Department of Mathematics and Systems Analysis

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

Alessandro Mancuso

Aalto University

DOCTORAL DISSERTATIONS

Aalto University publication series
DOCTORAL DISSERTATIONS 116/2020

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 Aalto University and Politecnico di Milano, at a public examination at the lecture hall H304 of Aalto University on September 18th 2020 at 12. The public defense will be also organized via remote technology.
Link: https://aalto.zoom.us/j/69611217934
Zoom quick guide: https://www.aalto.fi/en/services/zoom-quick-guide
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

POLITECNICO DI MILANO
DEPARTMENT OF ENERGY
DOCTORAL PROGRAMME IN ENERGY AND NUCLEAR SCIENCE AND TECHNOLOGY

RISK-INFORMED OPTIMIZATION OF MITIGATION STRATEGIES IN SAFETY-CRITICAL SYSTEMS

Doctoral Dissertation of:
Alessandro Mancuso

Supervisor:
Professor Enrico Zio
Professor Ahti Salo

Tutor:
Professor Francesco Di Maio

The Chair of the Doctoral Program:
Professor Vincenzo Dossena

2020 – XXXI

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
Professor Vincent Mousseau, CentraleSupelec, France

Opponent
Professor Lesley Walls, University of Strathclyde, UK

Aalto University publication series
DOCTORAL DISSERTATIONS 116/2020

ISBN 978-952-60-3984-8 (printed)
ISBN 978-952-60-3985-5 (pdf)
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)
http://urn.fi/URN:ISBN:978-952-60-3985-5

Unigrafia Oy
Helsinki 2020

Finland

Printed matter
4041-0619

Aalto University

Abstract

Aalto University, P.O. Box 11000, FI-00076 Aalto www.aalto.fi

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 116/2020

Field of research Systems and Operations Research

Manuscript submitted 17 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 enhance 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) 978-952-60-3984-8 **ISBN (pdf)** 978-952-60-3985-5

ISSN (printed) 1799-4934 **ISSN (pdf)** 1799-4942

Location of publisher Helsinki **Location of printing** Helsinki **Year** 2020

Pages 143 **urn** http://urn.fi/URN:ISBN:978-952-60-3985-5

Aalto University

Abstract

Aalto University, P.O. Box 11000, FI-00076 Aalto www.aalto.fi

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 116/2020

Field of research Systems and Operations Research

Manuscript submitted 17 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**

Sommario

Le organizzazioni industriali devono investire nella progettazione e nelle operazioni dei propri sistemi di produzione per migliorare l'affidabilità, la disponibilità, la manutenzione e la sicurezza. In genere, queste organizzazioni dispongono di risorse limitate tali da poter selezionare solo un sottoinsieme di azioni di mitigazione per proteggere il sistema dai rischi associati a scenari di incidenti e minacce. Per questo motivo, i modelli di ottimizzazione per l'allocazione delle risorse risultano fondamentali al fine di minimizzare i rischi di tali scenari.

Nelle pratiche attuali, l'allocazione delle risorse si basa sul rischio di fallimento dei singoli componenti, di conseguenza le soluzioni potrebbero risultare non ottimali per il sistema. Al contrario, questa tesi propone un'analisi sistemica degli scenari di incidenti e minacce al fine di selezionare la strategia di mitigazione ottimale per il sistema complessivo. La strategia ottimale è una combinazione (portfolio) di azioni di mitigazione per la progettazione e le operazioni del sistema che minimizzano i rischi sistemici, soddisfacendo al contempo i relativi vincoli tecnici e finanziari.

A tal fine, l'analisi probabilistica dei rischi sistemici viene eseguita attraverso modelli Bayesiani per cogliere le incertezze degli scenari di incidenti e minacce, mentre l'allocazione delle risorse si fonda sull'analisi decisionale dei portfoli per definire le soluzioni ottimali, costituite da una serie di alternative discrete. Inoltre, tali metodologie consentono analisi dettagliate sull'allocazione del budget e la gestione del rischio degli scenari di incidenti e minacce.

Le metodologie sono illustrate rivisitando casi studio reali ed esempi riportati in letteratura sia per la progettazione sia per le operazioni del sistema, per dimostrare che le analisi sistemiche integrano le attuali pratiche sull'allocazione delle risorse basata sui componenti. Le metodologie sono generiche in quanto possono essere eseguite in altre aree di applicazione con adattamenti ragionevoli.

Keywords: Gestione del Rischio, Sistemi Critici per la Sicurezza, Reti Bayesiane, Analisi Decisionale, Ottimizzazione Vincolata.

ISBN (printed) 978-952-60-3984-8 **ISBN (pdf)** 978-952-60-3985-5

ISSN (printed) 1799-4934 **ISSN (pdf)** 1799-4942

Location of publisher Helsinki **Location of printing** Helsinki **Year** 2020

Pages 143 **urn** http://urn.fi/URN:ISBN:978-952-60-3985-5

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, August 7, 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*, 25 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.

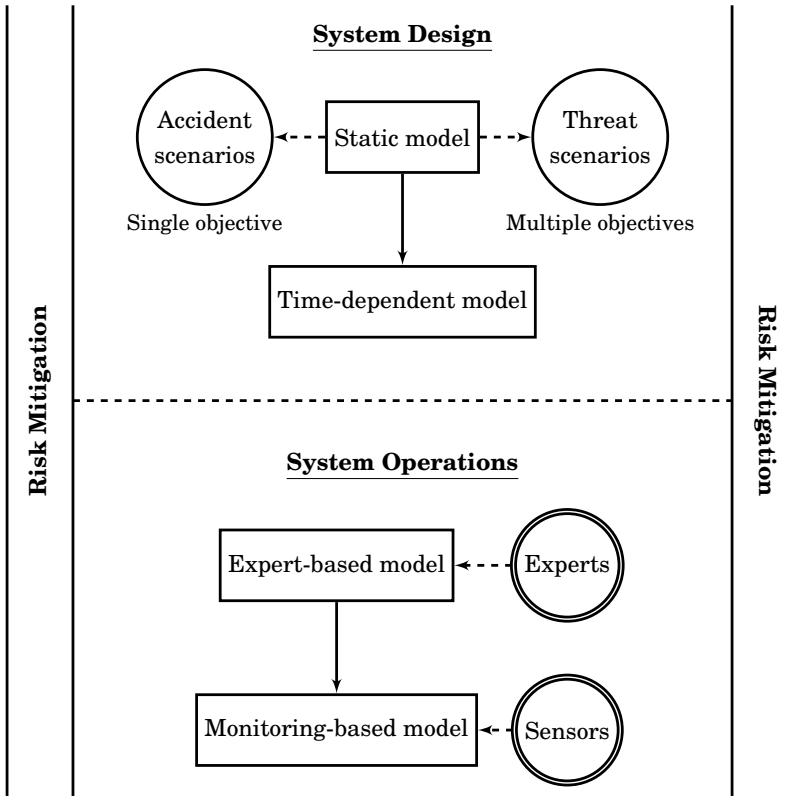

Figure 1.1. Dissertation structure.

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.

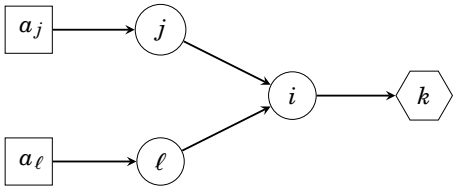

Figure 2.1. Example of influence diagram.

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 August 7, 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 August 7, 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 August 7, 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 August 7, 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*, 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 August 7, 2020].

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

Aalto-DD 116/2020

ISBN 978-952-60-3984-8 (printed)
ISBN 978-952-60-3985-5 (pdf)
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)

Aalto University
School of Science
Department of Mathematics and Systems Analysis
www.aalto.fi

BUSINESS + ECONOMY

ART + DESIGN + ARCHITECTURE

SCIENCE + TECHNOLOGY

CROSSOVER

DOCTORAL DISSERTATIONS