} \mathbb{S}_j, \tag{1}$$

where E denotes the set of all arcs.

Let the random variable X_i represent the probability distribution of event i over the states $s_i \in \mathbb{S}_i$. Then, $\hat{\mathbf{X}}_i$ is a vector of random events on which X_i directly depends, meaning the vector of random variables X_j for all nodes j such that $(j,i) \in E$. For the d-separation property of Bayesian networks [25], the probability that the events affecting the event i meets a specific combination of states $\delta_i \in \Delta_i$ is

$$\mathbb{P}[\hat{\mathbf{X}}_i = \delta_i] = \prod_{s_j \in \delta_i} \mathbb{P}[X_j = s_j] \quad \forall \delta_i \in \Delta_i. \tag{2}$$

Thus, the occurrence probability of the event i is computed by the *law of total probability* as the weighted average of the posterior probabilities across all $\delta_i \in \Delta_i$, such that

$$\mathbb{P}[X_i = s_i] = \sum_{\delta_i \in \Delta_i} \mathbb{P}[X_i = s_i | \hat{\mathbf{X}}_i = \delta_i] \, \mathbb{P}[\hat{\mathbf{X}}_i = \delta_i]. \tag{3}$$

Because the occurrence probabilities are computed recursively, it is necessary to start the computation from the initial events throughout the dependent events of the cyber threat scenarios. The risk of cyber threats is then evaluated as the expected impact of the scenarios for each criterion $k \in K$, such that

$$\mathbb{E}[V_k] = \sum_{\delta_k \in \Delta_k} \mathbb{P}[\hat{\mathbf{X}}_k = \delta_k] \, V_k[\hat{\mathbf{X}}_k = \delta_k], \tag{4}$$

where $V_k[\hat{\mathbf{X}}_k = \delta_k]$ is the score of the impact criterion k depending on the combination of states δ_k of the events leading to that specific impact.

The expected impacts can be significantly reduced by deploying mitigation actions on the cyber physical system. Specifically, the mitigation actions affect the occurrence probability of one or multiple events in the cyber threat scenarios. In Bayesian networks, decision nodes (shown as squares) represent the choice of mitigation actions, as illustrated in Figure 3. Each arc directed from a decision node to

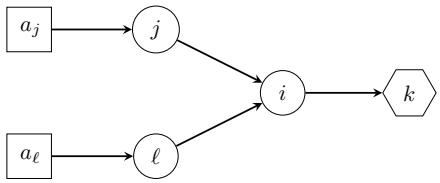


Figure 3: Example of a Bayesian network with decision nodes.

a chance node indicates that the deployment of the mitigation action affects the occurrence probability of the event represented by the chance node. Because this paper focuses on system design, the decision nodes do not depend on any event (no incoming arcs). Future research will focus on system control with decision nodes depending on other events.

Mitigation actions are numbered $a \in \{1, 2, ..., N\}$, such that the binary variable z_a indicates the deployment of the mitigation action a. Specifically, the binary variable is $z_a = 1$ for the deployment of the mitigation action a and $z_a = 0$ otherwise. Thus, a portfolio is defined by the binary vector $\mathbf{z}$ as a combination of binary variables z_a for all the possible mitigation actions. With no loss of generality, the vector $\mathbf{z}$ lists binary variables such that

$$\mathbf{z} = [z_1,\, z_2,\, ...\,,\, z_N]. \tag{5}$$

The deployment of mitigation actions reduces the occurrence probabilities of affected events. Bayesian networks compute probability updates of the cascading events throughout the cyber threat scenarios by the *law of total probability*, such that

$$\mathbb{P}[X_i = s_i|\mathbf{z}] = \sum_{\delta_i \in \Delta_i} \mathbb{P}[X_i = s_i|\hat{\mathbf{X}}_i = \delta_i]\ \mathbb{P}[\hat{\mathbf{X}}_i = \delta_i|\mathbf{z}]. \tag{6}$$

Thus, the risk of cyber threats depends on the portfolio $\mathbf{z}$ so that the expected impact of each criterion $k \in K$ is

$$\mathbb{E}[V_k](\mathbf{z}) = \sum_{\delta_k \in \Delta_k} \mathbb{P}[\hat{\mathbf{X}}_k = \delta_k|\mathbf{z}]\ V_k[\hat{\mathbf{X}}_k = \delta_k]. \tag{7}$$

This framework aims to compute the risk of cyber threats for each impact criterion, making it possible to select mitigation strategies based on the minimization of the expected impacts.

3.3 Optimization model

The risk-based selection of mitigation strategies is performed through a multi-objective optimization model. Unlike the EPRI practice, the selection of mitigation actions is not based on the additive model of scores across different impact criteria. Instead, our optimization model determines the portfolios of mitigation actions that minimize the risk of cyber threats for every impact criteria. The selection is based on the analysis of expected impacts derived from the deployment of different mitigation strategies, so that the optimization model determines the portfolios that fulfill the Pareto condition

$$\mathbf{z}^* \succ \mathbf{z} \Longleftrightarrow \begin{cases} \mathbb{E}[V_k](\mathbf{z}^*) \leq \mathbb{E}[V_k](\mathbf{z}) & \text{for all } k \\ \mathbb{E}[V_k](\mathbf{z}^*) < \mathbb{E}[V_k](\mathbf{z}) & \text{for some } k \end{cases}. \tag{8}$$

This condition states that portfolio $\mathbf{z}^*$ dominates $\mathbf{z}$ if it reduces the risk of cyber threats for any impact criterion without increasing the risk for other impact criteria.

In addition to the Pareto condition, the optimal mitigation strategies need to fulfill budget and technical constraints. Budget constraints specify the financial feasibility of the deployment of a mitigation strategy. Each mitigation action a is associated to a cost c_a, thus the overall cost of portfolio $\mathbf{z}$ must not exceed the budget B such that

$$\sum_a z_a \, c_a \leq B. \tag{9}$$

Technical constraints specify the properties of the system, such as mutually exclusive or mutually inclusive conditions of mitigation actions. For instance in Figure 3, the linear constraints

$$z_{a_j} + z_{a_\ell} \leq 1 \tag{10}$$

$$z_{a_j} - z_{a_\ell} = 0 \tag{11}$$

indicate that mitigation actions a_j and a_ℓ cannot be deployed together or they must be deployed together, respectively.

Technical constraints also include risk acceptability limits that are represented by non-linear inequalities. In particular, specific regulatory conditions may apply to some events of the cyber threat scenarios. For such event i, the subset $\tilde{\mathbb{S}}_i \subset \mathbb{S}_i$ includes the critical states whose occurrence probability must not exceed a risk acceptability threshold ϵ_i, such that

$$\sum_{s_i \in \tilde{\mathbb{S}}^i} \mathbb{P}[X_i = s_i | \mathbf{z}] \leq \epsilon_i. \tag{12}$$

Risk acceptability thresholds are usually provided by regulatory offices or internal company policies.

Feasible portfolios belong to the set $\mathbf{Z}_F$, which includes all binary vector $\mathbf{z}$ that fulfill linear and non-linear constraints. Then, the set of non-dominated solutions consists of the feasible portfolios that fulfill the Pareto condition for any other feasible portfolio, meaning that

$$\mathbf{Z}_{ND} = \{\mathbf{z}^* \in \mathbf{Z}_F | \nexists \, \mathbf{z} \in Z_F \text{ such that } \mathbf{z} \succ \mathbf{z}^*\}. \tag{13}$$

Generally, the set of non-dominated portfolios can include multiple alternative solutions, so the selection of a single mitigation strategy is not straightforward. For this reason, it is necessary to support the selection of the optimal mitigation strategy through additional analyses. A possible approach is the

computation of the *core index* of each mitigation action. Analogously to Liesiö et al. [28], the core index $CI(a)$ is defined as the fraction of non-dominated portfolios that include the mitigation action a, such that

$$CI(a) = \frac{|\{\mathbf{z}^* \in \mathbf{Z}_{ND} | z_a = 1\}|}{|\mathbf{Z}_{ND}|}. \tag{14}$$

The analysis of the core indexes helps determine the mitigation actions that should be selected or rejected. If the core index of a mitigation action is 1, that measure is included in all non-dominated portfolios; on the other hand, if the core index is 0, that measure is not included in any non-dominated portfolio. Finally, mitigation actions whose core index is in the range $(0, 1)$ require further analyses in order to be selected or rejected.

An implicit enumeration algorithm computes the set of non-dominated portfolios that minimize the risk of cyber threats over the impact criteria. The algorithm is an adaptation of Liesiö [29] and has been proposed by Mancuso et al. [30] for multi-objective optimization. This optimization algorithm is computationally efficient but it may be time consuming for a large amount of mitigation actions (over 40). In this case, evolutionary algorithms are a possible alternative to approximate non-dominated solutions for a lower computational time [31].

4 Case study

We illustrate the potential of the Bayesian framework by optimizing the selection of mitigation strategies for the Advanced Metering Infrastructure (AMI) of an electric power system. AMI systems have raised many security concerns since they connect traditionally self-contained power system operations with unreliable customer sites that are widely dispersed. The deployment of AMI systems is introducing millions of components to the electric grid that support two-way communication for next-generation grid applications. Although these systems can increase operational efficiency and enable new capabilities such as demand-response, they also increase the attack opportunity for potential adversaries. For this reason, electric power companies must address these new cybersecurity risks as part of their risk management strategy.

Information about AMI systems is provided by the National Electric Sector Cybersecurity Organization Resource (NESCOR), a program funded by the U.S. Department of Energy to protect electric power systems from cybersecurity incidents, both malicious and non-malicious. The NESCOR document "Electric Sector Failure Scenarios and Impact Analyses" [16] provides short descriptions of approximately 125 cyber threat scenarios in seven domains of the electric sector: *Advanced Metering Infrastructure*, *Distributed Energy Resources*, *Wide Area Monitoring, Protection and Control*, *Electric Transportation*,

Demand Response and *Distribution Grid Management*. Furthermore, the NESCOR document "Analysis of Selected Electric Sector High Risk Failure Scenarios" [13] presents the analyses of a selection of these cyber threat scenarios. Specifically, each analysis includes an attack graph that details the logical dependencies of events leading to a successful cyber attack. In addition to the attack graph, several of the analyses also provide a detailed description of each scenario.

Based on the NESCOR analyses, we select 8 cyber threats with the highest priority for AMI systems, in particular: invalid disconnect messages to meters impact customers and utility; reverse engineering of AMI equipment allows unauthorized mass control; threat agent obtains credentials for system or function; threat agent uses social engineering; threat agent gains access to network; threat agent exfiltrates data;

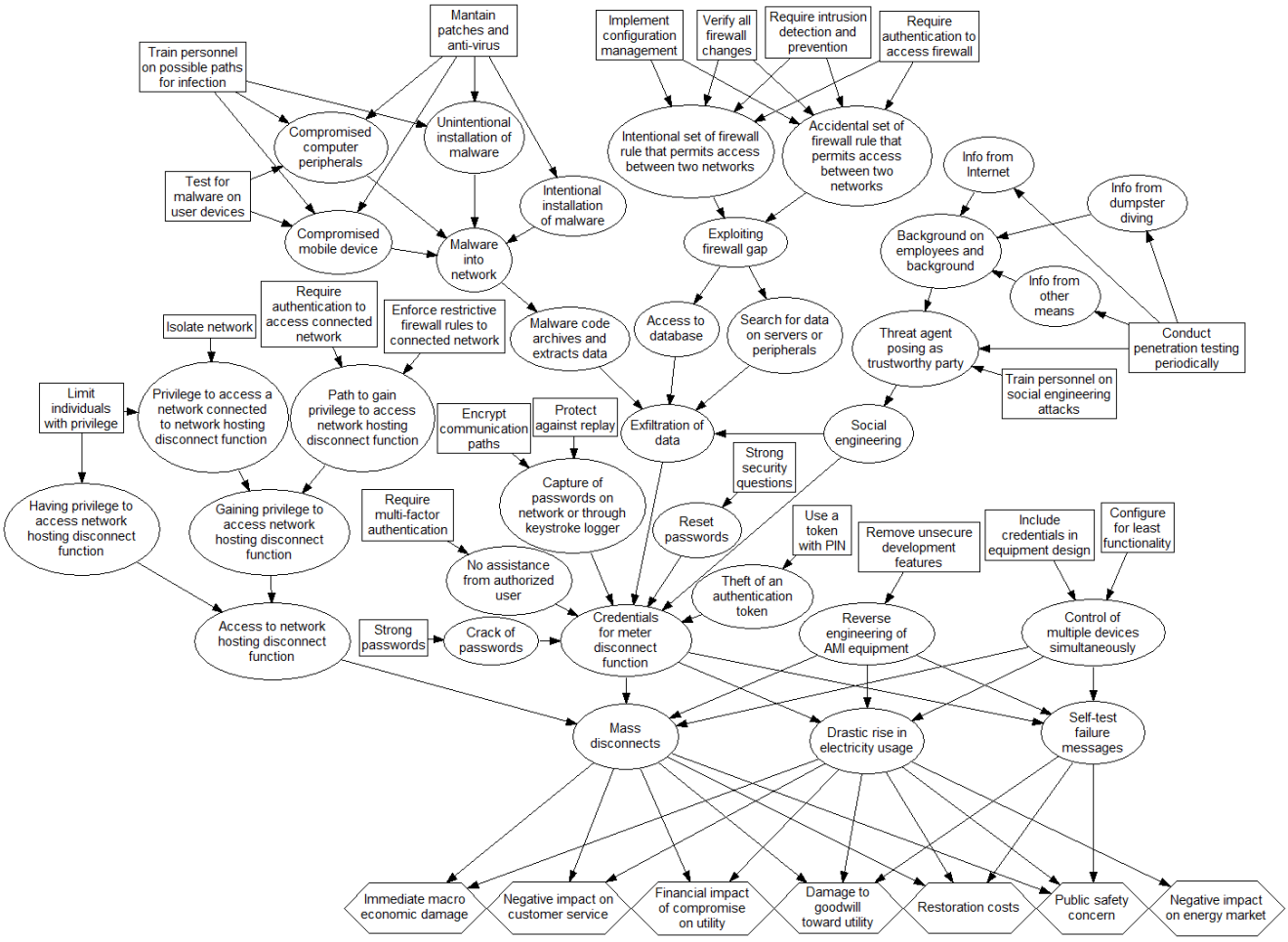


Figure 4: Bayesian network for selected cyber threat scenarios to the Advanced Metering Infrastructure of an electric power system.

authorized employee brings malware into system or network; threat agent exploits firewall gap.

These cyber threats potentially lead to "Threat agent performs mass disconnects", "Threat agent sends demand-response messages to drastically raise electricity usage" and "Threat agent causes devices to send last gasps or self-test failure messages", which indicate the possible outcomes of cyber attacks to the AMI systems. In Figure 4, the Bayesian network is based on the attack graphs of the 8 cyber threat scenarios to represent the alternative opportunities to attack the system. In particular, the circles represent the events of the cyber threat scenarios, the diamonds indicate the possible impacts of cyber attacks whereas the squares show mitigation actions that could be deployed for protecting the AMI system from cyber threats. Note that the event "Threat agent obtains credentials for the meter disconnect function" is equivalent among both cyber threat scenarios in Figures 1a and 1b. For this reason, this event has been represented by one chance node named "Credentials for meter disconnect function" in the Bayesian network. Reducing redundancies of equivalent events in multiple cyber threat scenarios facilitates the comprehensive analysis of cyber threats as a Bayesian network. In addition, the events "Threat agent has headend credentials and initiates disconnect(s) at headend" and "Threat agent has business system credentials and initiates disconnect(s) at business system" in Figure 1a are not considered in the Bayesian network because it is sufficient that the threat agent gains access to the network hosting the meter disconnect function and obtains the relative credentials to cause "Possible voltage/frequency fluctuations with disconnected customers".

In the Bayesian network, probability distributions of the chance nodes have been set according to information provided by the NESCOR documents. For instance, the psychological manipulation (social engineering) of an employee may be expensive and it could lead to a public disclosure if the attempt

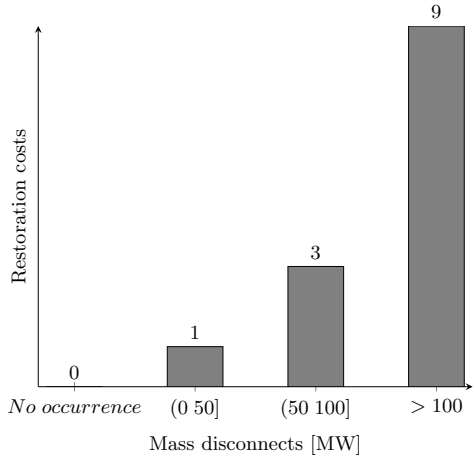


Figure 5: Illustrative impact scores for "Restoration costs".

fails, which summarizes to a low occurrence probability. However, such information is not sufficient to specifically quantify the occurrence probability. For this reason, the occurrence probabilities of this example are not meant to be representative of any existing AMI system, but they are illustrative values to prove the viability of the Bayesian framework. The value nodes list the impact criteria of Table 4, in particular the ones affected by a possible cyber attack to the AMI systems. For illustrative purposes, impacts V_k have been quantified based on the scoring system of Table 4 due to the lack of detailed information in literature. For instance, the event "Threat agent performs mass disconnects" is quantified in different states of mass disconnects: *No occurrence*, (0 50]MW, (50 100]MW, > 100MW. Thus, each value node maps the impact score depending on the states of that event, as illustrated in Figure 5 for the impact criterion "Restoration costs". Note that the impacts of cyber threats are not necessarily evaluated by every criteria of Table 4. For instance, the event "Threat agent performs mass disconnects" does not affect the impact criterion "Loss of privacy" for any state.

Assuming that event i is "Threat agent performs mass disconnects" and the value node represents the impact criterion "Restoration costs" in Figure 2, the expected impact of "Restoration costs" $[k = RC]$ is the weighted average of the impact scores for every state in Figure 5, such that

$$\mathbb{E}[V_{RC}] = \mathbb{P}[X_i \leq 50MW]\ V_{RC}[X_i \leq 50MW] + ... + \mathbb{P}[X_i \geq 100MW]\ V_{RC}[X_i \geq 100MW]. \quad (15)$$

The NESCOR documents also list possible mitigation actions that could be deployed to protect the AMI systems from cyber threats, specifying the events affected by each mitigation action. The deployment of a mitigation action affects the occurrence probability of the cyber threats according to the effect of

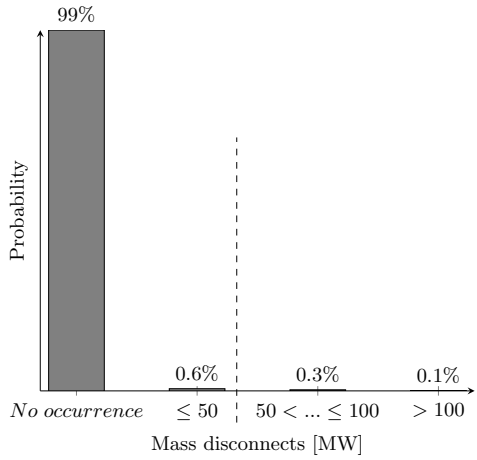


Figure 6: Illustrative probability distribution for mass disconnects.

the action. In particular, this case study accounts for 22 possible mitigation actions, which lead to 2^{22} mitigation strategies. Tables 5-10 list the 22 mitigation actions for the selected cyber threat scenarios, specifying the affected events based on the NESCOR analyses. The first column of the tables lists the index of the action in the portfolio $\mathbf{z}$, whereas the third column lists the cost of each mitigation action. The illustrative costs of mitigation actions aim to include a budget constraint to the optimization model. In addition, the optimization model includes a technical constraint on the risk acceptability of mass disconnects above 50MW. Figure 6 illustrates the probability distribution of the event "Threat agent performs mass disconnects" deriving from the deployment of a generic portfolio $\mathbf{z}$. Assuming that experts set the risk acceptability threshold to 0.5%, then the occurrence probability of the critical states must fulfill the constraint

$$\mathbb{P}[X_i > 50MW|\mathbf{z}] \leq 0.5\%. \tag{16}$$

The results of the multi-objective optimization show a decrease of the risk of every impact criteria by increasing the budget level. Figure 7 shows that larger budgets lead to more effective mitigation strategies to reduce the risk of every impact criteria. In this case study, the risk profiles of some impact criteria are overlapping because the impact scores are based on the same $0-9$ scale that limit the quantification of the impacts. The analysis of the risk profiles supports the definition of the optimal budget by selecting the budget level above which the risk converges for every impact criteria, such as $B \geq 400$ in this example. Computational time is around one hour on a regular laptop, however it depends on the constraints limiting the set of feasible portfolios. For instance, relaxing the budget constraint leads to higher computational time because the algorithm considers a larger set of feasible portfolios. In Figure 7, the risk profiles

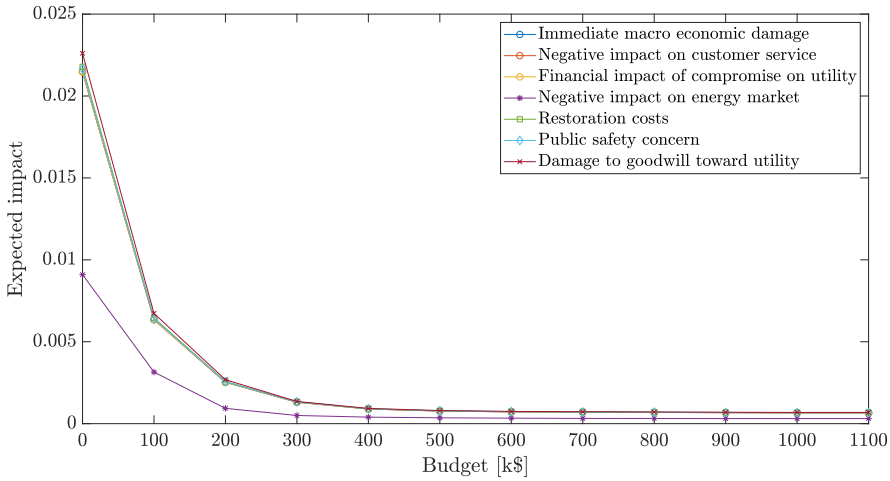


Figure 7: Expected impact of each impact criterion for different budget levels.

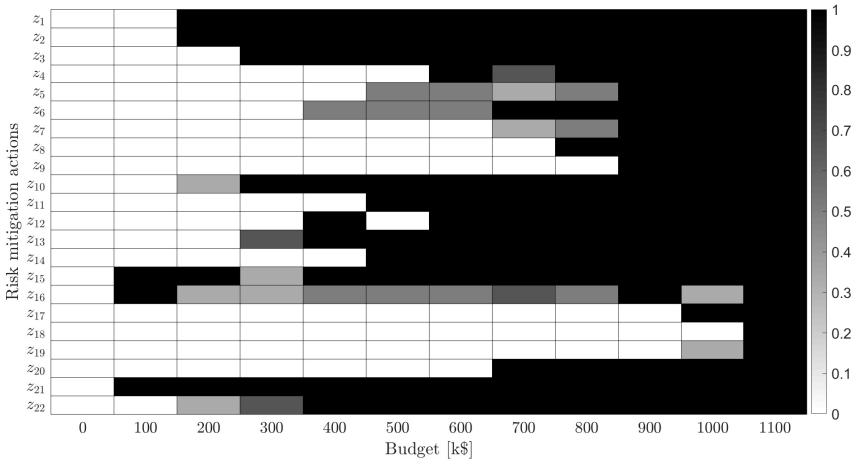


Figure 8: Core index map of mitigation actions for different budget levels.

consider all the non-dominated portfolios selected by the optimization algorithm for each budget level. Then, the core index of each mitigation action is computed to support the choice of actions that should be selected or rejected. Figure 8 maps the core index of each mitigation action through a gray scale. Specifically, a black square indicates that the action is included in every non-dominated portfolio, whereas a white square indicates that the action is not included in any non-dominated portfolio. Gray squares indicate a core index in the range $(0, 1)$, meaning that the mitigation action is included in some non-dominated portfolios, but not all.

As a result, the black-squared actions should be selected whereas the white-squared actions should be rejected. On the other hand, gray-squared actions need additional analyses to support the selection or rejection of the deployment on the AMI system. In this case study, the additional analyses would be necessary only for a limited number of mitigation actions for some budget levels. For instance, for budget $B = 500$k\$ the mitigation actions z_5, z_6 and z_{16} belong to 50% of the non-dominated portfolios. The other mitigation actions belongs to either all or none of the non-dominated portfolios, so they do not require any additional analysis.

5 Discussion

The case study shows the potential of a comprehensive analysis of multiple cyber threats. Integrating the cyber threat scenarios into a Bayesian network facilitates the detection of system vulnerabilities and the definition of appropriate mitigation actions for protecting the cyber physical system. In this respect, actions affecting multiple cyber threats and synergies of actions affecting the same event(s) can be easily

represented in a single model. This model results in a clear graphical representation of the possible cyber threats to the system by erasing the redundancies deriving from equivalent events in multiple scenarios.

The model relies on the definition of the occurrence probability of cyber threats, which could be a troublesome task. However, the decomposition of the cyber threat scenario into cascading events facilitates the definition of the occurrence probabilities of the single events. In addition, the collection of information on successful and unsuccessful cyber attacks could provide valuable data to estimate the occurrence probability of specific events [32]. These statistical analyses are not sufficient because the threat agents would exploit system vulnerabilities that were not necessarily available in past attacks, which by definition are not included in the existing data [33]. Specifically, a cyber threat may not be recognized until it manifests, thus it may be missed in threat scenarios that are examined as part of the risk assessment [34]. For this reason, it is necessary to integrate statistical analyses with information provided by experts based on investigations on possible system vulnerabilities.

The probabilistic representation of cyber threat scenarios provides a solid framework for the risk assessment of cyber physical system. It also enhances detailed analyses for risk management, in contrast to the binary representation through the attack graphs. Moreover, Bayesian networks make it possible to update the probability of the cascading events of cyber threat scenarios. As a result, the model represents the effect of the deployment of mitigation actions on the system, even considering intrusion detectors to tackle cyber threats that have not been examined for the risk assessment [35]. The evaluation of the risk for each impact criteria provides additional insights into risk management, which would not be possible with the additive model of scores proposed by the EPRI.

In the case study, the impacts of the cyber threats have been set according to the scoring system in Table 4. However, it is advisable to set different numeric scales based on the specificity of the impact criterion, for instance the criterion "Restoration costs" should be evaluated through a monetary scale. Note that the choice of the scale could lead to different solutions of the optimization model [36].

Finally, the Bayesian framework has broader applications than electric power systems to consider cyber threats on any cyber physical system. For instance, the National Vulnerability Database provides information about vulnerabilities of IT systems through the Common Vulnerability Scoring System [37].

6 Conclusions

In this paper, we have developed a Bayesian framework to analyze the vulnerabilities of cyber physical systems and optimize the resource allocation to protect the system from cyber threats. In particular, the selection of mitigation actions is based on the analysis of multiple outcomes of cyber attacks, including financial, safety and service impacts. Cyber threat scenarios are modeled through Bayesian networks

to overview the alternative opportunities to pursue a cyber attack leading to such impacts. Thus, the minimization of the expected impacts supports the choice of mitigation strategies based on a multi-objective optimization model.

The optimization model integrates budget and technical constraints that limit the set of feasible portfolios in order to select the optimal mitigation strategies. Specifically, the optimal mitigation strategies correspond to the portfolios that reduce the risk of cyber threats for any impact criterion without increasing the risk for other impact criteria. As a result, we have showed that a comprehensive analysis of the cyber threat scenarios leads to an optimal mitigation strategy for the system. The viability of the Bayesian framework has been illustrated through a case study concerning the Advanced Metering Infrastructure of an electric power system, which have raised several security concerns.

In conclusion, this framework can be introduced as a novel practice for assessing the risks of cyber threats and for supporting risk-based decisions on resource allocation to cyber physical systems. Possible extensions need to be investigated, such as modeling the objectives of the threat agent(s) through Adversarial Risk Analysis [38, 39]. Future research will focus on the analysis of the cyber resilience [40], meaning the ability of the cyber physical system to continuously deliver the intended outcome despite adverse cyber events.

Acknowledgments

The research was partly developed in the Young Scientists Summer Program at the International Institute for Applied Systems Analysis, Laxenburg (Austria) with financial support from the Academy of Finland. The research was partly supported by the European Union's Horizon 2020 project 740920 CYBECO.

References

[1] Lee, J., Bagheri, B. and Kao, H.A., 2015. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, 3, pp.18-23.

[2] Smith, M.D. and Paté-Cornell, M.E., 2018. Cyber Risk Analysis for a Smart Grid: How Smart is Smart Enough? A Multiarmed Bandit Approach to Cyber Security Investment. IEEE Transactions on Engineering Management.

[3] Whitehead, D.E., Owens, K., Gammel, D. and Smith, J., 2017, April. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In Protective Relay Engineers (CPRE), 2017 70th Annual Conference for (pp. 1-8). IEEE.

[4] Yaqoob, I., Ahmed, E., ur Rehman, M.H., Ahmed, A.I.A., Al-garadi, M.A., Imran, M. and Guizani, M., 2017. The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 129, pp.444-458.

[5] Nourian, A. and Madnick, S., 2018. A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet. IEEE Transactions on Dependable and Secure Computing, 15(1), pp.2-13.

[6] Lee, R.M., Assante, M.J. and Conway, T., 2014. German steel mill cyber attack. Industrial Control Systems, 30, p.62.

[7] Kshetri, N., 2010. The global cybercrime industry: economic, institutional and strategic perspectives. Springer Science and Business Media.

[8] Poolsappasit, N., Dewri, R. and Ray, I., 2012. Dynamic security risk management using bayesian attack graphs. IEEE Transactions on Dependable and Secure Computing, 9(1), pp.61-74.

[9] Shameli-Sendi, A., Louafi, H., He, W. and Cheriet, M., 2018. Dynamic optimal countermeasure selection for intrusion response system. IEEE Transactions on Dependable and Secure Computing, 15(5), pp.755-770.

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

[11] Barrett, M.P., 2018. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (No. NIST Cybersecurity Framework).

[12] Zio, E., 2009. Computational methods for reliability and risk analysis (Vol. 14). World Scientific Publishing Company.

[13] Electric Power Research Institute, 2015. Analysis of selected electric sector high risk failure scenarios. National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1.

[14] Ciapessoni, E., Cirio, D., Kjølle, G., Massucco, S., Pitto, A. and Sforna, M., 2016. Probabilistic risk-based security assessment of power systems considering incumbent threats and uncertainties. IEEE Transactions on Smart Grid, 7(6), pp.2890-2903.

[15] Shelar, D. and Amin, S., 2017. Security assessment of electricity distribution networks under DER node compromises. IEEE Transactions on Control of Network Systems, 4(1), pp.23-36.

[16] Electric Power Research Institute, 2015. Electric sector failure scenarios and impact analyses. National Electric Sector Cybersecurity Organization Resource (NESCOR) Technical Working Group 1.

[17] Johnson, P., Vernotte, A., Gorton, D., Ekstedt, M. and Lagerström, R., 2016, October. Quantitative information security risk estimation using probabilistic attack graphs. In International Workshop on Risk Assessment and Risk-driven Testing (pp. 37-52). Springer, Cham.

[18] Ni, H., Chen, A. and Chen, N., 2010. Some extensions on risk matrix approach. Safety Science, 48(10), pp.1269-1278.

[19] Cox Jr, L.A., 2008. What's wrong with risk matrices?. Risk Analysis, 28(2), pp.497-512.

[20] Duijm, N.J., 2015. Recommendations on the use and design of risk matrices. Safety science, 76, pp.21-31.

[21] Allodi, L. and Massacci, F., 2017. Security events and vulnerability data for cybersecurity risk estimation. Risk Analysis, 37(8), pp.1606-1627.

[22] Liu, Y. and Man, H., 2005, March. Network vulnerability assessment using Bayesian networks. In Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2005 (Vol. 5812, pp. 61-72). International Society for Optics and Photonics.

[23] Frigault, M. and Wang, L., 2008, July. Measuring network security using bayesian network-based attack graphs. In Annual IEEE International Computer Software and Applications Conference (pp. 698-703). IEEE.

[24] Kordy, B., Pitre-Cambacds, L. and Schweitzer, P., 2014. DAG-based attack and defense modeling: Dont miss the forest for the attack trees. Computer science review, 13, pp.1-38.

[25] Nielsen, T.D. and Jensen, F.V., 2009. Bayesian networks and decision graphs. Springer Science and Business Media.

[26] Xie, P., Li, J.H., Ou, X., Liu, P. and Levy, R., 2010, June. Using Bayesian networks for cyber security analysis. In Dependable Systems and Networks (DSN), 2010 IEEE/IFIP international conference on (pp. 211-220). IEEE.

[27] Couce-Vieira, A., Houmb, S.H. and Ros-Insua, D., 2017, August. CSIRA: A Method for Analysing the Risk of Cybersecurity Incidents. In International Workshop on Graphical Models for Security (pp. 57-74). Springer, Cham.

[28] Liesiö, J., Mild, P. and Salo, A., 2008. Robust portfolio modeling with incomplete cost information and project interdependencies. European Journal of Operational Research, 190(3), pp.679-695.

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

[30] Mancuso, A., Compare, M., Salo, A. and Zio, E., 2019. Portfolio optimization of safety measures for the prevention of time-dependent accident scenarios. Reliability Engineering and System Safety 190 (106500), pp. 1-9.

[31] Coello, C.A.C., Lamont, G.B. and Van Veldhuizen, D.A., 2007. Evolutionary algorithms for solving multi-objective problems (Vol. 5). New York: Springer.

[32] Holm, H., 2014. A large-scale study of the time required to compromise a computer system. IEEE Transactions on Dependable and Secure Computing, 11(1), pp.2-15.

[33] Paté-Cornell, M.E., Kuypers, M., Smith, M. and Keller, P., 2018. Cyber risk management for critical infrastructure: a risk analysis model and three case studies. Risk Analysis, 38(2), pp.226-241.

[34] Linkov, I., Eisenberg, D.A., Plourde, K., Seager, T.P., Allen, J. and Kott, A., 2013. Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), pp.471-476.

[35] Modelo-Howard, G., Bagchi, S. and Lebanon, G., 2008, September. Determining placement of intrusion detectors for a distributed application through bayesian network modeling. In International Workshop on Recent Advances in Intrusion Detection (pp. 271-290). Springer, Berlin, Heidelberg.

[36] Hämäläinen, R.P. and Lahtinen, T.J., 2016. Path dependence in Operational ResearchHow the modeling process can influence the results. Operations Research Perspectives, 3, pp.14-20.

[37] Zhang, Y., Wang, L., Xiang, Y. and Ten, C.W., 2015. Power system reliability evaluation with SCADA cybersecurity considerations. IEEE Transactions on Smart Grid, 6(4), pp.1707-1721.

[38] Banks, D.L., Aliaga, J.M.R. and Insua, D.R., 2015. Adversarial Risk Analysis. Chapman and Hall/CRC.

[39] Insua, D.R., CouceVieira, A., Rubio, J.A., Pieters, W., Labunets, K. and G. Rasines, D., 2019. An adversarial risk analysis framework for cybersecurity. Risk Analysis.

[40] Gisladottir, V., Ganin, A.A., Keisler, J.M., Kepner, J. and Linkov, I., 2017. Resilience of cyber systems with over and underregulation. Risk Analysis, 37(9), pp.1644-1651.

Supplementary tables

Table 3: Likelihood Criteria With Scoring System [16].

Likelihood criterion	**Scoring system**
Skill required	0: Deep domain/insider knowledge and ability to build custom attack tools; 1: Domain knowledge and cyber attack techniques; 3: Special insider knowledge needed; 9: Basic domain understanding and computer skills.
Accessibility (physical)	0: Inaccessible; 1: Guarded, monitored; 3: Fence, standard locks; 9: Publicly accessible.
Accessibility (logical, assume have physical access)	0: High expertise to gain access; 1: Not readily accessible; 3: Publicly accessible but not common knowledge; 9: Common knowledge or none needed.
Attack vector (assume have physical and logical access)	0: Theoretical; 1: Similar attack has been described; 3: Similar attack has occurred; 9: Straightforward, for example script or tools available.
Common vulnerability among others	0: Isolated occurrence; 1: More than one utility; 3: Half or more of power infrastructure; 9: Nearly all utilities.

Table 4: Impact Criteria With Scoring System [16].

Impact criterion	**Scoring system**
Public safety concern	0: none; 1: 10-20 injuries possible; 3: 100 injured possible; 9: one death possible.
Workforce safety concern	0: none; 3: any possible injury; 9: any possible death.
Ecological concern	0: none; 1: logical ecological damage such as localized fire or spill, repairable; 3: permanent local ecological damage; 9: widespread temporary or permanent damage to one or more ecosystems.
Financial impact of compromise on utility	0: petty cash or less; 1: up to 2% of utility revenue; 3: up to 5 %; 9: greater than 5 %.
Restoration costs	0: petty cash or less; 1: up to 1% of utility organization O&M budget; 3: up to 10%; 9: greater than 10%.
Negative impact on generation capacity	0: no effect; 1: small generation facility off-line or degraded operation of large facility; 3: more than 10% loss of generation capacity for 8 hours or less; 9: more than 10% loss of generation capacity for more than 8 hours.
Negative impact on the energy market	0: no effect; 1: localized price manipulation, lost transactions, loss of market participation; 3: price manipulation. lost transactions, loss of market participation impacting a large metro area; 9: market or key aspects of market non operational.
Negative impact on the bulk transmission system	0: no; 1: loss of transmission capability to meet peak demand or isolate problem areas; 3: major transmission system interruption; 9: complete operational failure or shut down of the transmission system.
Negative impact on customer service	0: no; 1: up to 4 hour delay in customer ability to contact utility and gain resolution, lasting one day; 3: up to 4 hour delay in customer ability to contact utility and gain resolution, lasting a week; 9: complete operational failure or shut-down of the transmission system.
Negative impact on billing functions	0: none; 1: isolated recoverable errors in customer bills; 3: widespread but correctible errors in bills; 9: widespread loss of accurate power usage data.
Damage to goodwill toward utility	0: no effect; 1: negative publicity but this does not cause financial loss to utility; 3: negative publicity causing up to 20% less interest in programs; 9: negative publicity causing more than 20% less interest in programs.
Immediate macro economic damage	0: none; 1: local businesses down for a week; 3: regional infrastructure damage; 9: widespread runs on banks.
Long term economic damage	0: none; 3: several years of local recession; 9: several years of national recession.
Loss of privacy	0: none; 1: 1000 or less individuals; 3: thousands of individuals; 9: millions of individuals.

Table 5: Mitigation Actions for Scenario "Authorized Employee Brings Malware Into System or Network".

Index	Mitigation actions	Cost [k$]	Affected event(s)
1	Train personnel on possible paths for infection	30	Compromised mobile device
			Compromised computer peripherals
			Unintentional installation of malware
2	Maintain patches and anti-virus	70	Compromised mobile device
			Compromised computer peripherals
			Unintentional installation of malware
			Intentional installation of malware
3	Test for malware before connection	50	Compromised mobile device
			Compromised computer peripherals

Table 6: Mitigation Actions for Scenario "Threat Agent Exploits Firewall Gap".

Index	Mitigation actions	Cost [k$]	Affected event(s)
4	Implement configuration management	40	Intentional set of firewall rule that permits access between two networks
			Accidental set of firewall rule that permits access between two networks
5	Verify all firewall changes	60	Intentional set of firewall rule that permits access between two networks
			Accidental set of firewall rule that permits access between two networks
6	Require intrusion detection	30	Intentional set of firewall rule that permits access between two networks
			Accidental set of firewall rule that permits access between two networks
7	Require authentication to access firewall	50	Intentional set of firewall rule that permits access between two networks
			Accidental set of firewall rule that permits access between two networks

Table 7: Mitigation Actions for Scenario "Threat Agent Uses Social Engineering".

Index	Mitigation actions	Cost [k$]	Affected event(s)
8	Conduct penetration testing periodically	70	Info from Internet
			Info from dumpster diving
			Info from other means
			Threat agent posing as trustworthy party
9	Train personnel on social engineering attacks	40	Threat agent posing as trustworthy party

Table 8: Mitigation Actions for Scenario "Threat Agent Obtains Credentials for System or Function".

Index	Mitigation actions	Cost [k$]	Affected event(s)
10	Strong passwords	30	Crack of passwords
11	Encrypt communication paths	80	Capture of passwords on network or through keystroke logger
12	Protect against replay	60	Capture of passwords on network or through keystroke logger
13	Strong security questions	30	Reset passwords
14	Require multi-factor authentication	50	No assistance from authorized user
15	Use a token with PIN	20	Theft of an authentication token

Table 9: Mitigation Actions for Scenario "Threat Agent Gains Access to Network".

Index	Mitigation actions	Cost [k$]	Affected event(s)
16	Limit individuals with privilege	30	Having privilege to access network hosting disconnect function
			Privilege to access a network connected to network hosting disconnect function
17	Isolate network	90	Privilege to access a network connected to network hosting disconnect function
18	Enforce restrictive firewall rules to access connected network	70	Path to gain privilege to access network hosting disconnect function
19	Require authentication to access connected network	40	Path to gain privilege to access network hosting disconnect function

Table 10: Mitigation Actions for Scenario "Reverse Engineering of AMI Equipment Allows Unauthorized Mass Control".

Index	Mitigation actions	Cost [k$]	Affected event(s)
20	Remove unsecure development features	80	Reverse engineering of AMI meters
21	Include credentials in equipment design	50	Control of many devices simultaneously
22	Configure for least functionality	30	Control of many devices simultaneously

Publication III

Alessandro Mancuso, Michele Compare, Ahti Salo and Enrico Zio. Portfolio optimization of safety measures for the prevention of time-dependent accident scenarios. *Reliability Engineering and System Safety*, 190(106500):1-9, October 2019.

Reliability Engineering and System Safety 190 (2019) 106500

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

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

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

[a] Department of Mathematics and Systems Analysis, Aalto University, Finland
[b] Department of Energy Engineering, Politecnico di Milano, Italy
[c] Aramis s.r.l., Milano, Italy
[d] MINES ParisTech, PSL Research University, CRC, Sophia Antipolis, France

ARTICLE INFO

Keywords:
Risk analysis
Preventive safety measures
Dynamic Bayesian Networks
Portfolio optimization

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 vapour 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 preventive safety measures, which provides additional management insights.

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. Therefore, we 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 [5–7]. Specifically, BNs make it possible (i) to circumvent the limitations of the 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 [9–11].

In this paper, we extend the PDA methodology to time-dependent accident scenarios by explicitly modelling 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 in the failure states

* Corresponding author.
E-mail address: alessandro.mancuso@aalto.fi (A. Mancuso).

https://doi.org/10.1016/j.ress.2019.106500
Received 23 January 2018; Received in revised form 5 March 2019; Accepted 12 May 2019
Available online 14 May 2019
0951-8320/

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 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 vapour 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. Fig. 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.

In particular, node $V^i(\tau)$ encodes the possible states of the failure event i at time $\tau \in \mathbb{T}$. In Fig. 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

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

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 Fig. 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

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

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

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 Fig. 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 $s \in \mathbb{S}^i(\tau)$ so 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

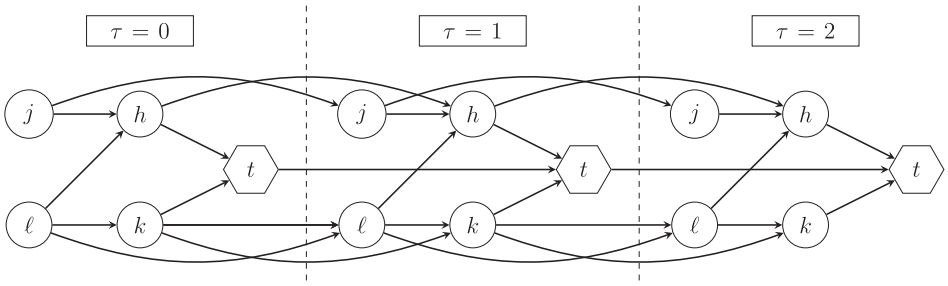


Fig. 1. Example of a Dynamic Bayesian Network.

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_a^i represents the choice of preventive safety measure $a \in \mathbb{A}^i$ such that $z_a^i = 1$ 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 $\mathbb{A}^i = \varnothing$ so that $|\mathbb{A}^i| = 0$. Thus, the binary vector $\mathbf{z}$ defines the portfolio of preventive safety measures as the concatenation of vectors $\mathbf{z}^i = [z_1^i, ..., z_{|\mathbb{A}^i|}^i]$ 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 the set $\mathbb{A}^i$ so that

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

Synergies between preventive safety measures can be modelled through 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 $\mathbb{P}^s_{X_a^i(\tau)}$ for each time $\tau \in \mathbb{T}$. Then, the marginal probability of the realization $s \in \mathbb{S}^i(\tau)$ is

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

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

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

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 $\mathbb{P}^s_{X_a^i(\tau)|\mathbf{x}^i_-(\tau)}$ 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

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

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 $\le$ 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

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

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

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

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

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

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 $\epsilon^s_{X^t}$ so that

$$\mathbb{Q}^s_{X^t(\tau)}(\mathbf{z}) \le \epsilon^s_{X^t}, \quad \forall\, \tau \in \mathbb{T}. \tag{18}$$

The values of $\epsilon^s_{X^t}$ 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

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

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

Initialization: $\mathbf{z} = [0, ..., 0]$; $m \leftarrow 1$; $\mathbf{Z}^* \leftarrow \emptyset$;
if $\mathbf{z} \in \mathbf{Z}_F$ **then**
  $\mathbf{Z}^* \leftarrow \mathbf{z}$;
end
while $m > 0$ **do**
  Forward-loop:
  while $m \leq M$ **do**
    $z_m \leftarrow 1$;
    if $\mathbf{z} \in \mathbf{Z}_F$ and $\mathbf{z}^* \not\succ \mathbf{z}\ \forall \mathbf{z}^* \in \mathbf{Z}^*$ **then**
      $\mathbf{Z}^* \leftarrow \mathbf{z} \cup \{\mathbf{z}^* \in \mathbf{Z}^* | \mathbf{z} \not\succ \mathbf{z}^*\}$;
    end
    if $\sum_{j=1}^{m} z_j H_j^\ell + \sum_{j=m+1}^{M} \min\{0, H_j^\ell\} > b^\ell$ for any $\ell = 1, ..., L$ **then**
      Break *Forward-loop*;
    end
    $m \leftarrow m + 1$;
  end
  Backtrack step:
  $z_M \leftarrow 0$;
  $m \leftarrow \max\left[\{j | z_j = 1\} \cup \{0\}\right]$;
  if $m > 0$ **then**
    $z_m \leftarrow 0$;
    $m \leftarrow m + 1$;
  end
end
$\mathbf{Z}_{ND} \leftarrow \mathbf{Z}^*$;

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

solutions of which one must be selected and deployed. For this purpose, we propose four possible procedures:

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

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

- 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.
- 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 [27] 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 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

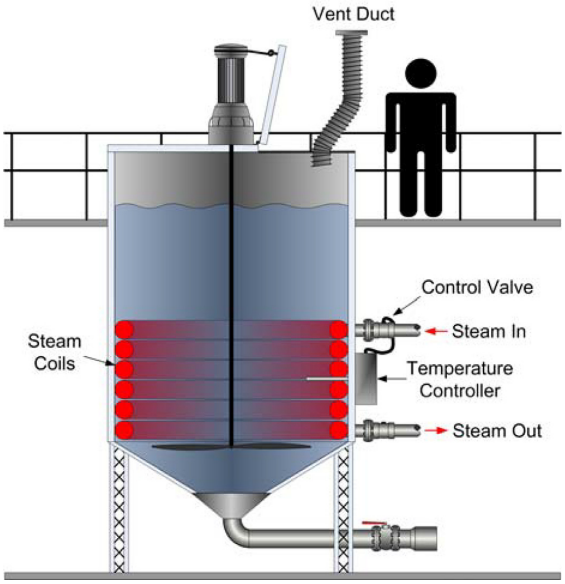


Fig. 2. Mixing tank mechanical system [28].

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.

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, 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 andsignificant 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 vapour emissions. Fig. 2 illustrates the process system.

According to the full-scale investigation conducted by the Chemical Safety Board [28], 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 vapour. Because the

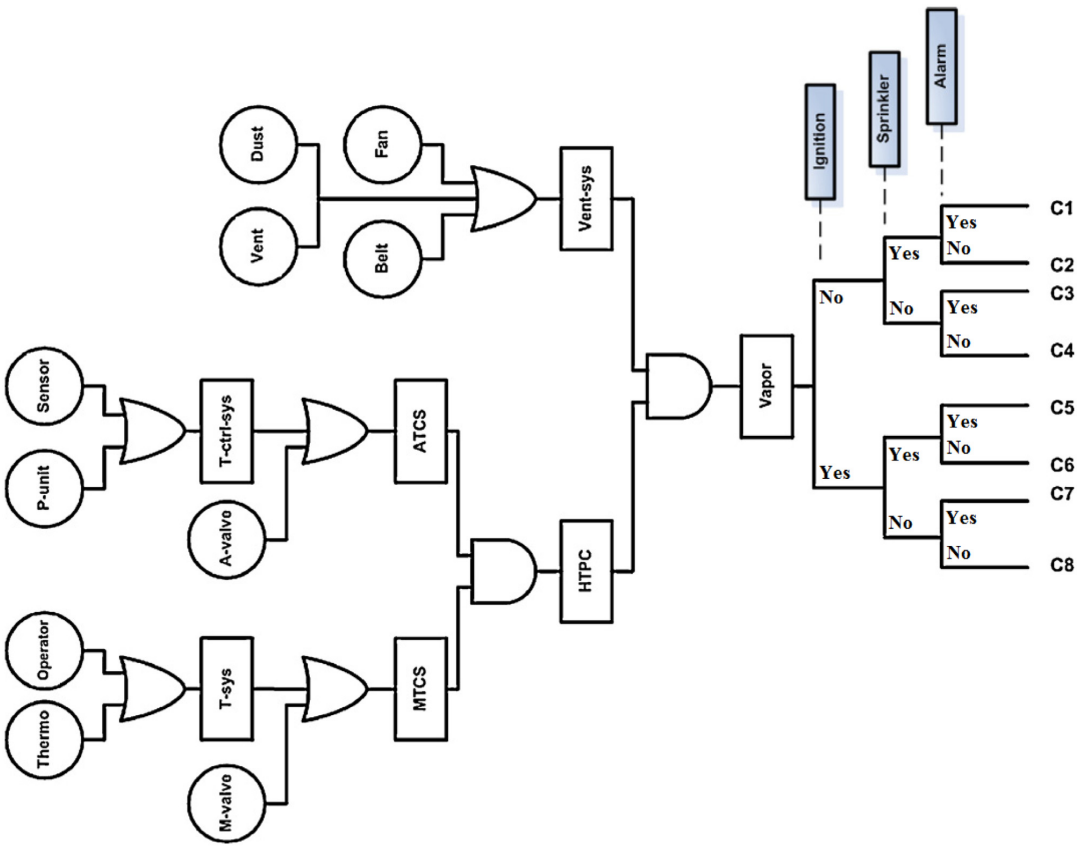


Fig. 3. Fault Tree and Event Tree for the accident scenarios of a mixing tank mechanical system [19].

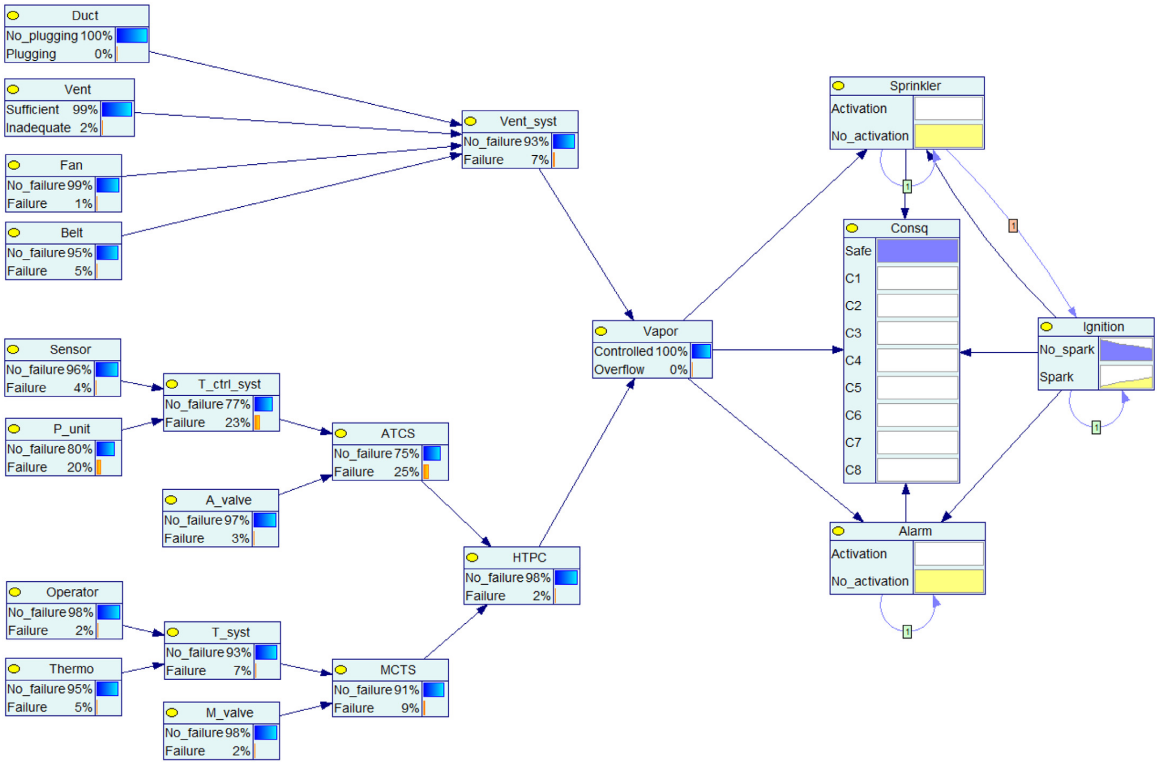


Fig. 4. DBN for the accident scenarios of a mixing tank mechanical system.

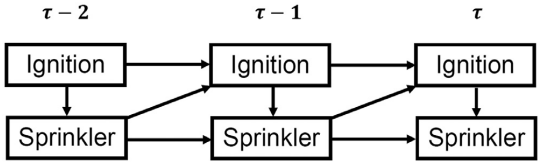


Fig. 5. Causal dependence of *Ignition* to *Sprinkler* throughout multiple time stages.

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. It was also found that the ventilation system would not have had enough capacity to collect such a high volume of vapour, even if it had been working. Following the accident investigation, Khakzad et al. [19] developed the Fault Tree and Event Tree in Fig. 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.

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*. Fig. 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.

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 vapour overflow. In Fig. 4, the temporal delay δ is specified by the squared number over the respective arc. If no squared number is associated with 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 $\tau - 1$. Fig. 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.

Because the vapour cloud is not toxic, any fatalities or injuries can be attributed to the vapour 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 the vapour 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 vapour concentration in the air even if the vapour is not ignited (*Vapor* = *Overflow* and *Ignition* = *No_spark*). The activation of *Sprinkler* and *Alarm* for a vapour 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 [29].

Preventive safety measures reduce the expected disutility of the negative outcomes at the safety target *Consq*. Our Data in Brief article [29] 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

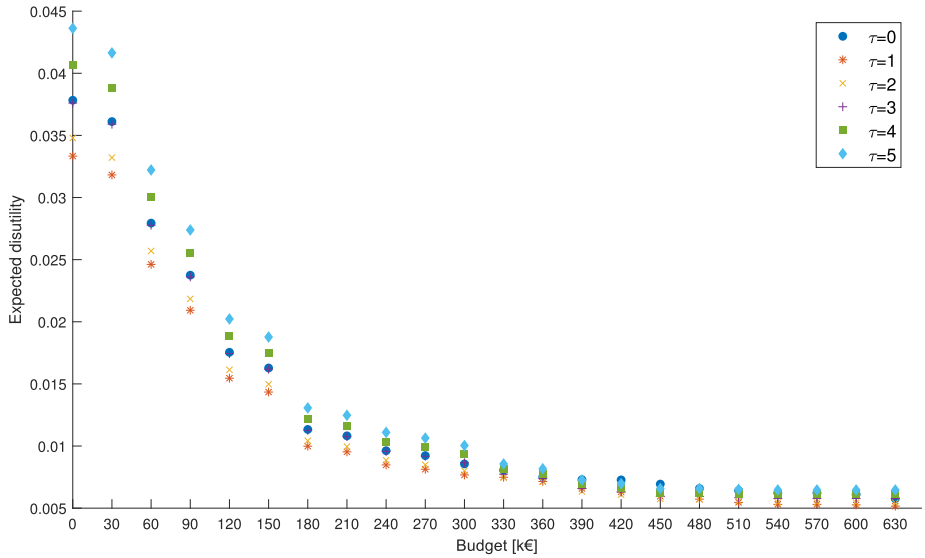


Fig. 6. Minimum expected disutility of safety target *Consq*.

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

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.

Fig. 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 Fig. 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. Fig. 6 also provides additional risk management insights, for instance for defining

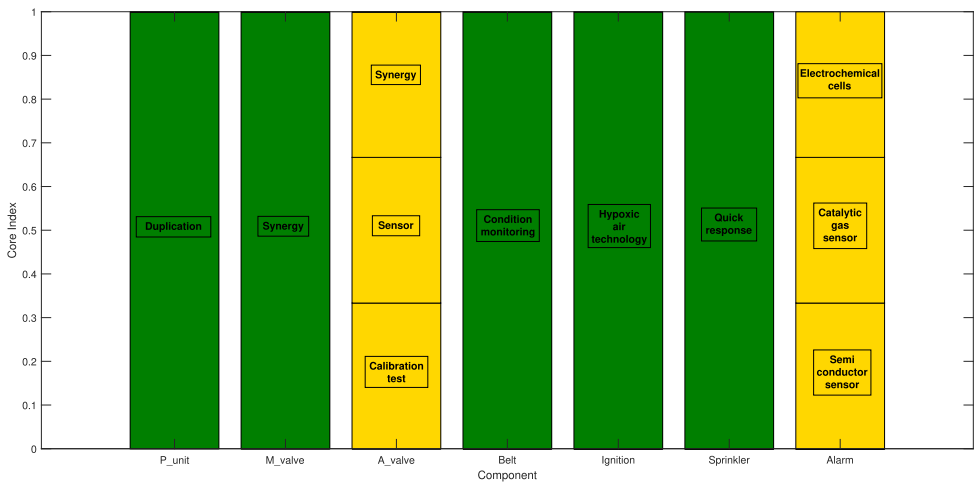


Fig. 7. Core index analysis of preventive safety measures.

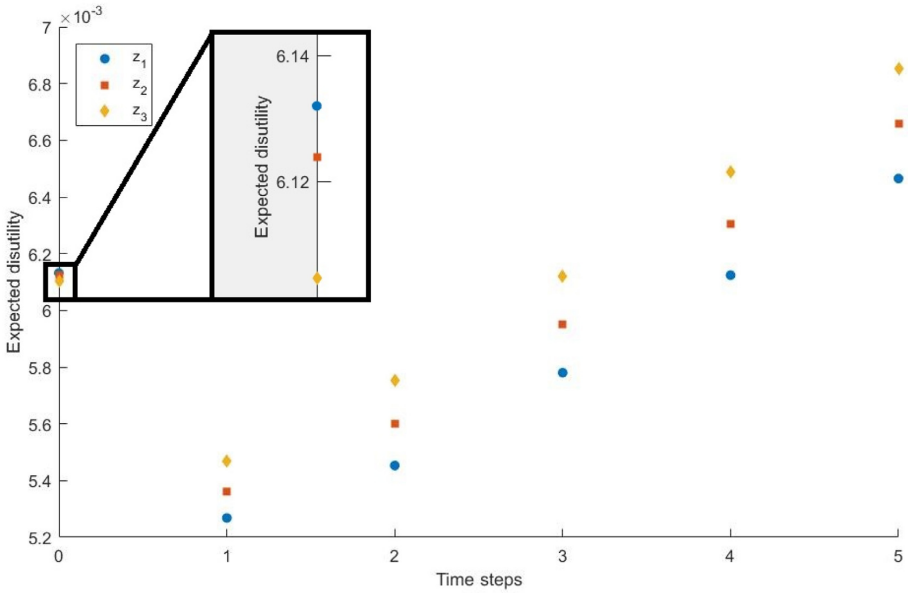


Fig. 8. Expected disutility of non-dominated portfolios by setting $B = 600$ k€.

the requisite budget to meet safety targets and for assessing how increases in the budget reduce the system risk [30].

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

The analysis of the core indexes in Fig. 7 recommends deploying 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.

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, Fig. 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.

4. Discussion

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. 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 make 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 [31] 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 vapour 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 be built through advances in dynamic optimization and contingent portfolio programming [32].

Acknowledgements

The research has been supported by the PRAMEA project of SAFIR2018 Research Programme and the PVN project, funded by the Strategic Research Council of the Academy of Finland (decision nr. 314207). 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. Reliab Eng Syst Saf 2017;167:20–9.
[3] Salo A, Keisler J, Morton A. Portfolio decision analysis: improved methods for resource allocation. Int Ser Oper Res Manage Sci 2011;162. Springer-Verlag. Springer-Verlag
[4] Nielsen TD, Jensen FV. Bayesian Networks and Decision Graphs. Springer Science and Business Media; 2009.
[5] Pollino CA, Woodberry O, Nicholson A, Korb K, Hart BT. Parametrisation and evaluation of a bayesian network for use in an ecological risk assessment. Environ Modell Softw 2007;22:1140–52.
[6] Marsh W, Bearfield G. Using bayesian networks to model accident causation in the UK railway industry. Probabilistic Safety Assessment and Management. 2004. p. 3597–602. Springer London
[7] Kabir G, Tesfamariam S, Francisque A, Sadiq R. Evaluating risk of water mains failure using a bayesian belief network model. Eur J Oper Res 2015;240:220–34.
[8] Weber P, Median-Oliva G, Iung B. Overview on bayesian networks application for dependability, risk analysis and maintenance areas. Eng Appl Artif Intell 2012;25:671–82.
[9] Aldemir T. A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. Ann Nucl Energy 2013;52:113–24.
[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. Reliab Eng Syst Saf 2010;95:49–57.
[11] Zio E, Di Maio F, Stasi M. A data-driven approach for predicting failure scenarios in nuclear systems. Ann Nucl Energy 2010;37:482–91.
[12] Murphy KP. Dynamic Bayesian Networks: Representation, Inference and Learning. Berkeley: Doctoral dissertation, University of California; 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. 2008. p. 23–9.
[14] Oniśko A, Druzdzel MJ. Impact of precision of bayesian networks parameters on accuracy of medical diagnostic systems. Artif Intell Med 2013:197–206.
[15] Poropudas J, Virtanen K. Simulation metamodeling with dynamic bayesian networks. Eur J Oper Res 2011;214:644–55.
[16] Boudali H, Dugan JB. A discrete-time bayesian network reliability modeling and analysis framework. Reliab Eng Syst Saf 2005;87:337–49.
[17] Barua S, Gao X, Pasman H, Mannan MS. Bayesian network based dynamic operational risk assessment. J Loss Prev Process Ind 2016;41:399–410.
[18] Khakzad N, Khan F, Amyotte P. Risk-based design of process systems using discrete-time bayesian networks. Reliab Eng Syst Saf 2013;109:5–17.
[19] Khakzad N, Khan F, Amyotte P. Dynamic safety analysis of process systems by mapping bow-tie into bayesian network. Process Saf Environ Prot 2013;91:46–53.
[20] Zio E. An Introduction to the Basics of Reliability and Risk Analysis. Singapore: World Scientific Publishing; 2007.
[21] Levitin G, Lisnianski A, Ushakov I. Reliability of multi-state systems: A historical overview. Mathematical and statistical methods in reliability, World Scientific. 2003. p. 123–37.
[22] Pearl J. Probabilistic Reasoning in Intelligent Systems. California: Morgan Kaufmann, San Francisco; 1988.
[23] Von Winterfeldt D, Edwards W. Decision Analysis and Behavioural Research. Cambridge: UK: Cambridge University Press; 1986.
[24] Edwards W, Barron FH. SMARTS and SMARTER: improved simple methods for multiattribute utility measurement. Organ Behav Hum Decis Process 1994;60:306–25.
[25] Liesiö J, Mild P, Salo A. Preference programming for robust portfolio modeling and project selection. Eur J Oper Res 2007;181:1488–505.
[26] Liesiö J, Mild P, Salo A. Robust portfolio modeling with incomplete cost information and project interdependencies. Eur J Oper Res 2008;190:679–95.
[27] Liesiö J. Measurable multiattribute value functions for portfolio decision analysis. Decis Anal 2014;11:1–20.
[28] 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/.
[29] 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.
[30] Modarres M, Kaminskiy MP, Krivtsov V. Reliability Engineering and Risk Analysis: A Practical Guide. New York: CRC press; 2016.
[31] Cozman FG. Credal networks. Artif Intell 2000;120(2):199–233.
[32] Gustafsson J, Salo A. Contingent portfolio programming for the management of risky projects. Oper Res 2005;53:943–53.

Publication IV

Alessandro Mancuso, Michele Compare, Ahti Salo and Enrico Zio. Probabilistic model data of time-dependent accident scenarios for a mixing tank mechanical system. *Data in Brief*, 25(104243):1-5, August 2019.

Data in brief 25 (2019) 104243

Contents lists available at ScienceDirect

Data in brief

journal homepage: www.elsevier.com/locate/dib

Data Article

Probabilistic model data of time-dependent accident scenarios for a mixing tank mechanical system

Alessandro Mancuso [a, b, *], Michele Compare [b, c], Ahti Salo [a], Enrico Zio [b, c, d]

[a] Department of Mathematics and Systems Analysis, Aalto University, Finland
[b] Department of Energy Engineering, Politecnico di Milano, Italy
[c] Aramis s.r.l, Milano, Italy
[d] MINES ParisTech, PSL Research University, CRC, Sophia Antipolis, France

ARTICLE INFO

Article history:
Received 22 May 2019
Received in revised form 14 June 2019
Accepted 2 July 2019
Available online 8 July 2019

Keywords:
Risk analysis
System reliability
Preventive safety measures
Dynamic bayesian networks
Portfolio optimization

ABSTRACT

This article presents the risk assessment of a mixing tank mechanical system based on the failure probabilities of the components. Possible component failures can cause accidents which evolve over multiple time stages and can lead to system failure. The consequences of these accident scenarios are analyzed by quantifying the failure probabilities and severity of their outcomes. Illustrative costs and updated failure probabilities are provided to evaluate preventive safety measures. Data refers to the results of the Bayesian model presented in our research article (Mancuso et al., 2019).

DOI of original article: https://doi.org/10.1016/j.ress.2019.106500.
* Corresponding author. Department of Mathematics and Systems Analysis, Aalto University, Finland.
E-mail address: alessandro.mancuso@aalto.fi (A. Mancuso).

https://doi.org/10.1016/j.dib.2019.104243

Specifications table

Subject	Safety, Risk, Reliability and Quality
Specific subject area	Portfolio optimization for risk mitigation
Type of data	Tables
How data were acquired	Analysis of the numerical results of the Bayesian model [1]
Data format	Analyzed data
Parameters for data collection	Journal reputation
Description of data collection	Literature review
Data source location	Institution: Aalto University City: Helsinki Country: Finland
Data accessibility	With the article
Related research article	Mancuso, A., Compare, M., Salo, A. and Zio, E., 2019. Portfolio optimization of safety measures for the prevention of time-dependent accident scenarios. Reliability Engineering & System Safety, 190 (106500). DOI: https://doi.org/10.1016/j.ress.2019.106500

Value of the data

- The failure probabilities of the components of a mixing tank mechanical system can be used for benchmarking in future research.
- Examples of conditional probability tables illustrate the modelling of time-dependent accident scenarios.
- Novel applications for probabilistic risk assessment are possible based on the data in this article.

1. Data

This article presents the probabilistic model data of the time-dependent accident scenarios for a mixing tank mechanical system. Specifically, we revisit the earlier analyses of the accident scenarios by Khakzad et al. [2] to illustrate the methodology presented in our research article [1]. One of such accident scenarios occurred on 14 June 2006 at Universal Form Clamp in Bellwood (Illinois, U.S.) through a vapor cloud ignition [3].

Table 1 shows the failure probabilities of *Alarm* and *Sprinkler* for different ways of activating such components during an accident. In particular, the activation occurs if the vapor is ignited or if there is a specific amount of vapor concentration in the air, even though the vapor is not ignited.

Based on the analyses by Khakzad et al. [2], Table 2 lists the system components and their failure probabilities. In addition, we assume that the activation of *Sprinkler* reduces the probability of delayed ignitions by 50%, as detailed in Table 3 (last row, first and second columns). For this reason, the activation of the *Sprinkler* for a vapor concentration in the air could prevent delayed ignitions.

Table 4 lists the nine possible outcomes of the accident scenarios where the state *Safe* represents the outcome following the non-occurrence of the system failure (*Vapor* = *Controlled*). The other outcomes are caused by malfunctions of some system components. Due to the activation of *Sprinkler*, accident consequences C_1 and C_2 are less severe than C_3 and C_4, respectively. This information is helpful in eliciting the disutility functions to specify the ranking of the outcome severity. The last column of Table 4 shows illustrative disutility values that quantify the severity of the outcomes.

Based on the failure probabilities in Table 2, the Bayesian model computes the occurrence probabilities of the outcomes of the accident scenarios, reported in Table 5 for each time stage. The deployment of preventive safety measures on some selected components mitigates the risk of the negative outcomes. Table 6 lists the alternative preventive safety measures (second column) that affect the occurrence of failures of specific components (first column). The last two columns of Table 6 report illustrative costs and updated failure probabilities of the components. In particular, the preventive safety measure *Synergy* refers to a combination of *Calibration test* and *Sensor*: if both

Table 1
Conditional probabilities of *Alarm* and *Sprinkler* at $\tau = 0$ (τ refers to the time stage of the Bayesian model).

	Vapor	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 respective failure probability.

Component	Symbol	Failure probability
Sensor	Sensor	0.0400
Pneumatic unit	P_unit	0.2015
Temperature control system	T_ctrl_sys	OR gate
Operator	Operator	0.0200
Infrared thermometer	Thermo	0.0468
Temperature measurement system	T_sys	OR gate
Manual steam valve	M_valve	0.0243
Automatic steam valve	A_valve	0.0276
Automatic temperature control system	ATCS	OR gate
Manual temperature control system	MTCS	OR gate
High temperature protection system	HTPS	AND gate
Ventilation	Vent	0.0150
Fan	Fan	0.0100
Belt	Belt	0.0500
Duct	Duct	0.0010
Ventilation system	Vent_sys	OR gate
Vapor overflow	Vapor	AND gate
Ignition barrier	Ignition	0.1000
Water sprinkler system	Sprinkler	0.0400, 0.3000
Alarm system	Alarm	0.0013, 0.2250

Table 3
Conditional probabilities of *Ignition* at $\tau > 0$ (τ refers to the time stage of the Bayesian model).

	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 accident outcomes (C refers to the accident consequences, numbered based on increasing severity).

Outcome	Symbol	Disutility
Controlled vapor	*Safe*	0
Safe evacuation	C_1	10
Wet vapor cloud near the ground	C_2	15
Safe evacuation with possibility of delayed ignition	C_3	30
Vapor 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 stage (C refers to the accident consequences).

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	6.539252e-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 preventive safety measures and respective failure probability.

Component	Preventive safety measure	Cost [k€]	Failure probability
P_unit	Inspection plan	60	0.1500
	Duplication	80	0.100
M_valve	Calibration test	30	0.0200
	Sensor	40	0.0150
	Synergy	60	0.0100
A_valve	Calibration test	30	0.0200
	Sensor	40	0.0150
	Synergy	60	0.0100
Belt	Periodic test	40	0.0300
	Condition monitoring	100	0.0100
Ignition	Tank blanketing	70	0.0800
	Inerting systems	100	0.0600
	Hypoxic air technology	150	0.0400
Sprinkler	Standard response	40	0.0300, 0.2000
	Quick response	80	0.0100,0.1000
Alarm	Semi-conductor sensor	60	0.0013, 0.2000
	Catalytic gas sensor	80	0.0013, 0.1500
	Electrochemical cells	100	0.0013, 0.1000

measures are installed, this synergy effect yields more benefits than installing independent measures. The updated failure probabilities of *Sprinkler* and *Alarm* refer to the two different failure scenarios detailed in Table 1.

2. Experimental design, materials, and methods

The failure probabilities of the components in Table 2 are provided by the article by Khakzad et al. [2]. Gates represents logic structures of the Bayesian model in our research article [1]. The failure probabilities in Table 6 have been obtained by reducing the initial failure probability of the components, based on a specific reduction rate for each preventive safety measure. These values illustrate the viability of the Bayesian model [1], but do not represent any actual system. The occurrence probabilities of the outcomes of the accident scenarios have been computed by GeNIe Modeler [4] through the Dynamic Bayesian Network presented in our research article [1]. Finally, the severity of the outcomes has been quantified through the trade-off weighing approach SWING [5].

Acknowledgments

The research has been supported by the PRAMEA project of SAFIR2018 Research Programme and the PVN project, funded by the Strategic Research Council of the Academy of Finland (decision nr. 314207).

Conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. Mancuso, M. Compare, A. Salo, E. Zio, Portfolio optimization of safety measures for the prevention of time-dependent accident scenarios, Reliab. Eng. Syst. Saf. (2019) 190 (106500).
[2] N. Khakzad, F. Khan, P. Amyotte, Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network, Process Saf. Environ. Protect. 91 (1–2) (2013) 46–53.
[3] U.S. Chemical, Safety Board, Mixing and Heating a Flammable Liquid in an Open Top Tank, Investigation No. 2006-08-I-IL, April 2007. Washington DC, https://www.csb.gov/universal-form-clamp-co-explosion-and-fire/. (Accessed 13 June 2019).
[4] GeNIe Modeler Software, BayesFusion LCC, http://www.bayesfusion.com/.
[5] D. Von Winterfeldt, W. Edwards, Decision Analysis and Behavioral Research, Cambridge University Press, Cambridge, UK, 1986.

Publication V

Alessandro Mancuso, Michele Compare, Ahti Salo, Enrico Zio and Tuija Laakso. Risk-based optimization of pipe inspections in large underground networks with imprecise information. *Reliability Engineering and System Safety*, 152:228-238, August 2016.

Reliability Engineering and System Safety 152 (2016) 228–238

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Risk-based optimization of pipe inspections in large underground networks with imprecise information

A. Mancuso [a,b], M. Compare [a,c], A. Salo [b,*], E. Zio [a,c,d], T. Laakso [e]

[a] Dipartimento di Energia, Politecnico di Milano, Italy
[b] Department of Mathematics and System Analysis, Aalto University School of Science, Finland
[c] Aramis s.r.l., Milano, Italy
[d] Chair on Systems Science and Energetic Challenge, Fondation Electricité de France (EDF), Centrale Supelec, Universite' Paris-Saclay, Chatenay-Malabry, France
[e] Department of Civil and Environmental Engineering, Aalto University School of Engineering, Finland

ARTICLE INFO

Article history:
Received 26 September 2015
Received in revised form
14 March 2016
Accepted 18 March 2016
Available online 26 March 2016

Keywords:
Risk-based inspection
Portfolio decision analysis
Imprecise information

ABSTRACT

In this paper, we present a novel risk-based methodology for optimizing the inspections of large underground infrastructure networks in the presence of incomplete information about the network features and parameters. The methodology employs Multi Attribute Value Theory to assess the risk of each pipe in the network, whereafter the optimal inspection campaign is built with Portfolio Decision Analysis (PDA). Specifically, Robust Portfolio Modeling (RPM) is employed to identify Pareto-optimal portfolios of pipe inspections. The proposed methodology is illustrated by reporting a real case study on the large-scale maintenance optimization of the sewerage network in Espoo, Finland.

1. Introduction

Large infrastructure networks, such as gas or water pipelines, are subjected to preventive renovation and condition inspection programs which account for a significant portion of the network operating costs [41,42]. The optimization of inspections is therefore fundamental for the efficient management and competitiveness of these complex networks. Information about the current condition of the network items is needed for developing the optimal renovation program; however, in practice, the actual conditions of network items such as pipes can be determined only approximately through inspections that can be very costly, especially in the case of large underground networks.

This calls for the optimization of renovation planning, which can be seen as a two-step process:

(i) identification of an optimal set of inspections of the network items whose subsequent renovation actions (if necessary) can be expected to reduce network-related risks most while reducing the cost of expected negative consequences as much as possible;

(ii) assessment by inspection of the degradation state of the network items in the selected portfolio and optimal planning of maintenance actions for the whole network.

In this paper, we develop a novel risk-based methodology for addressing the first issue, whereas the second issue is left for future research. The methodology has been motivated by and developed in the context of a real case study.

Although there are several definitions for risk (e.g., see [3,4,18] for reviews and comparisons), in maintenance engineering it has always been viewed as a combination of two attributes: *likelihood* (i.e., a description, even rough, of the uncertainty in the occurrence of the failure event) and *severity* (i.e., a quantification of the impact of the failure on properties, environment, safety, production, etc.) [17].

The idea of optimizing maintenance actions on the basis of a risk evaluation in view of likelihood and severity dates back to the 1980s, when the American Petroleum Institute (API) started the Risk-Based Inspection (RBI, [7,16,25]) project whose aim was to define a procedure for prioritizing and managing the efforts of an inspection program. In this procedure, resources are allocated to provide a higher level of coverage to high-risk items while maintaining an adequate effort on lower-risk equipment [14]. This methodology has become popular also in the nuclear industry (e.g., [37]) in which Probabilistic Risk Assessment (PRA) is used for maintenance prioritization: the more a given maintenance action

* Corresponding author. Tel.: +358 50 383 0636
E-mail address: ahti.salo@aalto.fi (A. Salo).

http://dx.doi.org/10.1016/j.ress.2016.03.011
0951-8320/

on a basic event can reduce the overall plant risk, the higher the priority of this action.

Later, especially after the year 2000, Risk-Based Maintenance (RBM, [6]) has gained popularity with the inclusion of risk-based inspection within the Reliability Centered Maintenance (RCM) paradigm and the Condition-Based Maintenance (CBM) strategies [1,20,29,36]. Subsequently, it has been applied in different industrial contexts (e.g., [1]), including critical infrastructures. For example, RBM models have been developed by Dey [10,11] for oil and gas pipelines by using the Analytic Hierarchy Process (AHP) [28] to guide the allocation of maintenance resources on the most risky pipeline stretches. However, the AHP method suffers from limitations such as the rank reversal phenomenon (i.e., the relative ranking of two alternatives may change when a new alternative is introduced), shortcomings of the 1–9 ratio scale, and pitfalls in quantification of qualitatively stated pairwise comparisons [30]. Moreover, the methodology proposed in [13,14] does not tackle the problem of how to optimize the inspection campaign, which, as a topic, has been addressed by researchers who have built RBI plans for wastewater networks (e.g., [6,18]).

Hahn et al. [18] proposed an approach to RBI based on Bayesian Belief Networks (BBN) for prioritizing the sewerage inspections (i.e., the domain of the case study discussed in this work). The model accounts for the uncertainty in the expert beliefs. However, the resulting decision recommendation considers neither the uncertainty in the state of the pipe nor any budget constraint. Moreover, it does not account for possible project interdependencies (e.g., cost synergies of checking pipes in the same region) and constraints concerning portfolio balance (e.g. to ensure that portfolios contain sufficiently many pipes with different characteristics).

A Multi-Objective Genetic Algorithms (MOGA, [8,12]) has been developed in [5] to identify the set of Pareto-optimal inspection programs. Network items are ranked based on how many times they are selected by the multi-objective algorithm to create an archive of "optimal" inspection policies. Although the selection of the items with the highest selection frequency approximately maximizes the expected number of correct item choices [26], this methodology for prioritizing network item inspections lacks a sound theoretical justification. Furthermore, the solution can be heavily dependent on the algorithm settings (e.g., number of generations, mutation rates, etc.). As a result, the Decision Maker (DM) cannot be sure that the proposed final solution belongs to the set of optimal solutions. Finally, this methodology is not able to deal with uncertain and imprecise information.

Against these backdrops, we propose a rigorous methodology for the optimal targeting of inspection activities in a generic underground network, with the aim of maximizing the aggregate value of these inspections as achieved through their contribution to risk reduction, subject to budget constraints and the presence of possible interdependencies among inspections and uncertainties about the model parameters. Our methodology combines aspects of Robust Portfolio Modeling (RPM, [23,24,26]) with the dynamic modeling approach [34] which uses multi-attribute value functions to model preferences on the quality distributions of assets and provides guidance for the optimal allocation of maintenance resources at the Finnish Road Administration. In particular, our methodology accommodates qualitative expert judgements about the risk of network items.

Our risk-based methodology for prioritizing network item inspections consists of two steps:

1. Rank all items of the network based on their risk level.
2. Select optimal portfolios of inspections among the items that have been ranked highest.

The separation of the two parts is motivated by practical reasons: the direct application of the procedure at the second step to all the items would require an excessive computational effort. Nonetheless, in the case of large networks, the number of risky items selected at step 1 is typically in the order of thousands and searching such a large search space is not computationally feasible. Thus, we have implemented the non-exhaustive search of the algorithm proposed by Mild et al. [26] to determine a large subset of optimal portfolios.

The proposed approach is able to guide risk-based inspection planning based on rough field data and qualitative statements from experts who have knowledge about the pipe degradation process as well as the risk scenarios caused by pipe failures. Alternatively, model-based risk estimates can be derived through analytical approaches and associated models. However, such models involve parameters whose values are usually not precisely known and may have to be fine-tuned on case-by-case basis; moreover, the more advanced analytical approaches also require model simulation [38]. In this sense, one advantage of our approach is that it offers a viable compromise between the need to incorporate sound risk estimates based on field data about the physical phenomena and the need to build a parsimonious model for the risk assessment of a very large number of maintenance items.

We also note that this methodology for identifying optimal portfolios of risk-based inspection programs is generic in that it can be applied to different types of underground networks (gas, water, wastewater, etc.). We illustrate this methodology by reporting a real case study in which it was applied to a large sewerage network in Espoo, Finland.

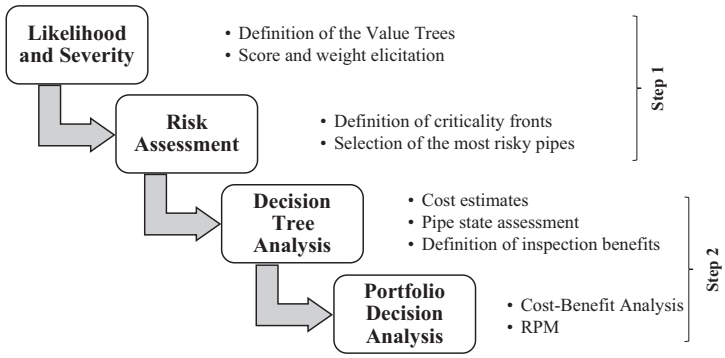


Fig. 1. Methodology snapshot.

The rest of the paper is structured as follows. Section 2 presents the methodology, focusing on risk identification, risk value trees definition and risk assessment in its first section, and describing the methodological steps to assess the inspection benefits and, on this basis, select the cost efficient inspection portfolios, in the second section. Section 3 presents the case study and describes the process and outcomes of eliciting statements by experts to build the value trees. Finally, Section 4 concludes the paper and outlines extensions for future research.

2. Overview of the methodology

Our approach builds on Multi-Attribute Value Theory (MAVT, [16,23]), which is a systematic methodology for evaluating decision alternatives with regard to multiple objectives. In MAVT, these objectives are operationalized by defining corresponding attributes which have performance scales for measuring the performance of alternatives. In our paper, the alternatives are network items which are evaluated with regard to the two main objectives of impacting most the likelihood of failures and contributing most to the severity of failure consequences, in order to establish inspection priorities. Each subset of these network items is called a "portfolio".

Fig. 1 summarizes the two-step risk-based methodology proposed for prioritizing item inspections in the presence of incomplete knowledge. The steps are detailed in next sections.

2.1. Rating of network items based on risk

In the proposed MAVT-based framework, the risk-based rating of network items has two main objectives:

1. Identify items which are most likely to fail.
2. Identify items whose failure has the most severe consequences.

For each objective, a team of experts analyzes which attributes contribute to failure likelihood and severity. These attributes are structured as a hierarchy when the overall objective (i.e. failure likelihood and failure severity) is decomposed into subobjectives until the lowest level of the hierarchy, which contains attributes with regard to which the alternatives can be meaningfully evaluated [19]. In particular, the hierarchy provides the DM with an overall view of the relationships between the different subobjectives and facilitates the assessment of the relative importance of objectives on each level. The decomposition proceeds until the experts agree that attributes do not need to be further disaggregated. The attributes at the lowest level of the hierarchy are called leaf attributes. For example, in the value tree for the objective of impacting most the likelihood of failure, the leaf attribute "Material" of a pipe has several material quality classes so that a pipe matches one of the following: "PVC", "cast iron", "concrete", "polyethylene", "renovated with trenchless socks".

For simplicity, suppose that the value tree of failure likelihood is composed of two levels. Specifically, assume that the first level l_1 represents the failure likelihood $V_L(x^j)$ of alternative x^j and the second level l_2 includes the set of leaf attributes A_L of failure likelihood (the same approach is used to build the value tree of failure severity). Each alternative x^j is characterized by specific quality classes x_i^j for each attribute i. For example, a pipe is characterized by a specific material among "PVC", "cast iron", "concrete", "polyethylene" and "renovated by trenchless socks". Each of these quality classes is assigned a score $v_i(x_i^j)$, which is evaluated through a modified SWING procedure [40] so that the expert assesses the relative importance of different quality classes x_i^j in determining the failure likelihood. Specifically, the weakest material ("renovated by trenchless socks") is assigned score $v_i(x_i^j)=100$, whereas the most reliable one ("concrete") is assigned score $v_i(x_i^j)=0$: every other quality class is scored according to these two reference points, whereby scores $v_i(x_i^j)$ can alternatively be evaluated through interval valued scores so that $v_i(x_i^j)=[\underline{v}_i(x_i^j);\overline{v}_i(x_i^j)]$. For example, score $[60-80]$ is assigned to quality class "cast iron" given that its reliability is much closer to "concrete" than "renovated by trenchless socks". Once the quality classes of every attribute have been scored, each alternative x^j is fully defined by the set of interval-valued scores $v_i(x_i^j)$ of the quality classes that characterize that alternative. Thus, the values of failure likelihood $V_L(x^j)=\left[\underline{v}_L(x^j);\overline{v}_L(x^j)\right]$ are calculated as the intervals

$$\underline{v}_L\left(x^j\right)=\min\left[\sum_{i\in A_L} w_i \underline{v}_i\left(x_i^j\right)\right] \tag{1}$$

$$\overline{v}_L\left(x^j\right)=\max\left[\sum_{i\in A_L} w_i \overline{v}_i\left(x_i^j\right)\right] \tag{2}$$

where w_i represents the weight of attribute i.

In this context, weights w_i are specified by the experts who may give imprecise preference statements about attributes such as "attribute $i\in A_L$ is more important than attribute $i'\in A_L$ which in turn is more important than attribute $i''\in A_L$". These preference statements imply weight constraints that limit the set of feasible weights. In the previous example, the imprecise statements lead to the weight constraints $w_i\geq w_{i'}\geq w_{i''}$ so that the feasible weight set consists of the extreme points $(1\ 0\ 0);(\frac{1}{2}\ \frac{1}{2}\ 0);(\frac{1}{3}\ \frac{1}{3}\ \frac{1}{3})$ and their convex combinations. Under mild assumptions, which are here fulfilled, the maximum and minimum values of Eqs. (1) and (2) are attained at the extreme points of the feasible weight set [35].

In value trees with multiple levels, the calculation of Eqs. (1) and (2) is propagated throughout the hierarchical structure until the topmost objective (i.e. failure likelihood or failure severity) is reached. The definition of failure likelihood and failure severity of each alternative x^j is based on the extension [32] of the PAIRS method [31], which admits imprecise preference statements about attributes. Specifically, PAIRS solves linear problems of Eqs. (1) and (2) at level l_h to identify the interval-valued scores at the next higher level l_{h-1}, and the computations are then repeated until the topmost objective of the value tree is reached. Note that Eqs. (1) and (2) are based on the assumption that the leaf attributes are mutually preferentially independent [15] which can usually be guaranteed by structuring the problem so that the contribution of a higher score on some leaf attribute to the overall performance does not depend on what the performance levels on other leaf attributes are.

Note that every item is characterized by a quality class for each leaf attribute. For instance, a pipe is characterized by a specific material, a specific diameter, etc. Thus, the score elicitation is applied to the quality classes of every leaf attribute so that the overall values of failure likelihood and failure severity of every pipe can be estimated once the pipe quality classes of every leaf attribute have been assessed. As a result, the calculation of failure likelihood and failure severity values does not take much computation time even if the number of items is large.

In the risk assessment part of the methodology, the aim is to identify the most critical network items with respect to failure likelihood and failure severity. These items form the Pareto optimal set, because they are not dominated by any other item, i.e., another item with a greater failure likelihood will have a lower failure severity or vice versa.

However, this concept of dominance needs to be extended for our analysis, because the overall values of both likelihood and severity are intervals (V_L and V_C, respectively). That is, for interval

scores, item x^j is said to dominate item x^k ($k \neq j$) if and only if the intervals $V_L(x^j)$ and $V_C(x^j)$ both lie above $V_L(x^k)$ and $V_C(x^k)$, respectively

$$x^j \succ x^k \leftrightarrow \left\{ \begin{matrix} \underline{v}_L(x^j) \geq \overline{v}_L(x^k) \\ \underline{v}_C(x^j) > \overline{v}_C(x^k) \end{matrix} \vee \begin{matrix} \underline{v}_L(x^j) > \overline{v}_L(x^k) \\ \underline{v}_C(x^j) \geq \overline{v}_C(x^k) \end{matrix} \right\} \quad (3)$$

This dominance definition allows us to identify the different Pareto-optimal frontiers F_i [9,19], where $i \in 1, 2, 3, \ldots$ represents the index of the non-dominated frontiers [10,12] and $|\bullet|$ indicates the dimension of the set.

On this basis, the items of the network can be compared to each other to identify those that have the highest failure likelihood and highest failure severity. In this respect, given the uncertainty in both the likelihood and severity values, the pairwise dominance concept of [32] is applied to select non-dominated items (i.e., the Pareto optimal set) in the two-dimensional space failure likelihood–failure severity. The second step of the analysis (i.e. portfolio optimization) is carried out on this reduced set F_1, containing the items which have been assessed to have the highest risk.

2.2. Portfolio optimization

The purpose of portfolio optimization is that of performing a cost-benefit analysis of the most critical network items with the aim of identifying the subset of those items whose inspection is expected to give the highest benefit in terms of reducing the cost of disruption.

The main goal is to make those inspection and renovation decisions that maximize the benefit-cost ratio of performing inspections in order to reduce expected disruption costs. We also account for the uncertainty in the direct and indirect costs associated to the pair of decisions, as well as the uncertainty in the actual degradation state of the pipe. In our setting, inspection plans are revised annually based on the available budget and the historical record of past inspection outcomes and maintenance actions. The prioritization of inspections is updated annually by relying on expert judgements, which, if needed, can also be elicited to revise the definition of the attributes and to adjust the weights.

Towards this end, we first build a decision tree model [16,23] to help experts decide whether an item needs inspection and whether or not it pays off to carry out maintenance actions on it. A decision tree shows the relationships between the decisions, the chance events that may occur, and the values that are generated through sequences of decisions and events. Probabilities are assigned to the chance events so that expected values are determined for each possible outcome.

For every network item in the previously selected set of risky items, the experts have two successive decisions to make:

1. Decide whether the item should be inspected. This decision tree is indicated by two branches corresponding to the two possible decisions: 'Yes' and 'No'.
2. If the item has been inspected, the next decision is whether or not to carry out renovation actions which may reduce the network disruption probability and consequently the expected severity of consequences. Otherwise, the indirect costs of not inspecting the item are considered (i.e., the expected disruption consequences). This second part of the decision tree is case-specific.

Consider the decision tree in Fig. 2, which is employed in the case study in Section 3. The DM first has to decide whether pipe x^j, $j \in F_1$ should be inspected to determine its degradation state (part 1 in Fig. 2). In this paper we employ a discrete, multi-state

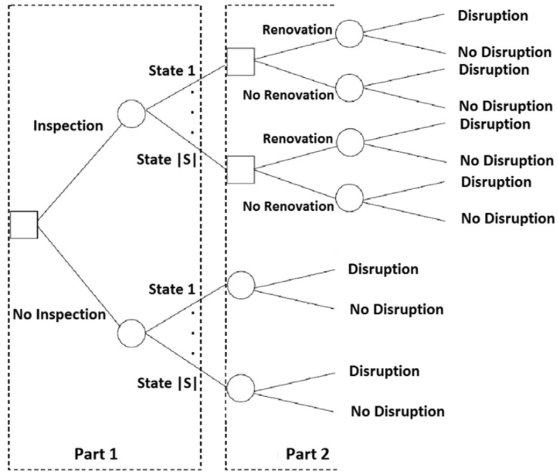


Fig. 2. Decision tree.

description of the degradation level of the network maintenance items, which is often the case in many industrial applications [22]. If no inspection is carried out, then the DM needs to associate with this decision the cost of indirect consequences. We assume that renovations are always preceded by item inspection, because it is not meaningful to carry out renovation activities without inspecting first. The expected value of disruption is calculated over the possible pipe degradation states (Fig. 2, bottom part). The more degraded the item state, the higher the probability of disruption.

If the item is inspected, the next decision is what renovation actions (part 2 in Fig. 2), if any, should be taken to improve the state of the items and, thus, to reduce the probability of disruption. In particular, items that have been renewed are all assumed as good as new, with disruption probability equal to that of the State 1.

To solve the decision tree, it is necessary to elicit case-specific probability and cost information which are attached to its branches.

Firstly, we need to estimate the probability of item x^j belonging to degradation state $s \in S = \{1, \ldots, \Sigma\}$. Here, different methodologies of probability elicitation can be employed, based on the available data and the specific case.

In our case, we considered the actual inspection outcomes on the J items and calculated the corresponding likelihood intervals $V_L(x^j) = \left[\underline{v}_L(x^j), \overline{v}_L(x^j)\right]$ derived from expert statements. Then, for every likelihood score $v_L = \{v_L \in \mathbb{N} | 0 \leq v_L \leq 100\}$, we selected all items x^j for which $v_L \in V_L(x^j)$. The resulting intervals were used to estimate the probability $p(s^j = s)$ of item x^j being in state $s \in S$. Namely, consider the interval $V_L(x^j)$ of likelihood values $v_L(x^j)$, then the probability $p(s^j = s)$ is

$$p(s^j = s) = \sum_{v_L \in v_L(x^j)} [p(s^j = s \,|\, v_L(x^j) = v_L) \bullet p(v_L(x^j) = v_L)], \quad (4)$$

where

$$p(s^j = s | v_L(x^j) = v_L) = \frac{|\{j \in \bigcup_\varphi F_\varphi | v_L \in V_L(x^j) \wedge s^j = s\}|}{|\{j \in \cup_\varphi F_\varphi | v_L \in V_L(x^j)\}|} \quad (5)$$

$$p(v_L(x^j) = v_L) = \frac{1}{\overline{v}_L(x^j) - \underline{v}_L(x^j)}, \quad (6)$$

if we assume a uniform distribution over the likelihood interval scores $v_L \in V_L(x^j)$. For simplicity, we only considered integer

likelihood values. This makes it possible to solve Eq. (4) as a sum rather than as an integral.

The disruption probabilities are contingent on the item states. To account for the corresponding uncertainty about disruption probability, experts were asked to estimate lower bounds $\underline{p}_s^d$ and upper bounds $\overline{p}_s^d$ of the disruption probability of each degradation state $s \in S$. As mentioned before, if the item is renovated, then the corresponding disruption probability is the one for the best State 1, i.e. $\left[\underline{p}_1^d,\ \overline{p}_1^d\right]$.

In addition, it is necessary to estimate (i) the disruption consequences, which are estimated as one number representing both direct and indirect costs $c_j^d = [\underline{c}_j^d; \overline{c}_j^d]$; (ii) the renovation costs $c_j^s = [\underline{c}_j^s; \overline{c}_j^s]$, $s \in S$ and (iii) the inspection costs $c_j^t = [\underline{c}_j^t; \overline{c}_j^t]$.

These parameters can be elicited as intervals defined by lower and upper bounds that are stated by the experts. Note that the choice of describing by intervals the uncertainty in the expert-estimated probability and consequence values is justified by the sake of generality of the proposed methodology. In fact, other approaches to represent uncertainty (e.g. by median and variance) would require more specific knowledge from experts, which is not always available. Note also that the interval-valued representation of uncertainty is compliant with non-probabilistic approaches to handle uncertainty, such as p-box and Dempster Shafer Theory of Evidence (e.g. [2,21]).

After the elicitation process, the analysis is based on the decision tree in Fig. 2 in which the goal is to select the optimal decision between committing or not committing renovation actions, which is applicable only when the item is inspected (top right part of the tree in Fig. 2). Specifically, we define the set $R = \{r^+, r^-\}$ such that $r = r^+$ stands for committing renovation actions while $r = r^-$ stands for not committing any renovation action.

The expected cost ϑ^{r_s} for action $r = r^+$ on item x^j in degradation state $s \in S$ is given by the sum of the actual cost for item renovation and the expected disruption cost in case of item renovation. Then, the interval of possible values of ϑ^{r_s} is given by

$$\underline{\vartheta}_j(r_s^+) = \left[\min\left\{c_j^d \cdot p_s^d\right\}\right] + \underline{c}_j^s = \underline{c}_j^d \cdot \underline{p}_1^d + \underline{c}_j^s \qquad \forall s \in S, j \in F_1 \tag{7}$$

$$\overline{\vartheta}_j(r_s^+) = \left[\max\left\{c_j^d \cdot p_s^d\right\}\right] + \overline{c}_j^s = \overline{c}_j^d \cdot \overline{p}_1^d + \overline{c}_j^s \qquad \forall s \in S, j \in F_1. \tag{8}$$

On the other hand, the expected cost ϑ^{r_s} for action $r = r^-$ on item x^j in degradation state $s \in S$ is given by the expected disruption cost, where the disruption probability is contingent to the item states

$$\underline{\vartheta}_j(r_s^-) = \left[\min\left\{c_j^d \cdot p_s^d\right\}\right] = \underline{c}_j^d \cdot \underline{p}_s^d \qquad \forall s \in S, j \in F_1 \tag{9}$$

$$\overline{\vartheta}_j(r_s^-) = \left[\max\left\{c_j^d \cdot p_s^d\right\}\right] = \overline{c}_j^d \cdot \overline{p}_s^d \qquad \forall s \in S, j \in F_1. \tag{10}$$

In the presence of incomplete information, the optimal alternative $r_s^*(x^j) \in R$, given that the item is in degradation state $s \in S$, is the one which minimizes the expected cost:

$$r_s^*\left(x^j\right) = \left\{\begin{array}{ccc} r^+ & \leftrightarrow & \overline{\vartheta}_j(r_s^+) < \underline{\vartheta}_j(r_s^-) \\ r^- & & \text{otherwise} \end{array}\right\} \qquad \forall s \in S, j \in F_1. \tag{11}$$

Note that renovation is an optimal decision only if the total costs of renovation are lower than the cost of not renovating. Thus, if the intervals overlap (i.e., there is no dominance structure), $r_s^*(x^j) = r^-$ is the preferred action in state $s \in S$.

For every possible state $s \in S$, we know the optimal decision $r_s^*(x^j) \in R$ for item x^j. To determine whether item x^j needs to be inspected, we consider the benefit from the inspection, which results from reduced cost of eventual disruption. That is, if the optimal choice in state $s \in S$ is not to renovate the item, then there is nothing to be gained from the inspection. On the other hand, if the optimal choice in state $s \in S$ is to renovate, then there is the benefit of reducing the expected disruption costs due to renovation.

From this, the benefit $B_j^s = [\underline{B}_j^s; \overline{B}_j^s]$ for item x^j in state $s \in S$ turns out to be an interval of values such that:

$$\underline{B}_j^s = \left\{\begin{array}{ll} 0, & \text{if } r_s^*(x^j) = r^- \\ \underline{\vartheta}_j(r_s^+) - \overline{\vartheta}_j(r_s^-), & \text{if } r_s^*(x^j) = r^+ \end{array}\right\} \tag{12}$$

$$\overline{B}_{j^1}^s = \left\{\begin{array}{ll} 0, & \text{if } r_s^*(x^j) = r^- \\ \overline{\vartheta}_j(r_s^+) - \underline{\vartheta}_j(r_s^-), & \text{if } r_s^*(x^j) = r^+ \end{array}\right\} \tag{13}$$

When the benefit for every state $s \in S$ has been assessed, the aggregate inspection benefit $B_j = [\underline{B}_j; \overline{B}_j]$ for item x^j is modeled as the weighed sum of the state benefits, whose bounds are

$$\underline{B}_j = \sum_{s \in S} p_j^s \cdot \underline{B}_j^s \qquad \forall j \in F_1 \tag{14}$$

$$\overline{B}_j = \sum_{s \in S} p_j^s \cdot \overline{B}_j^s \qquad \forall j \in F_1, \tag{15}$$

where $p_j^s = p(s^j = s)$ is the probability of item x^j being in state $s \in S$.

The decision tree provides useful insights for the next step of the renovation management process in which the decision is whether or not to perform renovation actions based on the inspection result. Specifically, from the decision tree of each item x^j, we determine the lowest item state $s_j^* \in S$ in which renovation is the preferred action

$$s_j^* = \min_{s \in S}\left\{s | r_s^*(x^j) = r^+\right\} \qquad \forall j \in F_1. \tag{16}$$

This helps the DM decide when to renovate, assuming that there is no uncertainty in the inspection outcomes. However, this decision also depends on the optimization of the renovation actions based on the inspection outcomes.

Finally, Portfolio Decision Analysis [33] is used to identify the cost efficient portfolios of item inspections. An inspection portfolio is cost-efficient if no other feasible portfolio gives a higher overall benefit B at a lower inspection cost c. Such portfolios can be determined from an optimization problem which has two objectives $T = \{c, B\}$, where the former is to be minimized and the latter maximized.

Given that costs and benefits are measures by intervals, we employ RPM ([23,24,26]) to identify efficient inspection portfolios. In RPM it is possible to incorporate network synergies and/or logic constraints among the inspection activities as well.

The optimization problem we are tackling is very complex, because the search space of the possible inspection portfolios contains $2^{|F_1|}$ solutions, with $|F_1| \gg 1$ (e.g., 2000). Consequently, the exact dynamic programming algorithms proposed in [23,24] are not applicable. We therefore use the extended RPM developed in [26].

In this approximate methodology, which is summarized in Appendix, we employ uniform distribution to draw weights $w \in S_w$ and random scores from $v \in S_v$, defined by

$$S_w = \{w \in \mathbb{R}^{|T|} | w^\tau \geq 0\ \forall \tau \in T, \sum_{\tau \in T} w^\tau = 1\} \tag{17}$$

$$S_v = \{v = [v^1; v^2] \in \mathbb{R}^{J^1 \times |T|} | v_j^1 \in \left[-\overline{c}_j^t; -\underline{c}_j^t\right], v_j^2 \in \left[\underline{B}_j; \overline{B}_j\right] \quad \forall j \in F_1\} \tag{18}$$

Note that the minus sign for v_j^1 is introduced to change the minimization problem into a maximization one.

In the RPM framework, an inspection portfolio $p \subseteq F_1$ is a subset of possible item inspections; thus, the set of all possible portfolios is the power set $P := 2^{F_1}$. The overall value of a portfolio is the sum of the overall values of its item inspections. For a given score matrix v and attribute weights w, the overall value of

portfolio p is

$$V(p,w,v) := z(p)\ v\ w, \tag{19}$$

where $z(\cdot)$ is a bijection $z{:}P \to 0,1^{|F_1|}$ such that $z_j(p)=1$ if $x^j \in p$ and $z_j(p)=0$ if $x^j \notin p$.

Under incomplete information about attribute weights and scores $\Upsilon = S_w \times S_v$, portfolio p dominates portfolio p' if p has an overall value greater than or equal to the one of p' for all feasible attributes weights and scores and strictly greater for some, i.e.,

$$V(p,w,v) \geq V(p',w,v) \text{ for all } (w,v) \in \Upsilon \tag{20}$$

$$V(p,w,v) > V(p',w,v) \text{ for some } (w,v) \in \Upsilon \tag{21}$$

Thus, a non-dominated portfolio is identified by maximizing the overall value $V(p,v,w)$ of the inspection portfolio $p \in P_F$ from the Integer Linear Programing Problem (ILP)

$$\max_{p \in P_F} \left\{ V(p,v,w) = z(p) v w \,|\, z(p) \in \{0,1\}^{|F_1|} \right\} \tag{22}$$

The set of feasible portfolios P_F is defined by a set of q linear inequalities, whose coefficients are recorded in matrix $A \in \mathbb{R}^{q \times |F_1|}$ and vector $U \in \mathbb{R}^q$ such that $P_F := \{p \in P | A \cdot z(p) \leq U\}$.

This procedure of sampling values of w and v, is repeated until a sufficient number of non-dominated portfolios have been identified. Hence, the output consists of portfolios, which are known to be potentially optimal, although the algorithm may not find all non-dominated portfolios very quickly.

To analyze the solutions provided by the algorithm, we consider the Core Index (CI) metric. Namely, the CI of item x^j represents the percentage of efficient portfolios which include inspection on that specific item x^j. When the CI of an item inspection is 1, then the item is included in all the identified efficient portfolios.

3. Case study

Helsinki Region Environmental Services Authority (HSY) provides water and wastewater services to one million customers. It was founded in 2010 through the merger of four separate water companies. Currently, this water utility is harmonizing its practices for network renovation, condition inspection and renovation planning.

The analyses in this paper are based on the large sewerage network in Espoo (a neighboring city of Helsinki) where there are more than 33,000 pipes with a total length of about 900 km. In this case study, we analyze a subset of $J = 6103$ pipes for which earlier inspection outcomes are available. This makes it possible to compare the results of our methodology with real inspection outcomes and to derive insights to calibrate the methodology. The analysis accounts for individual pipes, because the inspection and renovation decisions are typically made on this scale. However, the methodology could be applied on smaller scale network items as well, such as pipe length of one meter.

To support the effective management of the network, HSY has a database which contains the following information about every pipe:

- Pipe features: The ID code, installation year, location (in terms of spatial coordinates for both endpoints), diameter, type (gravitational or pressure sewer), renovation year (in case the pipe has been renovated) and material. The most common pipe material is concrete but some pipes are made of cast iron, polyethylene, PVC or they have been renovated by trenchless socks.
- Inspection results: The possible inspection year and outcome. For each inspected pipe, the inspection result is stored in the database together with the location and type of each defect that has been detected during inspection (e.g., slump, hole, tree roots, pile-up).
- Maintenance history: The number of blockages and flushing events.
- External context of the pipe: Other significant information related to the surrounding environment in which the pipe is located (i.e., buildings, traffic load, groundwater areas, and soil type).

In this case study, the methodology was tested using statements from one expert only. Further research will focus on incorporating the expertise of a group of experts, such as utility employees [39].

3.1. Failure likelihood and severity

A well-founded risk analysis forms the basis of the risk-based maintenance methodology [27], which, in this case, helps understand the risks associated with pipes by encoding expert statements about the likelihood and consequences of failures.

Fig. 3 shows the hierarchical objective structure of failure likelihood, identified by expert interviews. The attributes on the second level are:

- Pipe features: Pipe-specific characteristics, such as pipe material, age since last renovation and diameter are important determinants of failure likelihood.
- Past events: This attribute is relevant because it comes from the consideration that the larger the number of past blockages and flushing, the higher the probability of failures in the near future.
- Local circumstances: The elements of the surrounding environment can significantly contribute to the failure likelihood. In our case study, soil type and traffic load were considered the most important factors by expert judgement.

The weights were elicited with the PAIRS method [31]: for every objective at the second level, l_2, of the hierarchical tree, the attributes were ranked according to expert assessment on how important determinants of failure likelihood they were. The attribute 'Local circumstances' was reported to be the least important for failure likelihood, with no preference between 'Pipe Features' and 'Past Events'. These statements correspond to the following inequalities on attribute weights

$$w_{pipe\ features} \geq w_{local\ circumstances} \tag{23}$$

$$w_{past\ events} \geq w_{local\ circumstances}, \tag{24}$$

which, together with the constraint that the weights have to sum to 1, define the feasible region which contains the weight vector $(w_{pipe\ features}, w_{past\ events}, w_{local\ circumstances})$.

When evaluating the importance of the attributes on the third level, l_3, with regard to those at the second level, l_2, the expert stated that:

- 'Diameter' is the most important sub-indicator among those of the pipe features–the smaller the diameter, the higher the failure likelihood.
- The number of past 'Blockages' is more important than the number of past 'Flushings'.
- 'Soil' is as important as 'Traffic Load'.

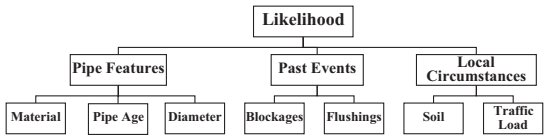


Fig. 3. Likelihood attribute hierarchical structure.

On the other hand, the consequence tree is a hierarchical representation of the conditions which define how severe impacts pipe failures have on properties, environment, and safety and how possible network malfunctions affect water consumers. In principle, the same methodology for assigning a likelihood value to the pipes could be adopted to evaluate the severity values. However, in this study, we derived these estimates from recent results on the evaluation of consequences mainly based on pipe location and surroundings as well as the estimated annual pipe specific sewage flow [21].

A severity value was assigned to each pipe based on the conditions in Table 1. A pipe was assigned to Class 1 only if it met at least one of the conditions 1–8; otherwise, if the pipe met one of the conditions 9–19, it was assigned to Class 2. The other pipes were assigned to the third class.

The SWING methodology [40] was applied to elicit scores by rating the pipes on each leaf attribute. For each attribute, the best measurement value (i.e., the one impacting the failure likelihood or severity the most) and the worst one (i.e., the one impacting the failure likelihood or severity the least) were assigned rates 100 and 0, respectively. Reminding the example of Section 2.1, for the leaf attribute 'Material' in the failure likelihood tree, the most reliable material is "concrete", while the least reliable material is "renovated by trenchless socks": these two have ratings 100 and 0, respectively.

Next, elicitation questions were posed by first mapping out expert opinions on ordinal preferences for quality differences. Specifically, the expert was asked which 'swing' from a specific attribute value to the best one would result in the largest improvement, the second largest improvement, etc. Again using the 'Material' attribute as an example, the answers to these questions led to the following ranking in ascending order: "concrete", "polyethylene", "cast iron", "PVC" and "renovated by trenchless socks".

Finally, the intermediate quality classes were evaluated with the extreme values and, for validation, with respect to each other, too. For example, one of the questions for the 'Material' attribute was: "Is the quality difference between cast iron and concrete pipes more or less significant than that between PVC and cast iron pipes?". The criticality of cast iron pipes is closer to concrete pipes than pipes renovated by trenchless socks, therefore, its interval score is closer to 0 (criticality score of concrete pipes) than 100 (criticality score of pipes renovated by trenchless socks).

In this way, interval scores were assigned to each class: after being recorded into an Excel file, they were adjusted and validated. By this procedure, an interval cardinal score in the range of $0-100$ was assigned to each leaf attribute class of the failure likelihood tree based on expert opinion.

Failure severity was evaluated for each pipe in view of the conditions in Table 1, which lists them according to their level of severity. For example, a pipe disruption close to a railway is more severe than a pipe failure near a beach. For this reason, the interval score of the former pipe is larger than that of the latter.

These critical conditions, then, were assigned uncertain ratings by applying the SWING procedure. Specifically, zero score was assigned to pipes of class 3, whereas a score of 100 was assigned to the most critical condition in class 1 (no. 8: "Very high pipe-specific sewage flow"). The remaining 18 intermediate conditions of severity conditions were evaluated by comparing the two extreme conditions and the other elicited ratings, which resulted in score intervals. This way, interval scores in the range of $0-100$ were identified for all intermediate conditions by expert opinion.

Alternative overall value $V_L(x^j)$ was determined following the procedure detailed in Section 2.1, so that the uncertainty with the score intervals of the leaf attributes was propagated through the likelihood value tree. The overall value $V_L(x^j)$ of failure likelihood was obtained per each pipe $x^j, j \in J$.

Table 1
Conditions used for evaluating the pipe-specific criticality classification for sewerage pipes [25].

	Class 1	Disruption cost estimate
1	Undoubled pressure pipes from critical pump stations	40,000€
2	Main tunnels	50,000€
3	Sewer mains and pressure sewers that are within significant groundwater areas	40,000€
4	Sewers close to primary or secondary raw water resources	30,000€
5	Pipes under railways	24,000€
6	Pipes under significant roads	35,000€
7	Sewer mains of crucial functional importance for the whole network	50,000€
8	Very high pipe-specific flow	50,000€
	Class 2	
9	Sewer mains not included in Class 1	30,000€
10	Sewers in protected areas/nature conservation areas	10,000€
11	Pipes crossing main water tunnels	24,000€
12	Pipes going under a water body (river, lake, sea)	35,000€
13	Pipes under buildings	40,000€
14	Pipes close to protected ditches	14,000€
15	Pipes close to swimming beaches	10,000€
16	Pipes other than sewer mains which are within significant groundwater areas	30,000€
17	Sewer mains within groundwater areas of less significance	24,000€
18	Sewers close to critical underground structures (e.g. subway)	20,000€
19	High pipe-specific flow	30,000€
	Class 3	
20	Every remaining pipe	10,000€

On the other hand, the severity overall value $V_C(x^j)$ was determined by the interval scores of the critical conditions that pipe x^j met. As in the paper by Laakso et al. [21], it was assumed that the pipe belonged to more than one condition and, then, the most critical one met by that pipe was considered.

3.2. Risk assessment

Risks were assessed by accounting for pipe overall values in the two-dimensional space failure likelihood–failure severity. That is, we first selected the $|F_1| = 2079$ non-dominated solutions among the $J=6103$, which belonged to the first Pareto front F_1 (circle marker and solid line in Fig. 4) in the remaining set. This procedure was applied until the set of remaining non-dominated solutions was empty. In the case study of Espoo sewerage system, three Pareto frontiers were identified; the third, F_3, is marked by squares in Fig. 4. The three frontiers indicate three different levels of criticality, which are defined according to the dominance relations between the pipes, as detailed in Eq. (3). In particular, the first Pareto frontier represents the set of most critical pipes, on which we focus the following analysis.

3.3. Decision tree

In order to identify optimal inspection strategies, we accounted not only for the actual inspection costs but also for the expected costs of future renovation actions or consequences of possible failures, given that the expected total pipe inspection cost depends on two decisions: whether or not to inspect, and whether or not to renovate.

To estimate the inspection costs in this situation, we used decision tree modeling [13,19].

The condition data input in this case study consisted of the CCTV inspection results which included information on several types of defects found in inspected pipes. For simplicity, the defect scores were aggregated into 6 states for each pipe, denoted by $s \in S = \{1;2;3;4;5;6\}$. The inspection results in Fig. 5 indicate the states of the inspected pipes as determined in the past inspections; the dash-dot lines in Fig. 5 represent the thresholds that map the underlying states of the HSY model into the 6 states considered in the case study.

In Fig. 5, we map the failure likelihood values (abscissa) onto the most significant percentiles (i.e., 5th, 50th and 95th) of the pipe states upon inspection. Specifically, for each value of likelihood v_L, we consider the subset of pipes x^j, $j \in J$ whose estimated likelihood value interval $V_L(x^j)$ includes v_L. The distribution of the degradation states at inspection of the pipes in such subset is summarized by its 5th, 50th and 95th percentiles, which are shown in Fig. 5 by squares, circles and diamonds, respectively.

The resulting statistics, which are summarized by their most significant percentiles in Fig. 5 (i.e., 5th, 50th and 95th), were used to estimate the probability $p(s^j = s)$ of the most critical pipes, as discussed in Section 2.2. Note that the most valuable information arises from high likelihood scores, given that our analysis focuses on the most risky pipes.

Fig. 6 summarizes the information available in the HSY dataset. Specifically, Fig. 6 shows the probability of a generic pipe being in state $s \in S$ given a specific value of failure likelihood (abscissa). The calculation of these probabilities (see Section 2.2) is based on the results of the past pipe inspections as recorded in the HSY dataset.

The probability of low degradation states decreases as the likelihood estimated by expert opinion increases, and the probability for the highest degradation states becomes larger with increasing level of estimated failure likelihood. The correspondence for State 4 and State 5 is not strong, partly because there are few pipes in these degradation states. As more condition inspections will be carried out, the growing dataset is expected to reveal a clearer connection between estimated failure likelihood and state probability.

Based on the above analysis and the information elicited from expert views (knowledge and information resulting from experience and past events), the link was established between the degradation state of the pipes and the probability of disruption (Table 2).

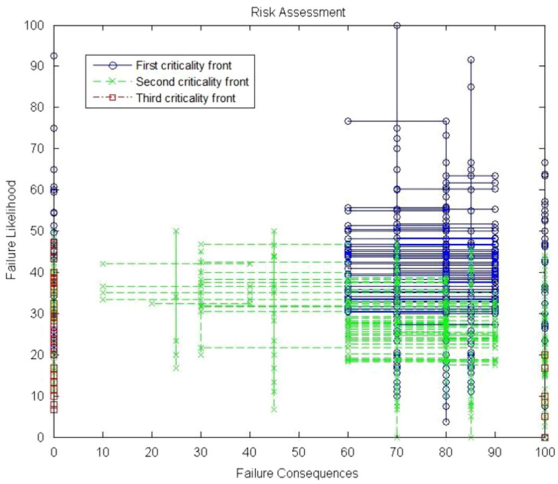


Fig. 4. Overall values of failure likelihood and severity of the 6103 pipes considered in the Espoo sewerage system.

Estimates of disruption costs were provided by the expert for each identified critical condition in Table 1, whereby both direct and indirect costs were taken into account. From these estimates, we calculated for each pipe x^j the expected disruption cost $c_j^d = [\underline{c}_j^d; \overline{c}_j^d]$ as the sum of the costs of the critical conditions it meets.

Estimates of both inspection costs c^t and renovation costs c^s were based on the length of each pipe (Table 3). Renovation costs can be contingent to the pipe states, but for the sake of simplicity we assumed the pipe replacement is always preferable to trenchless rehabilitation or patch repair. Note that rehabilitation and repairing techniques can be included in the decision process by increasing the complexity of the model.

Finally, the inspection benefits $B_j = [\underline{B}_j; \overline{B}_j]$ for each pipe x^j were determined by following the procedure explained in Section 2.2.

Thus, from the decision tree of each pipe x^j we determined the lowest pipe state $s_j^* \in S$ in which renovation becomes the dominant solution. Fig. 7 shows the distributions of $s_\varphi^* = \left\{ s_j^* \in S | x^j \in F_\varphi \right\}$, $\varphi = 1$, 2, 3, where F_φ represents the set of pipes belonging to the φ-th risk-based Pareto frontier and the additional pipe state 0 refers to the pipes for which renovation is never a dominant alternative, not even in case the pipe is in the worst condition state ($s = 6$).

From Fig. 7, one can note that large ranks of risk-based Pareto frontiers correspond to large portions of pipes for which the renovation is not worthwhile. In the case of the least critical pipes (third Pareto frontier in Fig. 4), the percentage of these pipes is more than 90%.

As can be expected, the portion of pipes in state 1 is always 0. This is due to the fact that there is no benefit from renovating a pipe in state 1, as this action does not improve pipe condition.

3.4. Results

The implementation of the approximate RPM accounted for the inspection benefits $B_j = [\underline{B}_j; \overline{B}_j]$ and costs $c_j^t = [\underline{c}_j^t; \overline{c}_j^t]$, for each pipe x^j. To identify the set of feasible inspection portfolios, the expert estimated the maximum yearly budget for inspections to be 300,000€ and indicated that there is a need to inspect at least 40 km of pipelines per year.

With respect to the approximate RPM algorithm, its termination condition was set as the convergence of the projects' Core Indexes. More specifically, the algorithm was set to stop when the difference of each project CI among the last 1000 iterations was lower than 1%. With this setting, the RPM algorithm provided more than 2000 efficient solutions in approximately 30 min (6529 iterations). Fig. 8 presents the CIs of the 2079 critical pipes (i.e., selected by risk assessment (Section 2.1)).

Recognizing that it can be difficult to choose from the set of non-dominated portfolios, the choice of the portfolio could be determined according to appropriate decision rules such as the *maximin* rule, which recommends the portfolio that yields the highest minimum overall benefit, or the *minimax-regret* rule, which recommends the action for which the worst case overall benefit difference is the smallest compared to the other portfolios. These rules coincide with the absolute robustness and robust deviation measures, respectively, in robust discrete optimization [24]. The results of decision rules depend on the set of non-dominated portfolios. This emphasizes the importance of finding as many non-dominated portfolios as possible.

Finally, as stressed in [23,24], one way to limit the number of optimal portfolios is to reduce the uncertainty in the expert preference statement and estimation and to choose appropriate constraints (positioning, strategic, budget, etc.) to limit the search space. In this respect, the continuous updating of inspection and

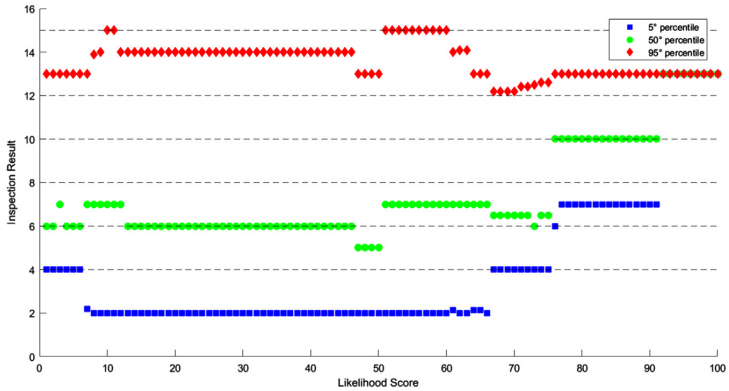


Fig. 5. Mapping between likelihood scores and past inspection results. (For interpretation of the references to color in this figure, the reader is referred to the web version of this article.)

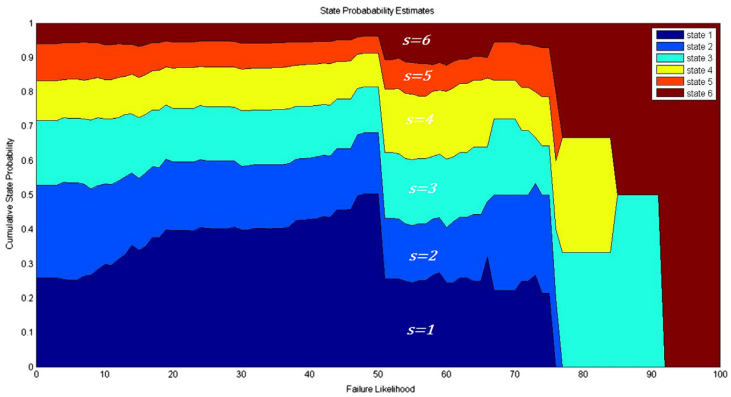


Fig. 6. Correspondence between failure likelihood and degradation state probability.

Table 2
Disruption probabilities for every degradation state: lower and upper bounds.

Degradation state	$\underline{p}_s^d$	$\overline{p}_s^d$
$s=1$	0	0.3
$s=2$	0.3	0.5
$s=3$	0.4	0.6
$s=4$	0.5	0.7
$s=5$	0.6	0.8
$s=6$	0.7	0.9

Table 3
Direct inspection and renovation costs, expressed in euro per meter.

Cost estimates	Lower bound [€/m]	Upper bound [€/m]
$[\underline{c}^t; \overline{c}^t]$	5	5
$[\underline{c}^s; \overline{c}^s]$, $s=1,\ldots,6$	343	370

maintenance data on the HSY network will reduce uncertainties in the model parameters and therefore lead to more conclusive results.

4. Conclusions

We have developed a risk-based inspection methodology for large infrastructure networks and described its application to the underground sewerage network in Espoo, Finland. The risk assessment based on failure likelihood and failure severity helps identify the most critical pipes among which the optimal portfolios of inspections can be found.

Another clear advantage of the methodology is that it allows for iterative improvement. Expert judgements may be biased or erroneous, especially regarding factors which have an impact on pipe states. This can lead to suboptimal pipes being included in the final portfolio for inspections. However, as inspections are carried out annually, the validity of decision attributes can be evaluated recurrently and modified if necessary.

Moreover, our methodology is capable of handling incomplete information by the use of SWING weighting, decision tree modeling and RPM. In particular, it accommodates incomplete information about state probabilities. In this respect, other ways to estimate the state probabilities are possible, such as logit regression or clustering. These will be investigated in future work.

In this case study on the underground sewerage network in Espoo, the large number of critical pipes in the network gives rise to a huge search space of inspection portfolios. Therefore, it is useful to perform the pipe risk assessment before the portfolio analysis. On the other hand, even if the set of pipes is reduced, there are still computational challenges in finding all solutions. Therefore, future research will focus on investigating the capability

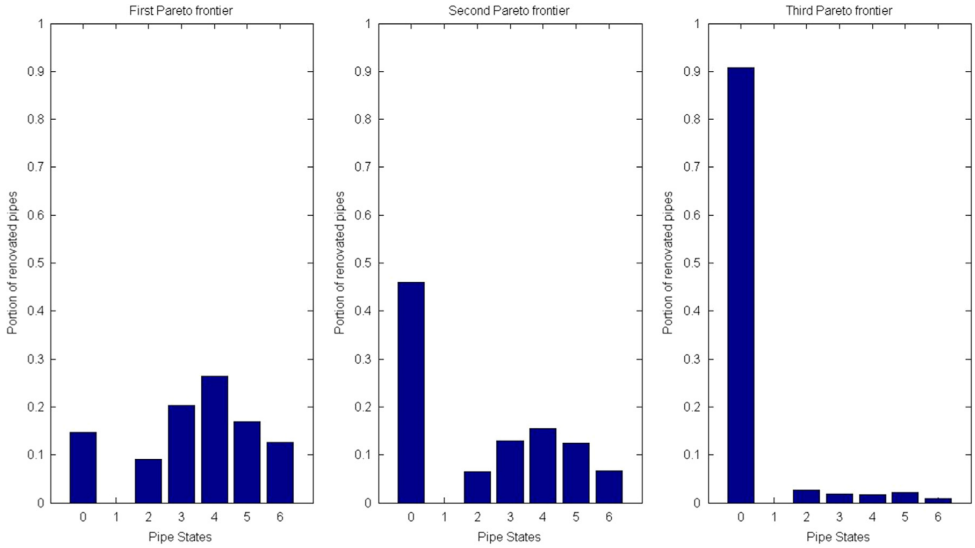


Fig. 7. Renovation policy.

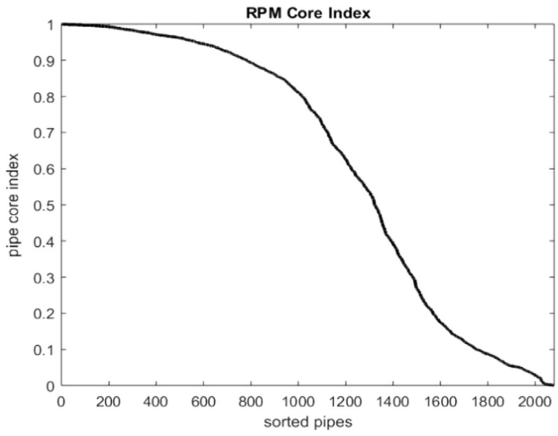


Fig. 8. RPM sorted Core Indexes of the most critical pipes.

of other algorithms in exploring large search spaces and in comparing its performance to that of RPM. Finally, future work will also focus on the definition of optimal renovation actions after pipe inspections, eventually avoiding the assumption of independence among pipe failures.

The proposed methodology can potentially be adapted for optimizing the inspections of other types of networks, such as gas distribution networks. In the future, we plan to investigate how the methodology can be extended to other systems by modifying the parameters affecting failure likelihood, failure severity as well as the costs of inspections and renovation actions.

Acknowledgements

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

Appendix

Approximate computation of Non-Dominated Portfolios in RPM ([26])

Let $V^u=[V_1^u, V_2^u]$ denote a utopian vector that sets strict upper bounds for the overall value of feasible portfolios in the extreme points $w_{ext}^{T=c^t}=[1,0]$ and $w_{ext}^{T=B}=[0,1]$ of S_w, such that:

$$V_\tau^u > \max_{p\in P_F}[V(p, w_{\text{ext}}^\tau, \overline{v})]\ \forall \tau \in T$$

where $\overline{v}=[-\overline{c}, \overline{B}]$.

The weighted max-norm distance of a portfolio p to the utopian vector is:

$$d(p,\mu,v)=\max_{\tau\in T}\left[\mu_\tau\left(V_\tau^u - V(p,\ w_{\text{ext}}^\tau,\ v)\right)\right]=\max_{\tau\in T}\left[\mu_\tau\ V_\tau^u-\mu_\tau\ z(p)\ v\ w_{\text{ext}}^\tau\right]$$

where $\mu\in M=\{\mu\in\mathbb{R}^2|\mu_\tau\geq 0, \sum_{\tau\in T}\mu_\tau=1\}$ and $v\in S_v$. With given $\mu\in M$ and $s\in S_v$ the set of feasible portfolios that minimize the distance to the utopian vector and are not dominated by another portfolio within the equal distance, is:

$$P_Q(\mu,v)=\{p'\in \arg\min_{p\in P_F} d(p,\mu,v)|\nexists p''\in \arg\min_{p\in P_F} d(p,\mu,v) s.t. p''\succ_S p'\}$$

where $S=S_v\times S_w$.

The set of portfolios $\arg\min_{p\in P_F}[d(p,\mu,v)]$ is obtained by solving the MILP problem

$$\min_{p\in P_F} d(p,\mu,v)=$$

$$\min_{\substack{z(p)\in\{0,1\}^{|\cdot|}\\ \Delta\in R}}\left\{\Delta\,|\,\Delta\geq\mu_\tau\ V_\tau^u-\mu_\tau\ z(p)\ v\ w_{ext}^\tau\ \ \forall\tau\in T,\ Az(p)\leq U\right\}$$

Portfolios in $P_Q(\mu,v)$ are non-dominated for any $\mu\in M$ and $v\in S_v$, and any non-dominated portfolio belongs to $P_Q(\mu,v)$ for some $\mu\in M$ and $v\in S_v$ (proof presented in [26]).

The algorithm that identifies a set of non-dominated portfolios $\hat{P}_N\subseteq P_F$ can be formulated as follows:

1. **Initialization.** Construct the utopian vector V^u as explained previously. Set $\hat{P}_N\leftarrow\varnothing$.
2. **Computation.** Repeat until enough non-dominated portfolios have been found:
   a. Generate random $\mu\in M$ and $v\in S_v$.

b. Determine $\arg\min_{p \in P_F} [d(p, \mu, v)]$.
c. Define $P_Q(\mu, v)$.
d. Set $\hat{P}_N \leftarrow \hat{P}_N \cup P_Q(\mu, v)$.

There are several methodologies for specifying the termination condition for the Computation loop consisting of steps 2a–2d. One methodology is tracking the number of new non-dominated portfolios found per iteration and, then, terminate the loop if, for instance, no new non-dominated portfolios have been found in the last 100 iterations. Another methodology is to compute the projects' Core Index values at each iteration based on the set of portfolios $\hat{P}_N$ and then terminate the loop when these values stabilize.

Generating values for scores and the max-norm weights in Step 2a can be implemented by considering systematic grid of values or by randomly choosing these values from suitable distributions. In this work, we have mainly relied on uniformly distributed weights within the simplex M and scores that have equal probability to be set to their lower or upper bounds per project.

Uniformly distributed max-norm weights are given by $\mu_\tau = \rho_\tau / \sum_\tau \rho_\tau$, where ρ_τ:s are drawn from an exponential distribution with expectation equal to one (Rubinstein, 1982).

References

[1] Arunraj NS, Maiti J. Risk-based maintenance – techniques and applications. J Hazard Mater 2007;142(3):653–61.
[2] Aven T. On the interpretations of alternative uncertainty representations in a reliability and risk analysis context. Reliab Eng Syst Saf 2011;96:353–60.
[3] Aven T. The risk concept – historical and recent development trends. Reliab Eng Syst Saf 2012;99:33–44.
[4] Aven T, Renn O. On risk defined as an event where the outcome is uncertain. J Risk Res 2009;12:1–11.
[5] Berardi L, Giustolisi O, Savić DA, Kapelan Z. An effective multi-objective methodology to prioritisation of sewer pipe inspection. Water Sci Technol 2009;60(4):841–50.
[6] Calixto E. Gas and oil reliability engineering, modeling and analysis. Gulf Professional Publishing; 2012.
[7] Calixto E. Integrated asset integrity management: Risk management, human factor, reliability and maintenance integrated methodology applied to subsea case. In: Safety and reliability of complex engineered systems – Proceedings of the 25th European safety and reliability conference; 2015. p. 3425–32.
[8] Deb K. Multi-objective optimization using evolutionary algorithms. Chichester: John Wiley & Sons, New York; 2001.
[9] Deb K, Agrawal S, Pratap A, Meyarivan T. A fast elitist non-dominated soring genetic algorithm for multi-objective optimization: NSGA-II. IEEE Trans Evolut Comput 2002;6(2):182–97.
[10] Dey PK. Analytic hierarchy process analyzes risk of operating cross-country petroleum pipelines in India. Nat Hazards Rev 2003;4(4):213–21.
[11] Dey PK, Ogunlana SO, Naksuksakul S. Risk-based maintenance model for offshore oil and gas pipelines: a case study. J Qual Maint Eng 2004;10(3):169–83.
[12] Fonseca CM, Fleming PJ. An overview of evolutionary algorithms in multiobjective optimization. Evol Comput 1995;3(1):1–16.
[13] French S. Decision theory: an introduction to the mathematics of rationality. New York: John Wiley & Sons; 1988.
[14] Galixto E. Gas and oil reliability engineering: modeling and analysis. 1st ed. Gulf Professional Publishing; 2007.
[15] Hahn MA, Palmer RN, Merril MS, Lukas AB. Expert system for prioritizing the inspection of sewers: knowledge base formulation and evaluation. J Water Resour Plan Manag 2002;128(2):121–9.
[16] Hassan J, Khan F. Risk-based asset integrity indicators. J Loss Prev Process Ind 2012;25(3):544–54.
[17] Helton JC, Johnson JD, Oberkampf WL. An exploration of alternative approaches to the representation of uncertainty in model predictions. Reliab Eng Syst Saf 2004;85:39–71.
[18] Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Anal 1981;1:11–27.
[19] Keeney RL, Raiffa H. Decisions with multiple objectives: preferences and value trade-offs. New York: John Wiley & Sons; 1976.
[20] Khan FI, Haddara MM. Risk-based maintenance (RBM): a quantitative methodology for maintenance/inspection scheduling and planning. J Loss Prev Process Ind 2003;16(6):561–73.
[21] Laakso T, Lampola T, Rantala J, Kuronen R, Ahopelto S, Vahala R. Pipe-specific criticality classification as a tool for managing risks related to water and wastewater systems, In: Proceedings of the 2nd New Developments in IT & Water Conference, Rotterdam, The Netherlands.
[22] Levitin G, Lisnianski A, Ushakov I. Reliability of multi-state systems: a historical overview. In: Lindqvist Doksum, editor. Mathematical and statistical methods in reliability. World Scientific; 2003. p. 123–37.
[23] Liesiö J, Mild P, Salo A. Preference programming for robust portfolio modeling and project selection. Eur J Oper Res 2007;181(3):1488–505.
[24] Liesiö J, Mild P, Salo A. Robust portfolio modeling with incomplete cost information and project interdependencies. Eur J Oper Res 2008;190(3):679–95.
[25] Marlow DR, Beale DJ, Mashford JS. Risk-based prioritization and its application to inspection of valves in the water sector. Reliab Eng Syst Saf 2012;100:67–74.
[26] Mild P, Salo A, Liesiö J. Selecting infrastructure maintenance projects with robust portfolio modeling. Decis Support Syst 2015;77:21–30.
[27] Modarres M. Risk analysis in engineering: techniques, tools and trends. CRC Press; 2006.
[28] Saaty TL. How to make a decision: the analytic hierarchy process. Eur J Oper Res 1990;9(26):9–26.
[29] Sakai S. Risk-based maintenance. J East Tech Rev 2010;17:1–4.
[30] Salo A, Hämäläinen RP. On the measurement of preferences in the analytic hierarchy process. J Multi-Criteria Decis Anal 1997;6:309–19.
[31] Salo A, Hämäläinen RP. Preference assessment by imprecise ratio statements. Oper Res 1992;40(6):1053–61.
[32] Salo A, Hämäläinen RP. Preference programming through approximate ratio comparisons. Eur J Oper Res 1995;82(3):458–75.
[33] Salo A, Keisler J, Morton A. Portfolio decision analysis, improved methods for resource allocation. International series in operations research & management science. . New York: Springer; 2011.
[34] Salo A, Mild P. Combining a multi-attribute value function with an optimization model: an application to dynamic resource allocation for infrastructure maintenance. Decis Anal 2009;6(3):139–52.
[35] Salo A, Punkka A. Rank inclusion in criteria hierarchies. Eur J Oper Res 2005;163(2):338–56.
[36] Vaurio JK. Optimization of test and maintenance intervals based on risk and cost. Reliab Eng Syst Saf 1995;49:23–36.
[37] Vesely WE, Belhadj M, Rezos JT. PRA importance measures for maintenance prioritization applications. Reliab Eng Syst Saf 1993;43:307–18.
[38] Vianello C, Maschio G. Quantitative risk assessment of the Italian gas distribution network. J Loss Prev Process Ind 2014;32(1):5–17.
[39] Vilkkumaa E, Salo A, Liesiö J. Multicriteria portfolio modeling for the development of shared action agendas. Group Decis Negot 2014;23:49–70.
[40] Von Winterfeldt D, Edwards W. Decision analysis and behavioral research. Cambridge, UK: Cambridge University Press; 1986.
[41] Zhao, JQ. Trunk Sewers in Canada 1998. APWA International Public Works Congress Seminar Series. Las Vegas: American Public Works Association; September 14–7, 1998.
[42] Zhao JQ, Rajani B. Construction and rehabilitation costs for buried pipe with a focus on trenchless. Research report No. 101 technologies. Ottawa, ON, Canada: Institute for Research in Construction, National Research Council Canada; 2002.

Publication VI

Alessandro Mancuso, Michele Compare, Ahti Salo and Enrico Zio. Optimal Prognostics and Health Management-driven inspection and maintenance strategies for industrial systems. *Manuscript*, 24 pages, December 2019.

Optimal Prognostics and Health Management-driven inspection and maintenance strategies for industrial systems

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

[1]Department of Mathematics and Systems Analysis, Aalto University, Finland

[2]MINES ParisTech, PSL Research University, CRC, Sophia Antipolis, France

[3]Dipartimento di Energia, Politecnico di Milano, Italy

[4]Aramis s.r.l., Milano, Italy

Abstract

The performance of the Prognostics and Health Management (PHM) depends both on the functioning of the measurement acquisition system and on the actual state of the system being monitored. The dependencies between these systems must be considered when developing optimal inspection and maintenance strategies. This paper develops a methodology to support maintenance decisions for industrial systems with PHM capabilities. The methodology employs influence diagrams when seeking to maximize the expected utility of system operation. The optimization problem is solved by mixed-integer linear programming, subject to budget and technical constraints. Chance constraints can be also included, for instance to curtail risks based on measures such as the Value at Risk (VaR) and the Conditional Value at Risk (CVaR) of system operation. The viability of the methodology is demonstrated by optimizing the inspection and maintenance strategy for a gas turbine equipped with PHM capabilities. The computation of the Value of Perfect Information (VoPI) provides additional insights on maintenance management.

Keywords: Predictive Maintenance, Prognostics and Health Management, Influence Diagrams, Decision Programming, Value of Perfect Information, Gas Turbine.

*Corresponding author. Tel.: +358 504084419. E-mail address: alessandro.mancuso@aalto.fi (A. Mancuso)

1 Introduction

Digitalization is a fundamental driver of Industry 4.0, a novel paradigm which enhances production efficiency through information and communication technologies [1, 2]. These technologies also provide a foundation for Predictive Maintenance (PM) for industrial components and systems, whereby condition monitoring data is employed to perform three tasks:

(i) **detection** of abnormal states, by identifying deviations from normal operating conditions in production processes, manufacturing equipment and products;

(ii) **diagnostics**, by classifying abnormal states;

(iii) **prognostics**, by predicting the evolution of abnormal states up to failure.

Detection, diagnostics and prognostics constitute the Prognostics and Health Management (PHM, [3, 4, 5, 6]). These tasks help implement efficient, just-in-time and just-right maintenance strategies by selecting the right action for the right component at the right time, thus maximizing production revenues and minimizing costs and losses, including assets [7]. Furthermore, PHM performance metrics have been introduced to characterize errors in detection, diagnostics and prognostics [8, 9]. Based on these metrics, several models have been developed to optimize Operations and Maintenance (O&M) decisions [7] and investments in PHM capabilities [10, 11, 12, 13].

A main limitation of earlier PM models is the assumption that sensors always work correctly, although in practice sensors may malfunction: freezing (or constant), noise, spike (or short), drift and quantization are the most common sensor malfunctions [14]. Faulty sensors may provide inaccurate measurements of the monitored physical parameters, affecting the performance of the PHM algorithms by conveying inaccurate or misleading information about the actual system state. This can cause missing alarms or unnecessary system downtimes, resulting in large financial losses. For example, the spillover effect (cross-sensitivity [15]) is known to propagate the anomalous monitoring data from a faulty sensor to other healthy signals, causing difficulties in choosing the correct maintenance action (i.e., fix or replace the sensor).

The detection of a sensor malfunction, which is often performed through *sensor data validation*, has been addressed by different methods, including Auto Associative Neural Network (AANN, [16]), Nonlinear Partial Least Squares Modeling (NLPLS, [17]), Principal Component Analysis (PCA, [18, 19]), Auto Associative Kernel Regression [20, 21] and Multivariate State Estimation Technique (MSET, [22]). However, algorithms for sensor validation too are affected by errors that depend on the health state of the monitored system. Specifically, if the monitored system does not work correctly, sensor validation is less effective in detecting incoherent deviations of the faulty sensor values with respect to data provided

by other sensors. The main reason is that sensor validation algorithms are generally trained by signal data which is generated by healthy system operation only. Based on this training data, the algorithm learns to reconstruct the behaviors of the monitored signals when the system operates normally, which differs from those acquired when the system operates in a degraded state. Although the change in the signal behaviors is fundamental to the early detection of the system anomaly, it nonetheless lowers the performance of the sensor validation algorithms, because they have not been trained in the degraded setting.

When a system is equipped with PHM capabilities, maintenance decisions refer to two sequential actions: first, the inspection of either the sensors or the industrial system; second, the necessary repairs depending on the inspection outcomes. The costs of the sequential actions are very different, with different effects on the health state of the system and uncertainties about the performance of the PHM algorithms.

The above considerations suggest that optimal maintenance decision problems in a PM setting must be framed as a multi-stage decision problem, encoding the mutual dependence of the PHM algorithms tracking the system health state on those for sensor validation [23, 24]. On this topic, Driessen et al. [25] present a cost evaluation of maintenance policies for a single-component system, which is periodically subject to imperfect inspections. Do et al. [26] evaluate different maintenance policies for a deteriorating system in which the inspection policy is based on the residual useful life. Papakonstantinou and Shinozuka [27] employ Partially Observable Markov Decision Processes (POMDP) to optimize inspection and maintenance policies based on stochastic models and uncertain structural data in real time. Literature reviews (e.g., [28, 29]) call for increased attention to optimization models on condition-based maintenance, but they do not account for the imperfect performance of condition monitoring and inspections [30, 31, 32].

Influence diagrams [33] are one of the well-established techniques for structuring and solving multi-stage decision problems. They are commonly solved, for instance, through local transformations such as arc reversals and node removals in the diagram [34]. Tatman et al. [35] develop the equivalent decision tree representation, which is solved by dynamic programming [36]. Nonetheless, these standard techniques have limitations. First, they rely on the "no-forgetting" assumption, meaning that earlier decisions are known when making later ones. Although this may be not too limiting in practice, the information flow in industrial practice can at times be disrupted due to communication failures. Second, the use of dynamic programming is restrictive in that the objective function cannot include risk measures such as Value-at-Risk or semi-absolute deviation, which reflect the variability of consequences across all possible outcomes.

To overcome these limitations, we employ the Decision Programming approach proposed by Salo et al. [37], which employs Mixed Integer Linear Programming (MILP, [38, 39]) to solve multi-stage decision problems under uncertainty. Specifically, we employ Decision Programming to identify the

optimal inspection and maintenance strategy for an industrial system with realistic PHM capabilities and sensor validation algorithms: each combination of states of the nodes of the influence diagram is mapped onto the two-stage decision maximizing the system utility. To the authors' best knowledge, this is the first time that a maintenance decision support model is developed in this practical setting, considering realistic PHM and sensor validation systems. In current industrial practice, the choice of maintenance strategies for industrial systems with PHM capabilities has been driven mainly by expert judgment [40].

The remainder of the paper is as follows. Section 2 introduces the influence diagrams and the problem formulation. Section 3 presents the optimization model and additional constraints. Section 4 proposes a case study from industry, concerning the optimization of inspection and maintenance strategies of a gas turbine. Section 5 discusses the potential and limitations of the proposed methodology. Finally, Section 6 concludes the paper and outlines extensions for future research.

2 Formulation of the influence diagram

An *influence diagram* is a directed acyclic graph that represents probabilistic causal dependencies between events and decisions [33]. Figure 1 shows an example of influence diagram which consists of three types of nodes:

(i) *chance nodes* C (indicated by circles) represent the random events of the scenarios;

(ii) *decision nodes* D (indicated by squares) represent possible choices of actions;

(iii) *value nodes* U (indicated by hexagons) represent the utility of system operation.

Causal dependencies in the set of nodes $N = C \cup D \cup U$ are represented by directed arcs $A \subseteq \{(i,j)|i,j \in N,\ i \neq j\}$. Specifically, arc $(i,j) \in A$ connects node i to node j to show that the state at node j is conditionally dependent on that at node i. The direct predecessors of node j belong to the *information set* $I(j) = \{i \in N|(i,j) \in A\}$. The arcs directed to chance nodes indicate probabilistic dependencies, whereas those directed to decision nodes denote the availability of information [34]. Because the network is acyclic, the nodes can be indexed with consecutive integers so that the indexes of nodes $i \in I(j)$ are lower than the index of node j.

Node $j \in C \cup D$ corresponds to the variable X_j, whose realization s_j assumes values in the discrete set of states S_j. The meaning of these variables is different for chance and decision nodes. Specifically, the states of decision nodes denote the choice of the risk mitigation actions that can be taken to reduce the probability of system failure. The decision X_j at node $j \in D$ depends on the *information state* $s_{I(j)}$

which belongs to the Cartesian product

$$S_{I(j)} = \bigtimes_{i \in I(j)} S_i, \tag{1}$$

defined by the combinations of states for all nodes in the information set. The information state determines what information is available when making the decision.

On the other hand, the states of chance nodes denote the health state of the system components [41]. These states represent mutually exclusive events, for which the uncertainty in the realization is described by the probability distribution on the states S_j. If the chance node does not depend on other nodes (no incoming arcs), there is an unconditional probability distribution $\mathbb{P}[X_j]$on the set S_j. For each chance node $j \in C$ which has a non-empty information set $I(j)$, the conditional probability of the state $s_j \in S_j$ is $\mathbb{P}[X_j = s_j | X_{I(j)} = s_{I(j)}]$, where $X_{I(j)} = s_{I(j)}$ denotes that the realizations of the variables X_i for nodes $i \in I(j)$ are the same as those in the information state $s_{I(j)}$.

A *policy* for decision node $j \in D$ is a function Z_j that maps information state to corresponding decisions $Z_j : S_{I(j)} \mapsto S_j$. The binary variables $z[s_j|s_{I(j)}]$ model the policy Z_j such that

$$Z_j[s_{I(j)}] = s_j \iff z[s_j|s_{I(j)}] = 1. \tag{2}$$

Specifically, the policy of decision node $j \in D$ depends on the information state $s_{I(j)}$, meaning that the choices of actions depend on the information provided by sensors and inspections. The set of combinations of policies for all decision nodes D is a *strategy* Z.

A *scenario* s is a specific combination of states s_i of all chance and decision nodes. Thus, the set of all possible scenarios is $\mathbb{S} = \bigtimes_{i \in C \cup D} S_i$, each scenario defining a specific combination of random events and a respective strategy of actions. For a specific strategy Z, the probability of scenario s is

$$p(s) = \prod_{j \in C} \mathbb{P}[X_j = s_j | X_{I(j)} = s_{I(j)}], \tag{3}$$

if Z is such that it consists of policies Z_j such that $Z_j[s_{I(j)}] = s_j$, and 0 otherwise. In summary, the probability $\pi(s)$ of scenario s is

$$\pi(s) = \begin{cases} p(s), & \text{if } z[s_j|s_{I(j)}] = 1 \, \forall j \in D \\ 0, & \text{otherwise} \end{cases}. \tag{4}$$

Finally, each scenario s is associated with a consequence whose value $V(s)$ represents the utility of system operation discounted by the costs of deploying of the selected actions. The value nodes U encode the

values $V(s)$ for all scenarios s. While it is possible to consider multiple value nodes, this paper focuses on a single objective optimization in which the aim is to maximize the utility of system operation, subject to possible resource and risk constraints.

3 Optimization model

The optimal strategy can be found through a mixed-integer linear programming model formulation, proposed by Salo et al. [37]. In this model, the probability $\pi(s)$ of scenario s is defined through the equations:

$$\sum_{s_j \in S_j} z[s_j|s_{I(j)}] = 1, \quad \forall j \in D, \forall s_{I(j)} \in S_{I(j)} \tag{5}$$

$$0 \leq \pi(s) \leq p(s), \quad \forall s \in \mathbb{S} \tag{6}$$

$$\pi(s) \geq p(s) + \sum_{j \in D} z[s_j|s_{I(j)}] - |D|, \quad \forall s \in \mathbb{S} \tag{7}$$

$$\pi(s) \leq z[s_j|s_{I(j)}], \quad \forall s \in \mathbb{S} \tag{8}$$

$$z[s_j|s_{I(j)}] \in \{0, 1\}, \quad \forall j \in D, \forall s_j \in S_j, \forall s_{I(j)} \in S_{I(j)}. \tag{9}$$

If $z[s_j|s_{I(j)}] = 1$ for all s_j in scenario s, then probability $\pi(s)$ is the upper bound $p(s)$ because constraints (6) and (7) imply

$$\begin{cases} 0 \leq \pi(s) \leq p(s) \\ \pi(s) \geq p(s). \end{cases} \tag{10}$$

On the other hand, if any binary variable $z[s_j|s_{I(j)}] = 0$ for any s_j in scenario s, then probability $\pi(s) = 0$ because constraint (8) implies $\pi(s) \leq 0$.

The optimal strategy Z^* is the strategy that maximizes the expected utility of system operation so that

$$\mathbb{E}[V(Z)] = \sum_{s \in \mathbb{S}} \pi(s)\, V(s) \tag{11}$$

subject to constraints (5)-(9). Specifically, constraints (5) ensure that only one decision $s_j \in S_j$ is taken at each decision node $j \in D$ for every information state $s_{I(j)} \in S_{I(j)}$. Constraints (6) bound the probabilities $\pi(s)$ of scenarios $s \in \mathbb{S}$. Constraints (7) ensure that the scenario probabilities $\pi(s)$ cannot be smaller than

their upper bounds $p(s)$ for scenario s such that $z[s_j|s_{I(j)}] = 1$, $j \in D$. Constraints (8) ensure that only those scenarios for which $z[s_j|s_{I(j)}] = 1$ for all $j \in D$ can have positive probabilities. Finally, constraints (9) specify the domain of all binary variables $z[s_j|s_{I(j)}]$.

In addition, the optimization model can include technical constraints that affect the deployment of risk mitigation actions. For instance, the constraint

$$z[s_j|s_{I(j)}] \leq z[s_\ell|s_{I(\ell)}] \quad \forall (s_{I(j)}, s_{I(\ell)}) \in S_{I(j)} \times S_{I(\ell)} \tag{12}$$

means that the action s_j cannot be deployed unless action s_ℓ is employed, regardless of the information states $s_{I(j)}$ and $s_{I(\ell)}$ of nodes j and ℓ.

3.1 Additional constraints

Let $Q(s_j|s_{I(j)})$ be the cost of risk mitigation action s_j at decision node $j \in D$ for the information state $s_{I(j)}$, then the total cost $Q(s)$ of implementing the actions for scenario $s \in \mathbb{S}$ is

$$Q(s) = \sum_{j \in D} Q(s_j|s_{I(j)})\, z[s_j|s_{I(j)}]. \tag{13}$$

For each scenario $s \in \mathbb{S}$, it is possible to require that the total cost of risk mitigation actions is lower than the budget B, so that $Q(s) \leq B$. If this constraint is too strict, chance constraints can be introduced, for instance to limit the probability of exceeding the budget to $\beta \in [0, 1)$ as

$$\sum_{\{s \in \mathbb{S} | Q(s) > B\}} \pi(s) \leq \beta. \tag{14}$$

One can also consider constraints on risk measures, for instance to bound the Value at Risk (VaR) and the Conditional Value at Risk (CVaR) of system operation [42]. At probability level $\alpha > 0$, the Value at Risk of strategy Z is

$$\text{VaR}_\alpha(Z) = \sup \{t \in \mathbb{R} \mid \sum_{\{s \in \mathbb{S} | V(s) \leq t\}} \pi(s) < \alpha\}, \tag{15}$$

where the sum of probabilities considers only the scenarios for which the value $V(s)$ meets or exceeds the target level $t \in \mathbb{R}$.

In addition to the VaR, constraints on the Conditional Value at Risk (CVaR) limit the expected shortfall in the worst performing scenarios [43]. Thus, the Conditional Value at Risk of strategy Z is the

expected value of the α-tail distribution of the utility function so that

$$\mathrm{CVaR}_\alpha(Z) = \mathrm{VaR}_\alpha(Z)\,[\alpha - \sum_{\{s\in\mathbb{S}|V(s)<\mathrm{VaR}_\alpha(Z)\}} \pi(s)] + \sum_{\{s\in\mathbb{S}|V(s)<\mathrm{VaR}_\alpha(Z)\}} \pi(s)\,V(s). \tag{16}$$

Conditional Value at Risk is a coherent risk measure: unlike VaR, it also reflects the shape of the distribution tail. For this reason, it is commonly considered a more informative risk measure than VaR [44].

3.2 Value of Perfect Information

The Value of Perfect Information (VoPI) refers to the additional value that can be gained by obtaining perfect information about the system state, based on which the operations are optimized. Thus, VoPI quantifies the willingness to pay for the transition from the current PHM system to the perfect one [45]. As mentioned in Section 1, PHM monitoring and system inspections provide imperfect information about the state of the industrial system. In this framework, it is possible to compute VoPI as the difference between the optimal expected value for two situations: (i) when the system state is correctly observed and (ii) when the system state is observed with possible errors. The first situation corresponds to perfect information on the system state, whereas the second situation to imperfect information. Consequently, the VoPI can be computed as

$$\mathrm{VoPI} = \mathbb{E}[V(Z^{**}|\text{Perfect Information})] - \mathbb{E}[V(Z^*)]. \tag{17}$$

In the case of inspection and maintenance decisions, perfect information refers to a situation in which sensors and inspections correctly indicate the state of the industrial system [46]. Specifically, the system state is reported correctly by the monitoring system with probability one if and only if the monitored state equals the actual system state, and 0 otherwise. Perfect information makes it possible to select the optimal strategy Z^{**}, which may differ from the optimal strategy Z^* with imperfect information.

The VoPI represents the increase in expected value when the maintenance strategy can be decided based on perfect information about the system state [47]. This provides insights into the value of investing in improving the PHM capabilities. Note that this analysis can be performed before any additional information, by assuming that perfect measurement information is obtained.

4 Case study

The case study presents a maintenance decision framework for a Gas Turbine (GT) equipped with PHM and sensor validation capabilities, which provide imperfect information on the current state of the GT and its sensors. In industrial practice, the PHM of a GT relies on hundreds of sensors tracking the health states of a large number of components with different impacts on GT operation. For illustrative purposes, we assume that global indicators on the states of the GT and PHM system are available.

The GT undergoes periodic inspection and maintenance actions on which decisions are taken every 4000 working hours. Figure 1 represents the influence diagram for planning the GT inspections and maintenance, composed of the set of chance nodes (circles), the set of decision nodes (squares) and the value node (hexagon). In particular, node H refers to the working hours of the GT, which are technically referred to as *fired hours*. The realizations are discrete states with time interval of 4000 hours so that

$$s_H \in \{0, 4000, 8000, 12000, 16000, 20000, ...\}. \tag{18}$$

Node H is deterministic, which can be considered as a degenerate chance node with probability one for the current state only. This representation is useful for modelling the causal dependence between (i) the GT states and (ii) sensor states from the working hours of the GT, allowing the optimization problem can be solved for each of the states of working hours.

The fired hours affect the *sensor* state s_{SS} and the *turbine* state s_{TS}, which implies $I(SS) = I(TS) = \{H\}$. The sensor and the GT health states are qualitative evaluations included in the sets

$$s_{SS}, s_{TS} \in \{Excellent, Good, Fair, Poor, Failing\}, \tag{19}$$

Figures 2 and 3 illustrate the probability distributions of turbine and sensor states, respectively. Specifically, the probability of these states depend on the fired hours H (horizontal line), in keeping with the conditional probabilities $\mathbb{P}[X_{SS} = s_{SS}|X_H = s_H]$ and $\mathbb{P}[X_{TS} = s_{TS}|X_H = s_H]$. These values can be inferred from the inspection outcomes, when the multi-state degradation setting is adopted in the GT maintenance practice [31, 48].

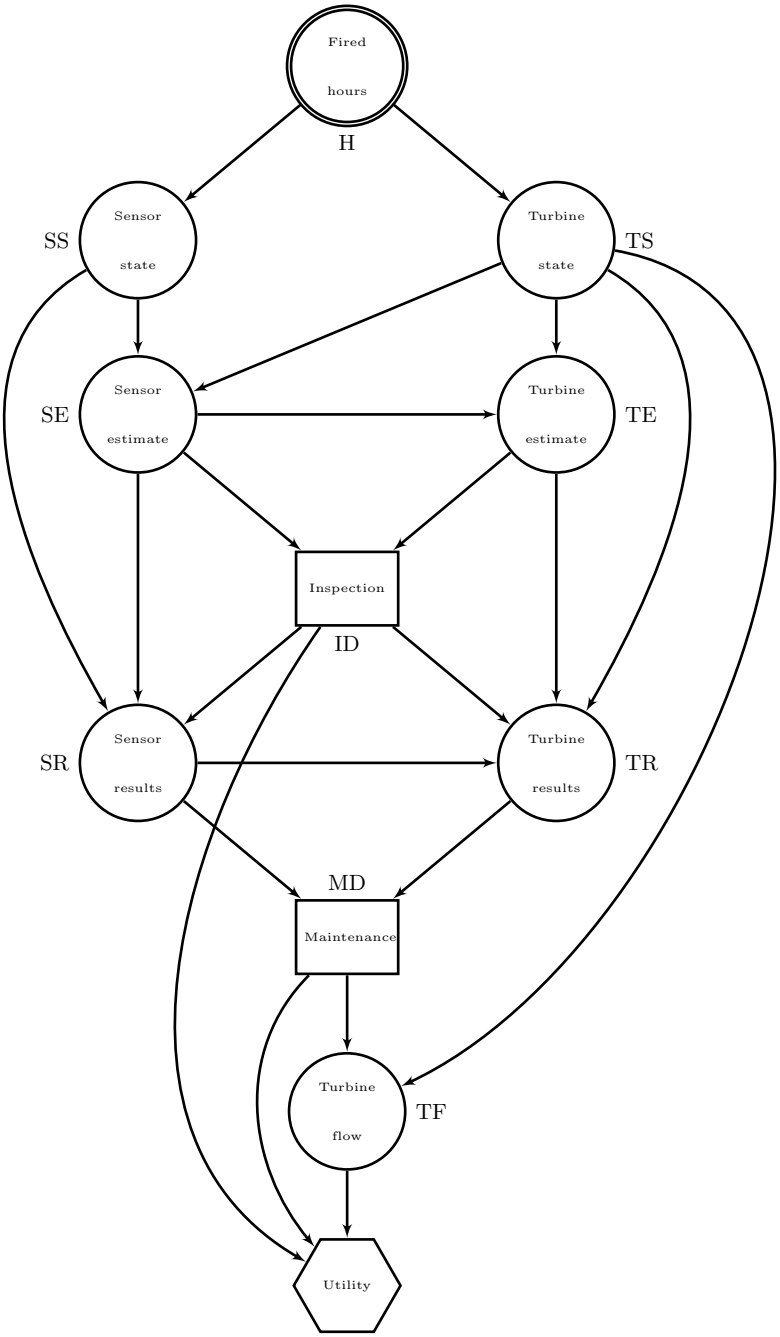


Figure 1: Influence diagram for programming inspections and maintenance of a turbine.

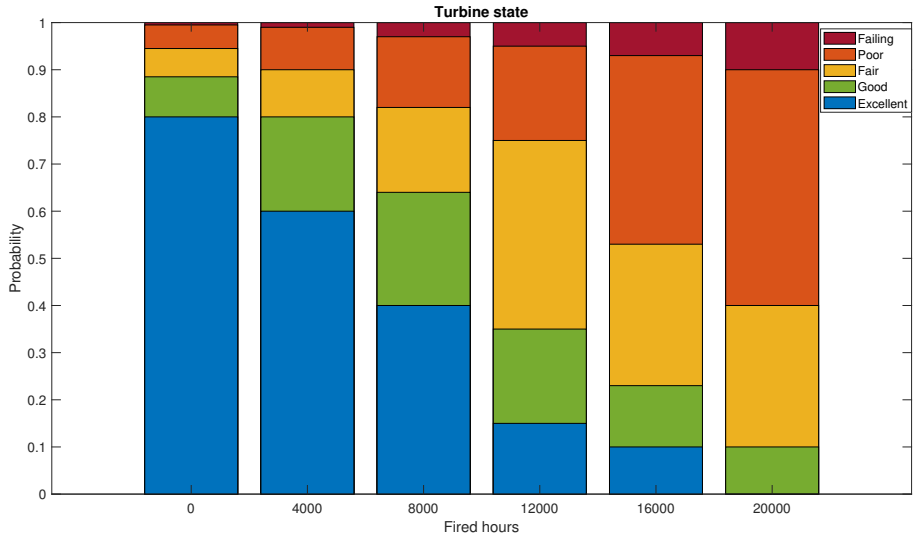


Figure 2: Probability distribution for *Turbine state*.

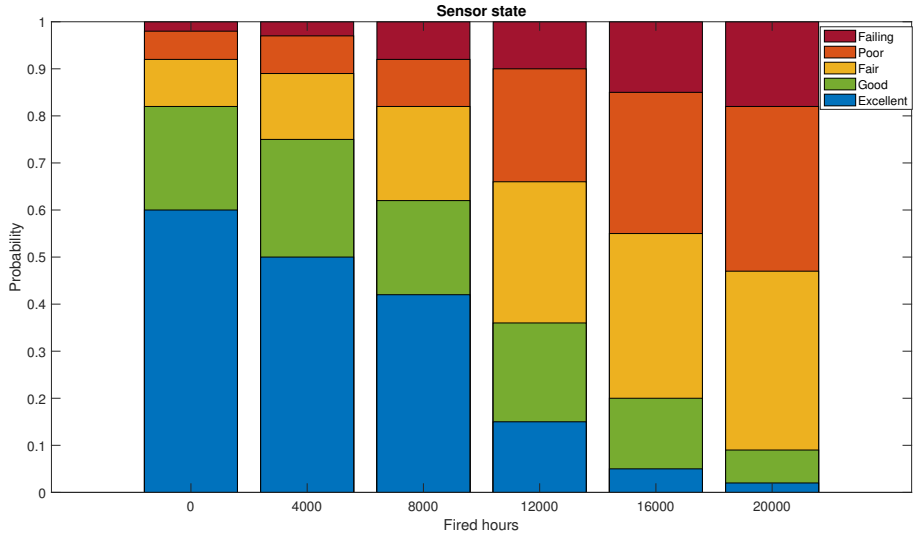


Figure 3: Probability distribution for *Sensor state*.

Based on machine-learning models [49], the PHM algorithms provide following *estimates* of the sensor state and the turbine state

$$s_{SE}, s_{TE} \in \{Excellent, Good, Fair, Poor, Failing\}, \tag{20}$$

The estimate s_{SE} of the sensor state depends on both the actual state of the sensor and the actual state of the GT. The estimate s_{TE} of the GT state depends on both its actual state and the estimate of the sensor state, because the sensor validation affects the PHM performance.

The PHM estimates on sensors and turbine provide information for the *Inspection Decision*, in the set

$$s_{ID} \in \{None, Sensor\,Check, Condition\,Monitoring\}, \tag{21}$$

where $Sensor\,Check$ indicates an analysis of the signal data and $Condition\,Monitoring$ refers to a maintenance action on the sensor acquisition chain. Neither action requires the GT to stop, and the *result* s_{SR} on the sensor state is in the set

$$s_{SR} \in \{Excellent, Good, Fair, Poor, Failing\}. \tag{22}$$

Without inspection, the results s_{SR} on the sensor state correspond to the sensor estimate s_{SE} provided by the PHM. If any inspection is performed, the results s_{SR} on the sensor state report the actual sensor state s_{SS} correctly with 95% probability. The observation is erroneous with 5% probability, which has been equally distributed across the two incorrect states close to the actual state.

The sensor inspection provides relevant information on the accuracy of the estimate s_{TE}. Specifically, it supports the definition of an updated estimate s_{TR} of the turbine state such that

$$s_{TR} \in \{Excellent, Good, Fair, Poor, Failing\}. \tag{23}$$

The results s_{TR} on the turbine state depend also on the results s_{SR} on sensor state and on the actual and estimated turbine states (i.e, s_{TS} and s_{TE}, respectively). Without inspection, the results s_{TR} on the turbine state correspond to the estimate s_{TE} of the turbine state, provided by the PHM. If the inspection is $Sensor\,Check$, the results s_{TR} on the turbine state correspond to the actual turbine state s_{TS} with a probability which depends on the sensor results s_{SR}. Finally, if the inspection is $Condition\,Monitoring$, the results s_{TR} on the turbine state report the actual turbine state s_{TS} correctly with 98% probability. The observation is erroneous with 2% probability, which has been equally distributed across the two incorrect states close to the actual state.

The results s_{SR} and s_{TR} on the sensor state and the turbine state provide information for the *Maintenance Decision*, in the set

$$s_{MD} \in \{None, Level1, Level2\}, \tag{24}$$

where $Level1$ restores the turbine state to 4000 hours earlier and $Level2$ restores the turbine state effectively to 0 hours of operation, i.e. as good as new. In this respect, Figure 4 represents the model of degradation and restoration processes of the GT and the PHM. Arrows indicate probabilistic transitions between states during the next 4000 hours, based on the maintenance decision. For illustration, Table 1 reports the transition probabilities for the degradation and renovation of the GT. For example, if the turbine is currently in state $s_{TS} = Good$ and the maintenance decision $s_{MD} = Level2$ is deployed, the turbine is in state $s_{TS} = Excellent$ with probability 99% and in state $s_{TS} = Good$ with probability 1% during the next 4000 hours.

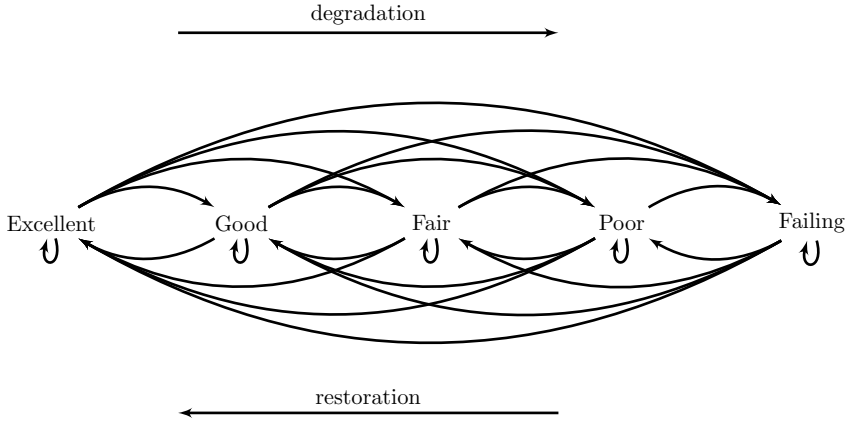


Figure 4: Probabilistic model of the degradation and restoration process of the turbine.

Table 1: Probabilistic transitions between turbine states.

		s_{TF}				
s_{TS}	s_{MD}	*Excellent*	*Good*	*Fair*	*Poor*	*Failing*
Excellent	None	0.80	0.10	0.05	0.03	0.02
	Level 1	0.90	0.05	0.03	0.02	0
	Level 2	0.99	0.01	0	0	0
Good	None	0	0.80	0.10	0.07	0.03
	Level 1	0.03	0.90	0.05	0.02	0
	Level 2	0.99	0.01	0	0	0
Fair	None	0	0	0.75	0.15	0.1
	Level 1	0	0.03	0.90	0.05	0.02
	Level 2	0.99	0.01	0	0	0
Poor	None	0	0	0	0.75	0.25
	Level 1	0	0.05	0.85	0.07	0.03
	Level 2	0.99	0.01	0	0	0
Failing	None	0	0	0	0	1
	Level 1	0	0	0.75	0.15	0.1
	Level 2	0.99	0.01	0	0	0

The turbine state s_{TS} and maintenance decision s_{MD} affect the *Turbine Flow*, which has the following discrete values

$$s_{TF} \in \{Excellent, Good, Fair, Poor, Failing\}. \tag{25}$$

The GT flow rate impacts the utility of the system operation, reduced by the costs of inspections s_{ID} and maintenance s_{MD}. Figure 5 shows illustrative utilities based on the state of the turbine flow, whereas Table 2 shows the costs for inspection and maintenance actions. The utilities and costs are illustrative units but have not been derived from an actual industrial system.

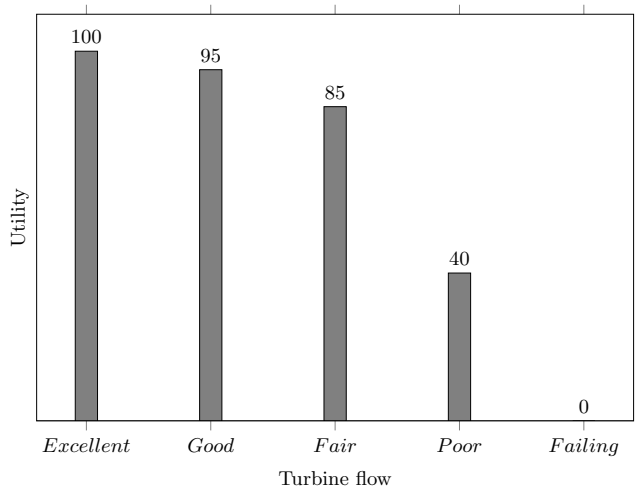


Figure 5: Illustrative utilities of the system operation.

Table 2: Costs for inspection and maintenance actions.

		s_{MD}		
		None	Level 1	Level 2
s_{ID}	None	0	25	50
	Sensor check	2	27	52
	Condition monitoring	8	33	58

The solution of the optimization model provides the optimal inspection and maintenance strategies for every level of *fired hours* and for each information state which is available when making these decisions. For illustration, Tables 3 and 4 present the optimal inspection and maintenance strategies of the GT at $H = 16000$ fired hours, respectively. Specifically, the inspection strategy depends on the estimates s_{SE} and s_{TE} of the sensor and turbine states, whereas the maintenance strategy depends on the results of the inspections s_{SR} and s_{TR}.

Table 3: Optimal inspection strategy at $H = 16000$ hours.

		s_{TE}				
		Excellent	*Good*	*Fair*	*Poor*	*Failing*
s_{SE}	*Excellent*	None	None	None	None	None
	Good	None	None	None	None	None
	Fair	None	None	None	None	None
	Poor	None	None	Monitoring	None	None
	Failing	Monitoring	Monitoring	Monitoring	None	None

Table 4: Optimal maintenance strategy at $H = 16000$ hours.

		s_{TR}				
		Excellent	*Good*	*Fair*	*Poor*	*Failing*
s_{SR}	*Excellent*	None	None	None	Level 1	Level 2
	Good	None	None	None	Level 1	Level 2
	Fair	None	None	None	Level 1	Level 1
	Poor	None	None	None	Level 1	Level 1
	Failing	None	None	None	Level 1	Level 1

The optimal inspection strategy is such that no inspection is performed if the sensor state estimate is *Excellent*, *Good* or *Fair* and if the turbine state estimate is *Poor* or *Failing*. On the other hand, Condition Monitoring needs to be performed if the sensor state estimate is *Poor* or *Failing* for specific circumstances of the turbine state estimate. Furthermore, the optimal maintenance strategy shows not to perform any maintenance if the turbine state estimate is *Excellent*, *Good* or *Fair*, but Level 1 maintenance should be performed if the turbine state is *Poor*. If the turbine state estimate is *Failing*, the optimal maintenance strategy depends on the sensor state estimate: Level 2 maintenance is necessary if the sensor state estimate is *Excellent* or *Good* and Level 1 maintenance otherwise.

The solutions in Tables 3 and 4 need to be examined together. Specifically, when the turbine is estimated to be in a degraded state (*Poor* or *Failing*), the optimal strategy is to proceed with maintenance actions, without improving the accuracy of the estimate of the turbine state through inspections. This choice depends on the high reliability of the monitoring sensors. On the other hand, when the estimate of the turbine is in a healthy state (*Excellent*, *Good* or *Fair*), the choice on the inspections depends on the estimated state of the monitoring sensors. Thus, the optimal strategy is to inspect the turbine when the sensors are expected to be degraded. Note that the optimization results are not generic in that they depend on the parameters of this case study.

Figure 6 illustrates the optimal expected utility of the system and the respective Value of Perfect Information, for each discrete state of the turbine fired hours. To model perfect information on the system state, the probabilities of the estimates s_{SE} and s_{TE} of the sensor and turbine states are defined as

$$\mathbb{P}[X_{SE} = s_{SE} | X_{SS} = s_{SS}, X_{TS} = s_{TS}] = \begin{cases} 1, & \text{if } s_{SE} = s_{SS} \\ 0, & \text{otherwise,} \end{cases} \tag{26}$$

$$\mathbb{P}[X_{TE} = s_{TE} | X_{SE} = s_{SE}, X_{TS} = s_{TS}] = \begin{cases} 1, & \text{if } s_{TE} = s_{TS} \\ 0, & \text{otherwise.} \end{cases} \tag{27}$$

By increasing the fired hours, the expected utility decreases due to increasing chances of degradation of the GT. For the same reason, the VoPI increases as information on the actual state of the GT yields more value for system operation [50]. Thus, investments in improving the PHM and sensor validation can be expected to yield higher returns when the GT has degraded more. The computation of the VoPI is obtained by assuming that the PHM provides perfect information on the system state.

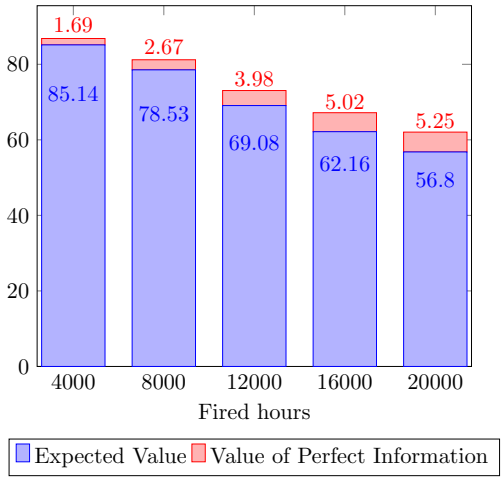


Figure 6: Expected Value and Value of Perfect Information of the turbine operation.

Besides employing risk measures as constraints of the optimization model, it is possible to analyse the VaR and CVaR of the optimization solutions to better understand the results. This analysis provides additional insights on these solutions without the need to specify the threshold probability α and target level t before the optimization. For some choices of the parameters α and t, these parameters could be so stringent that the optimization model has no feasible solutions. For this reason, an ex-post analysis of the results bypasses this issue, avoiding optimization runs with long computational times.

Figure 7 shows the cumulative probability of the utility for the optimal strategy Z^* at $H = 16000$

hours. From this probability distribution, it is possible to compute $\mathrm{VaR}_\alpha(Z^*)$ and $\mathrm{CVaR}_\alpha(Z^*)$ at probability level α, as defined in Eqs. (15) and (16). Table 5 lists the VaR and CVaR of system operation at different probability levels α: by increasing the α value, both the VaR and the CVaR also increase.

For the analysed probability levels α, the CVaR is higher than zero only for $\alpha > 0.1$. In view of these results, the optimal strategy for $H = 16000$ hours involves limited risks in that the expected utilities will be negative with probability of less than 10%.

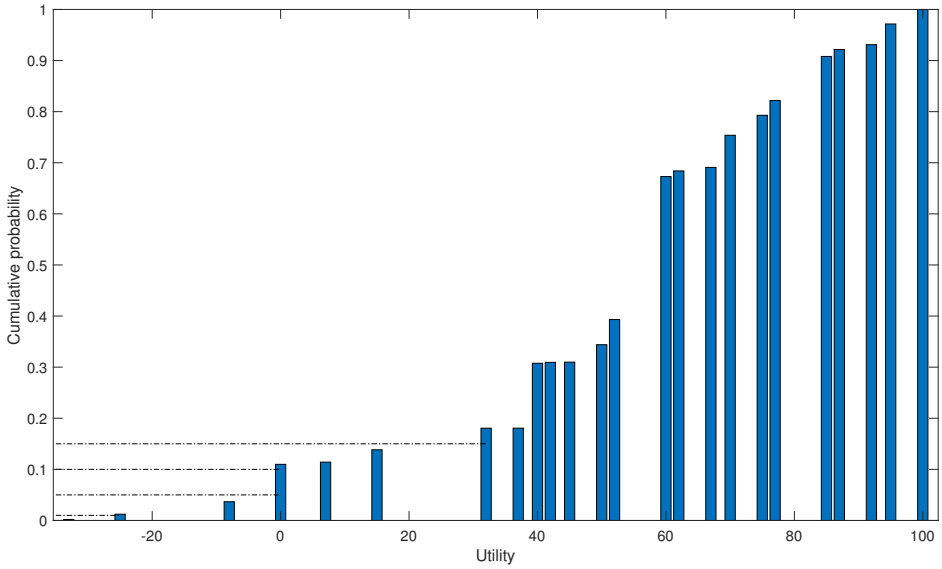


Figure 7: Cumulative probability distribution of system utility.

Table 5: VaR and CVaR for different α values.

α	VaR	CVaR
0.01	-25	-26.466
0.05	0	-10.3156
0.1	0	-5.1578
0.15	32	1.6781

5 Discussion

The computation of the VoPI makes it possible to assess investments which seek to improve the PHM capabilities. In this case, it is necessary to compare the VoPI with the costs for improving the PHM capabilities. Specifically, if the costs for improvement are lower than the VoPI, it is recommended to renovate the monitoring sensors, because the renovation leads to savings on system inspections.

The value of the PHM capabilities would increase if the company owns a fleet of industrial systems. In this case, the influence diagram represents the states of all the systems and the state of the monitoring sensors with a unique value node. The optimization model would then suggest the optimal combination of inspections for the fleet of systems, leading to additional savings for the company due to sharing fixed costs among several systems. In addition, the cost of the PHM capabilities would be shared among the fleet of systems with benefits on the failure detection, diagnostics and prognostics, due to the collection of a larger amount of data to build statistical analyses. However, the optimization may require more computational time for a large number of node states due to the curse of dimensionality. For this purpose, it is possible to decompose the large problem into a hierarchy of sub-problems to optimize the resource allocation across the fleet of industrial systems.

This framework can be extended to account for decisions in multiple time stages through Dynamic Bayesian Networks [51]. In this case, the chance nodes represent the random events of the state of the system components over the time stages and the decision nodes represent the decisions on inspections and maintenance at each time stage [52]. This gives rise to a model for long-term decisions on the industrial system in order to anticipate or postpone inspections and maintenance actions according to the predicted development of system failure. However, the number of decision variables will grow with the number of time stages, meaning that the computational time for the optimization solutions would increase.

Finally, the optimization results rely on the discretization of the probability distribution on the states of industrial systems and sensors [53]. Increasing the number of component states improves the accuracy of the model in the definition of the probability distribution, but it also increases the number of scenarios to be evaluated to define the optimal strategy. If the optimal strategy is the same for different information sets, it can be helpful to aggregate the information sets in order to limit the probability elicitation of the states and the computational time of the following runs of the optimization problem.

6 Conclusion

In this paper, we have developed a methodology for the optimal selection of inspection and maintenance strategies for industrial systems equipped with PHM. These strategies maximize the value for the company

deriving from system operation, computed as the system utility discounted by the costs for inspection and maintenance actions.

The framework employs influence diagrams to model causal dependencies between system states and decisions on risk mitigation actions. Based on Decision Programming, the optimization model defines the optimal strategies for the system, accounting for budget and technical constraints. The solution is obtained through a mixed-integer linear problem, which considers all possible scenarios on the system states and decisions. The viability of the methodology has been illustrated with an example concerning a gas turbine equipped with PHM.

Overall, we have demonstrated that in the choice for inspection and maintenance strategies, there is a need to consider the unreliability of the PHM as well, given that the optimal strategies depend on both the healthy or degraded state of the industrial system and the state of the monitoring sensors.

This framework requires that the conditional probability tables can be specified, depending on the amount of health states of the system and the sensors. Possible extensions include the introduction of imprecise and uncertain information about the model parameters. For instance, an expert may provide imprecise values about state probabilities and impacts of risk mitigation actions. Such imprecision and uncertainty must be properly represented and propagated throughout the optimization model to obtain robust solutions.

Acknowledgements

The research has been supported by the Strategic Research Council of the Academy of Finland, specifically the research project Platform Value Now. The case study has been performed using Julia Programming language with the technical support of M.Sc. Juho Andelmin.

References

[1] M. Hermann, T. Pentek, and B. Otto. Design principles for industrie 4.0 scenarios. In *Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS)*, pages 3928–3937. IEEE, 2016.

[2] H. Lasi, P. Fettke, H.G. Kemper, T. Feld, and M. Hoffmann. Industry 4.0. *Business and Information Systems Engineering*, 6(4):239–242, 2014.

[3] E. Zio and M. Compare. Evaluating maintenance policies by quantitative modeling and analysis. *Reliability Engineering and System Safety*, 109:53–65, 2013.

[4] E. Zio. Some challenges and opportunities in reliability engineering. *IEEE Transactions on Reliability*, 65(4):1769–1782, 2016.

[5] M. Pecht. Prognostics and Health Management of Electronics. *Encyclopedia of Structural Health Monitoring*, 2009.

[6] J.M. Simões, C.F. Gomes, and M.M. Yasin. A literature review of maintenance performance measurement: A conceptual framework and directions for future research. *Journal of Quality in Maintenance Engineering*, 17(2):116–137, 2011.

[7] R Rocchetta, L Bellani, M Compare, E Zio, and E Patelli. A reinforcement learning framework for optimal operation and maintenance of power grids. *Applied Energy*, 241:291–301, 2019.

[8] A. Saxena, J. Celaya, B. Saha, S. Saha, and K. Goebel. Evaluating algorithm performance metrics tailored for prognostics. In *Proceedings of the 2009 IEEE Aerospace Conference*, pages 1–13. IEEE, 2009.

[9] A. Saxena, J. Celaya, B. Saha, S. Saha, and K. Goebel. Metrics for offline evaluation of prognostic performance. *International Journal of Prognostics and Health Management*, 1(1):4–23, 2010.

[10] K. Feldman, T. Jazouli, and P.A. Sandborn. A methodology for determining the return on investment associated with Prognostics and Health Management. *IEEE Transactions on Reliability*, 58(2):305–316, 2009.

[11] B.D. Youn, C. Hu, and P. Wang. Resilience-driven system design of complex engineered systems. *Journal of Mechanical Design*, 133(10):1–15, 2011.

[12] M. Compare, L. Bellani, and E. Zio. Reliability model of a component equipped with PHM capabilities. *Reliability Engineering and System Safety*, 168:4–11, 2017.

[13] M. Compare, L. Bellani, and E. Zio. Availability model of a PHM-equipped component. *IEEE Transactions on Reliability*, 66(2):487–501, 2017.

[14] A.B. Sharma, L. Golubchik, and R. Govindan. Sensor faults: Detection methods and prevalence in real-world datasets. *ACM Transactions on Sensor Networks (TOSN)*, 6(3):23, 2010.

[15] J. Coble, P. Ramuhalli, R. Meyer, and H. Hashemian. Online sensor calibration assessment in nuclear power systems. *IEEE Instrumentation & Measurement Magazine*, 16(3):32–37, 2013.

[16] J.W. Hines, D.J. Wrest, and R.E. Uhrig. Signal validation using an adaptive neural fuzzy inference system. *Nuclear Technology*, 119(2):181–193, 1997.

[17] B. Rasmussen, J.W. Hines, and R.E. Uhrig. A novel approach to process modeling for instrument surveillance and calibration verification. *Nuclear Technology*, 143(2):217–226, 2003.

[18] G. Kerschen, P. De Boe, J.C. Golinval, and K. Worden. Sensor validation using principal component analysis. *Smart Materials and Structures*, 14(1):36–42, 2005.

[19] P. Baraldi, G. Gola, E. Zio, D. Roverso, and M. Hoffmann. A randomized model ensemble approach for reconstructing signals from faulty sensors. *Expert Systems with Applications*, 38(8):9211–9224, 2011.

[20] P. Baraldi, F. Di Maio, P. Turati, and E. Zio. Robust signal reconstruction for condition monitoring of industrial components via a modified auto associative kernel regression method. *Mechanical Systems and Signal Processing*, 60:29–44, 2015.

[21] D. Garvey, J. Garvey, R. Seibert, J.W. Hines, and S.A. Arndt. Application of on-line monitoring techniques to nuclear plant data. In *Proceedings of the 5th International Topical Meeting on Nuclear Plant Instrumentation Controls, and Human Machine Interface Technology*, 2006.

[22] K.C. Gross, R.M. Singer, S.W. Wegerich, J.P. Herzog, R. VanAlstine, and F. Bockhorst. Application of a model-based fault detection system to nuclear plant signals. In *Proceedings of the International Conference on Intelligent Systems Applications to Power Systems*, 1997.

[23] F. Khan and M. Haddara. Risk-based maintenance (RBM): a quantitative approach for maintenance/inspection scheduling and planning. *Journal of Loss Prevention in the Process Industries*, 16(6):561–573, 2003.

[24] L. Krishnasamy, F. Khan, and M. Haddara. Development of a risk-based maintenance (RBM) strategy for a power-generating plant. *Journal of Loss Prevention in the Process Industries*, 18(2):69–81, 2005.

[25] J.P.C. Driessen, H. Peng, and G.J. Van Houtum. Maintenance optimization under non-constant probabilities of imperfect inspections. *Reliability Engineering & System Safety*, 165:115–123, 2017.

[26] P. Do, A. Voisin, E. Levrat, and B. Iung. A proactive condition-based maintenance strategy with both perfect and imperfect maintenance actions. *Reliability Engineering & System Safety*, 133:22–32, 2015.

[27] K.G. Papakonstantinou and M. Shinozuka. Planning structural inspection and maintenance policies via dynamic programming and Markov processes. Part I: Theory. *Reliability Engineering & System Safety*, 130:202–213, 2014.

[28] S. Alaswad and Y. Xiang. A review on condition-based maintenance optimization models for stochastically deteriorating system. *Reliability Engineering & System Safety*, 157:54–63, 2017.

[29] M. Keizer, S.D.P. Flapper, and R.H. Teunter. Condition-based maintenance policies for systems with multiple dependent components: A review. *European Journal of Operational Research*, 261(2):405–420, 2017.

[30] S. Panagiotidou and G. Tagaras. Optimal integrated process control and maintenance under general deterioration. *Reliability Engineering & System Safety*, 104:58–70, 2012.

[31] M. Compare, F. Martini, and E. Zio. Genetic algorithms for condition-based maintenance optimization under uncertainty. *European Journal of Operational Research*, 244(2):611–623, 2015.

[32] N. Rasmekomen and A.K. Parlikad. Condition-based maintenance of multi-component systems with degradation state-rate interactions. *Reliability Engineering & System Safety*, 148:1–10, 2016.

[33] T.D. Nielsen and F.V. Jensen. *Bayesian Networks and Decision Graphs*. Springer Science & Business Media, 2009.

[34] R.D. Shachter. Evaluating influence diagrams. *Operations Research*, 34(6):871–882, 1986.

[35] J.A. Tatman and R.D. Shachter. Dynamic programming and influence diagrams. *IEEE Transactions on Systems, Man, and Cybernetics*, 20(2):365–379, 1990.

[36] D.P. Bertsekas. *Dynamic Programming and Optimal Control*, volume 1. Athena scientific Belmont, MA, 1995.

[37] A. Salo, J. Andelmin, and F. Oliveira. Decision programming for multi-stage optimization under uncertainty. `https://arxiv.org/pdf/1910.09196.pdf`, 2019. [Online: accessed 11-December-2019].

[38] D. Bertsimas and J.N. Tsitsiklis. *Introduction to Linear Optimization*, volume 6. Athena Scientific Belmont, MA, 1997.

[39] C.A. Floudas and X. Lin. Mixed integer linear programming in process scheduling: Modeling, algorithms, and applications. *Annals of Operations Research*, 139(1):131–162, 2005.

[40] A.J. Guillén, A. Crespo, M. Macchi, and J. Gómez. On the role of Prognostics and Health Management in advanced maintenance systems. *Production Planning & Control*, 27(12):991–1004, 2016.

[41] G. Levitin, A. Lisnianski, and I. Ushakov. Reliability of multi-state systems: a historical overview. In *Mathematical and Statistical Methods in Reliability*, pages 123–137. World Scientific, 2003.

[42] P. Artzner, F. Delbaen, J.M. Eber, and D. Heath. Coherent measures of risk. *Mathematical Finance*, 9(3):203–228, 1999.

[43] Juuso Liesiö and Ahti Salo. Scenario-based portfolio selection of investment projects with incomplete probability and utility information. *European Journal of Operational Research*, 217(1):162–172, 2012.

[44] R.T. Rockafellar and S. Uryasev. Conditional Value-at-Risk for general loss distributions. *Journal of Banking & Finance*, 26(7):1443–1471, 2002.

[45] M. Memarzadeh and M. Pozzi. Value of information in sequential decision making: Component inspection, permanent monitoring and system-level scheduling. *Reliability Engineering & System Safety*, 154:137–151, 2016.

[46] Ronald A Howard. Information value theory. *IEEE Transactions on Systems Science and Cybernetics*, 2(1):22–26, 1966.

[47] E. Vilkkumaa, J. Liesiö, and A. Salo. Optimal strategies for selecting project portfolios using uncertain value estimates. *European Journal of Operational Research*, 233(3):772–783, 2014.

[48] M. Compare, F. Martini, S. Mattafirri, F. Carlevaro, and E. Zio. Semi-Markov model for the oxidation degradation mechanism in gas turbine nozzles. *IEEE Transactions on Reliability*, 65:574–581, 2016.

[49] Chunsheng Yang, Takayuki Ito, Yubin Yang, and Jie Liu. Developing machine learning-based models to estimate time to failure for PHM. In *Proceedings of the 2016 IEEE International Conference on Prognostics and Health Management (ICPHM)*, pages 1–6. IEEE, 2016.

[50] J. Keisler. Value of information in portfolio decision analysis. *Decision Analysis*, 1(3):177–189, 2004.

[51] K.P. Murphy and S. Russell. *Dynamic Bayesian Networks: Representation, Inference and Learning*. University of California, Berkeley Dissertation, 2002.

[52] A. Mancuso, M. Compare, A. Salo, and E. Zio. Portfolio optimization of safety measures for the prevention of time-dependent accident scenarios. *Reliability Engineering & System Safety*, 190(106500):1–9, 2019.

[53] C. Li and A. Der Kiureghian. Optimal discretization of random fields. *Journal of Engineering Mechanics*, 119(6):1136–1154, 1993.