Aalto University
School of Science
Degree Programme in Engineering Physics and Mathematics

# Optimal Risk Reduction Portfolios in Fault Tree Analysis

Bachelor's thesis
September 30, 2013

Markus Losoi

Aalto University

AALTO UNIVERSITY
SCHOOL OF SCIENCE
PO Box 11000, FI-00076 AALTO
http://www.aalto.fi

ABSTRACT OF THE BACHELOR'S THESIS

Author: Markus Losoi

Title: Optimal Risk Reduction Portfolios in Fault Tree Analysis

Degree programme: Degree Programme in Engineering Physics and Mathematics

Major subject: Systems Sciences

Major subject code: F3010

Supervisor: Prof. Ahti Salo

Instructor: M.Sc. (Tech.) Antti Toppila

Abstract:

Failures of technical systems can cause extensive physical, material or financial damage to both people and the environment. Fault tree analysis is a method to quantify and model the causes of these failures. In this method, a system is decomposed into components that fail with a given probability and the failure of the system is modeled as a function of these probabilities.

Failure probabilities can be reduced by securing them, which reduces also system failure probability, i.e., system unreliability. This can be accomplished, e.g., by replacing a component with a parallel configuration of identical components. However, reducing a failure probability has a cost and budget available is typically limited. For this reason, only a strict subset of components can be secured. This subset is called a risk reduction portfolio.

In this thesis, a mixed-integer linear programming (MILP) problem is formulated to minimize system unreliability within a budget. The solution of the problem is the set of components that are secured, and it is called an optimal risk reduction portfolio. The MILP problem is utilized in two types of computational experiments. First, optimal risk reduction portfolios are solved as a function of budget. Second, uncertainty on failure probabilities is modeled with probability intervals. In this case, potentially non-dominated portfolios and approximate core indices of components are computed by solving the MILP problem with point-estimate probabilities taken randomly from their respective intervals.

Computational experiments are performed with two systems. First, an example test system is analysed. The structure of this system allows checking without a great effort that the solutions of the MILP problem were reasonable. This was observed to be the case. The second system is based on a residual heat removal system of a nuclear reactor. The optimal risk reduction portfolios as a function of budget revealed that the optimal order to secure components in this system resembles roughly the Fussel-Vesely risk importance order of the components. With probability intervals, 97 potentially non-dominated porfolios of ten components were found and core index approximations suggested that the securing of particular components should be prioritized while the securing of particular others should be the last priority.

Date: 30.9.2013

Language: English

Number of pages: 4+35

Keywords: fault tree, reliability, portfolio optimization, redundancy allocation, epistemic uncertainty

AALTO-YLIOPISTO
PERUSTIETEIDEN KORKEAKOULU
PL 11000, 00076 Aalto
http://www.aalto.fi

KANDIDAATINTYÖN TIIVISTELMÄ

Tekijä: Markus Losoi

Työn nimi: Optimaaliset riskinalentamisportfoliot vikapuuanalyysissä

Tutkinto-ohjelma: Teknillisen fysiikan ja matematiikan tutkinto-ohjelma

Pääaine: Systeemitieteet

Pääaineen koodi: F3010

Vastuuopettaja(t): prof. Ahti Salo

Ohjaaja(t): DI Antti Toppila

Tiivistelmä:

Teknisten järjestelmien, kuten liikennevälineiden, tietoverkkojen ja voimalaitosten, vikaantuminen voi aiheuttaa merkittäviä materiaalisia ja taloudellisia vahinkoja. Vikapuuanalyysi on menetelmä näiden vikaantumisten aiheuttajien kvantitatiiviseen analysoimiseen. Tässä menetelmässä järjestelmä jaetaan komponentteihin, joille arvioidaan vikaantumistodennäköisyys, ja koko järjestelmän vikaantuminen mallinnetaan yksittäisten komponenttien vikaantumisten funktiona.

Komponenttien vikaantumistodennäköisyyksiä voidaan pienentää varmentamalla komponentteja. Tällöin myös koko järjestelmän vikaantumistodennäköisyys, eli järjestelmän epäluotettavuus, pienenee. Komponentti voidaan varmentaa esim. vaihtamalla se usean vastaavanlaisen komponentin rinnankytkentään. Varmentamistoimenpiteet aiheuttavat kuitenkin kustannuksen, ja käytettävissä oleva budjetti on yleensä rajoitettu. Näin ollen vain aito osajoukko komponentteja voidaan varmentaa. Tällaista osajoukkoa kutsutaan tässä työssä riskinalentamisportfolioksi.

Tässä työssä muotoillaan lineaarinen kokonaislukutehtävä (engl., mixed-integer linear programming problem; MILP problem), joka ratkaisee järjestelmän epäluotettavuuden minimoivan riskinalentamisportfolion budjetin rajoissa. Ratkaisua kutsutaan optimaaliseksi riskinalentamisportfolioksi. MILP-ongelmaa käytetään kahdenlaisissa kokeissa. Ensiksi ongelman avulla ratkaistaan optimaaliset riskinalentamisportfoliot budjetin funktiona. Toiseksi vikaantumistodennäköisyyksien epävarmuuksia mallinnetaan todennäköisyysintervalleilla, jolloin optimointimallia käytetään potentiaalisten ei-dominoitujen portfolioiden ja approksimatiivisten ydinlukujen laskemiseen valitsemalla pistetodennäköisyydet todennäköisyysintervalleilta.

Kokeet suoritetaan kahdella järjestelmällä. Aluksi analysoidaan seitsemän komponentin esimerkkijärjestelmää, jonka rakenne mahdollistaa tulosten oikeellisuuden tarkistamisen ilman huomattavaa työtä. Tulosten havaittiin olevan järkeviä. Lisäksi työssä analysoidaan ydinreaktorin jälkilämmönpoistojärjestelmää. Tälle järjestelmälle optimaaliset riskinalentamisportfoliot budjetin funktiona paljastivat, että komponenttien optimaalinen varmistusjärjestys vastaa karkeasti komponenttien Fussel-Vesely-riskitärkeysmitan mukaista järjestystä. Todennäköisyysintervalleja käytettäessä puolestaan löytyi 97 potentiaalisesti ei-dominoitua kymmenen komponentin portfoliota, ja ydinlukuapproksimaatiot antoivat suosituksia tiettyjen komponenttien varmentamisen priorisoimiseen ja toisten komponenttien varmentamisen sivuuttamiseen.

Päivämäärä: 30.9.2013

Kieli: englanti

Sivumäärä: 4+35

Avainsanat: vikapuu, luotettavuus, portfolio-optimointi, redundanssin allokointi, episteeminen epävarmuus

# Contents

# 1 Introduction

Failures of technical systems, such as means of transportation, information networks and power plants can cause extensive physical, material or financial damage to both people and the environment. For example, the failure of the trim servo motor control system caused the accident of the Boeing 707 aircraft at Paris-Orly airport in 1962 [1]. The accident involved 132 occupants of which 130 were fatally injured. These accidents are often analysed to prevent or mitigate their harmful consequences.

Fault tree analysis is a method to quantify and model causes of failures in a technical system. In this method, the system is decomposed into components. The failures of these components are modeled with probabilities, and the failure of the system is modeled as a function of these component failures. The system failure probability is called system unreliability. Fault tree analysis is used in the field of probabilistic risk assessment (PRA), which is widely applied in, e.g., construction, energy, military and aerospace [2]. For instance, Boeing engineers chose fault tree analysis as the method to analyse the safety of an aircraft when they built the Boeing 747 [3].

A method to reduce the failure probability of a technical system is to secure components by allocating redundancy [4]. This means that a component is replaced with a parallel configuration of several components identical to the original one. This parallel configuration fails iff all the components in the configuration fail, which typically is more unlikely than the failure of a single component. However, securing components has a cost and available resources are typically limited. For this reason, it is sensible to consider which components should be secured when the budget is limited. The set of components that are secured is called a risk reduction portfolio.

This thesis develops a mathematical model that solves which components should be secured within a budget when the failure probability of a system is reduced. The optimal set of secured components with a given budget minimizes system failure probability over all sets of secured components that are feasible within the given budget. This optimal set is referred to as the optimal risk reduction portfolio.

Previously, system failure probability minimization has been studied in the case of a series system [5]. The analysis of a series system reliability has been extended to consider optimal redundancy allocation [6]. In this case, the series configuration consists of subsystems, and the optimal number of components for each subsystem is solved to minimize system failure probability.

The failure probabilites of components may contain uncertainties. These uncertainties can be modeled with probability intervals. That is, the failure probability of a component is estimated to be on a real interval, but the exact value of it is unknown. Probability intervals have been applied, e.g., in the reliability analysis of a series-parallel system [7]. In this thesis, risk reduction portfolios are analysed also in the case of probability intervals. To compare different portfolios, the concept of dominance relation is defined and applied in the analysis.

The rest of this thesis is structured as follows. Section 2 reviews previous studies on risk reduction in technical systems. Section 3 formulates the optimal risk reduction portfolio problem. Section 4 applies the problem in optimal redundancy allocation while Section 5 applies the problem in the analysis of epistemic uncertainties. Section 6 covers computational experiments related to optimal redundancy allocation and the analysis of epistemic uncertainties.

# 2 Optimal risk reduction of systems

The problem of system failure probability, i.e., system unreliability minimization under a budget constraint has been studied before. Cho and Sung formulated a nonlinear binary integer programming problem and derived a branch-and-bound algorithm to maximize the reliability of a series system with multiple-choice constraints and a budget constraint [5].

In the problem formulation of Cho and Sung, the structure of a system is limited to a series configuration of components. Each component is selected from a set that is specific to the corresponding stage in the series configuration. This selection process is modeled with multiple-choice constraints. In addition, each component consumes a specific amount of budget, and the budget constraint ensures that the total consumption stays within a budget. From the budget constraint, it follows that the component with the highest reliability cannot always (if ever) be selected in each stage.

System unreliability minimization has been studied also in the context of redundancy allocation. Kuo and Prasad considered optimal redundancy allocation in a coherent system that consists of a series configuration of subsystems [6]. They defined a coherent system as a system in which replacing failed components by working components will not cause system failure when the system is functioning.

Unlike Cho and Sung, Kuo and Prasad assumed less on the subsystem structures of the stages in a series configuration. In the study of Cho and Sung, each stage consists only of one component that was selected from a set that is specific to this stage. While this is one possible substructure in the study of Kuo and Prasad, also alternative substructures exist. The redundant components in a stage can form, e.g., a parallel configuration or a $k$-out-of-$m$ configuration, in which all the components have the same reliability.

Kuo and Prasad presented a method to solve the optimal number of redundant components in each stage given that the lower and the upper bound for the number of components in each stage is known. Their problem formulation includes also budget constraints for different types of resources. The consumption of a particular resource in a particular stage is a function of the number of components in that stage.

Interval probabilities have been applied to the problem of optimal redundancy allocation by Feizollahi and Modarres [7]. In their study, system structure is limited to a series-parallel configuration of components. That is, a system is represented as a series configuration of parallel configurations whose numbers of components are to be solved. In addition, the components in a parallel configuration are assumed to be identical in the sense that their reliability intervals are equal.

Feizollahi and Modarres defined a scenario as the vector of reliabilities whose values are taken from their respective intervals. They presented four exact algorithms to find the solution with the minimal deviation in reliability from the solution with the maximal reliability over all scenarios and combinations of components. This solution is called a min-max regret solution. In addition, the problem formulation contains budget constraints that are similar to the corresponding constraints in the formulation of Kuo and Prasad.

# 3 Methodological development of the optimal risk reduction portfolio problem

The problem of minimizing system unreliability by securing components is introduced and described in two parts. First, the problem is formulated and explained. Second, a simple example case is studied to help the understanding of the problem formulation. A solution of this problem is the set of components, i.e., a portfolio, that reduces the unreliability of a system the most. Because unreliabilty of a system can be viewed as a risk, this problem is called an optimal risk reduction portfolio problem. In addition, a scaling method to overcome numerical difficulties is presented.

## 3.1 Problem formulation

In fault tree analysis, the failure of a technical system is modeled as a set of basic events and logical connectors between them. A basic event is the failure event of a component, and basic events are assumed to be statistically independent. Logical connectors, such as AND and OR gates define the relationships between basic events [8]. The basic events in a fault tree can be enumerated from 1 to $n$, so the set of all basic events can be defined as

$$BE = \{1, ..., n\}\,.$$

Together, basic events and logical connectors form the top event of a fault tree. The top event indicates whether the entire system fails, which occurs if a particular set of basic events occur.

A minimal set of basic events that leads to system failure is called a minimal cut set (MCS) [9]. The probability of a minimal cut set is the probability of the event in which all the basic events in the MCS occur. Thus, a minimal cut set probability is the product of basic event probabilities with respect to the basic events in the MCS. Minimal cut sets can be enumerated from 1 to $N$, and the minimal cut set $j$ is denoted as

$$MCS_j \subset BE.$$

System failure probability, i.e., system unreliability $Q$, can be derived from the fault tree presentation of a system. It can be approximated by the sum of all minimal cut set probabilities

$$Q \approx \sum\nolimits_{j=1}^{N} \prod\nolimits_{i \in MCS_j} p_i,$$

where $p_i$ is the probability of the basic event $i$ and $\prod_{i \in MCS_j} p_i$ is the probability of the minimal cut set $j$. This approximation is called the rare event approximation, and it gives an upper bound for system unreliability [8]. The approximation is close to the exact value when all basic events have low probabilities [10].

Assume that the probability of basic events can be reduced from $p_i$ to $p_i^r < p_i$ with a cost $c_i$. A risk reduction portfolio $P \subset BE$ is defined as the set of basic events whose probabilities are reduced. This portfolio is denoted by $P$.

For each basic event $i$, a binary indicator variable is defined as

$$b_i = \begin{cases} 0, & i \notin P \\ 1, & i \in P \end{cases} . \tag{1}$$

Using this definition, the total cost of a risk reduction portfolio $P$ is $\sum_{i=1}^{n} b_i c_i$. A risk reduction portfolio $P$ is optimal with a budget $B$ iff portfolio $P$ is a solution of the problem

$$\begin{aligned} \min_{P} \quad & Q \\ \text{s.t.} \quad & \sum\nolimits_{i=1}^{n} b_i c_i \leq B \end{aligned}$$

The problem of finding an optimal risk reduction portfolio $P$ can be formulated as a mixed-integer linear programming (MILP) problem. The parameters of the MILP problem are listed and described in Table 1 and the decision variables in Table 2.

A probability product decision variable $q_{j,i}$ in Table 2 denotes the probability product of $i$ basic events in the minimal cut set $j$. These basic events and the multiplication order of their probabilities is specified by the first $i$ elements in the ordering vector $\mathbf{m}_j$. Consequently, the probability product $q_{j,|MCS_j|}$ equals to the probability of the minimal cut set $j$.

An ordering vector $\mathbf{m}_j$ in Table 1 denotes the ascending order of the basic events in the minimal cut set $j$. Thus, the dimension of the vector equals to $|MCS_j|$. However, the vector could denote an arbitrary order instead of the ascending one. This is because multiplication of real numbers is commutative and the vector $\mathbf{m}_j$ specifies the order in which basic event probabilities are multiplied to construct the probability of the minimal cut set $j$. For instance, if $MCS_j = \{4, 5, 1\}$, then $\mathbf{m}_j = (1, 4, 5)$, but the MILP model would work with, e.g., $\mathbf{m}_j = (4, 1, 5)$ or $\mathbf{m}_j = (5, 4, 1)$, as well.

The binary indicator variables $b_i$ are collected into the vector

$$\mathbf{b} = (b_1, ..., b_n) , \tag{2}$$

Table 1: The parameters of the optimal risk reduction portfolio MILP problem.

| | |
|---|---|
| $n$ | The number of basic events in the fault tree. |
| $p_i$ | The original probability of the basic event $i$. |
| $p_i^r$ | The reduced probability of the basic event $i$. |
| $c_i$ | The cost of reducing the probability of the basic event $i$. |
| $B$ | The budget. |
| $N$ | The number of minimal cut sets in the fault tree. |
| $\mathbf{m}_j$ | A vector representing the ascending order of the basic events in the minimal cut set $j$. |

Table 2: The decision variables of the optimal risk reduction portfolio MILP problem.

| | |
|---|---|
| $b_i$ | A binary variable that indicates whether the basic event $i$ belongs to the risk reduction portfolio. |
| $q_{j,i}$ | The product of the first $i$ basic events probabilities in $MCS_j$. The multiplication order is specified by the vector $\mathbf{m}_j$. |

and the probability products $q_{j,i}$ are collected into the set

$$Q_p = \{q_{j,i}\},$$

where $j \in \{1, ..., N\}$ and $i \in \{1, ..., |MCS_j|\}$. For instance, consider a fault tree of a system that contains the basic events $BE = \{1, 2, 3\}$ and the minimal cut sets $MCS_1 = \{1, 2\}$ and $MCS_2 = \{3\}$. In this case, the binary indicator vector is $\mathbf{b} = (b_1, b_2, b_3)$ and the set of probability products is $Q_p = \{q_{1,1}, q_{1,2}, q_{2,1}\}$. In addition, the ordering vectors are $\mathbf{m}_1 = (1, 2)$ and $\mathbf{m}_2 = (3)$. Let $q_i$ denote the probability of the basic event $i$ after risk reduction decision. That is, $q_i = p_i$ iff $b_i = 0$ and $q_i = p_i^r$ iff $b_i = 1$. Using this notation, $q_{1,1}$ corresponds to $q_1$, $q_{1,2}$ to $q_1 q_2$ and $q_{2,1}$ to $q_3$.

The objective of the MILP optimization problem is formulated as

$$\min_{\mathbf{b},Q_p} \sum_{j=1}^{N} q_{j,|MCS_j|} \tag{3}$$

The objective function in Equation (3) is the rare event approximation of system unreliability. Thus, the objective function is the sum of minimal cut set probabilities $q_{j,|MCS_j|}$ over $j \in \{1, ..., N\}$. This sum is to be minimized to reduce the upper bound of system unreliability as much as possible.

The constraints of the MILP problem are:

$$b_i \in \{0,1\} \qquad \forall i \in BE \tag{4}$$

$$\sum\nolimits_{i=1}^{n} c_i b_i \leq B \tag{5}$$

$$q_{j,1} = p_{\mathbf{m}_{j,1}} \left(1 - b_{\mathbf{m}_{j,1}}\right) + p^r_{\mathbf{m}_{j,1}} b_{\mathbf{m}_{j,1}} \qquad \forall j \in \{1, ..., N\} \tag{6}$$

$$q_{j,i} \leq p_{\mathbf{m}_{j,i}} q_{j,i-1} + b_{\mathbf{m}_{j,i}} \qquad \forall j \in \{1, ..., N\}, \ \forall i \in \{2, ..., |MCS_j|\} \tag{7}$$

$$q_{j,i} \geq p_{\mathbf{m}_{j,i}} q_{j,i-1} - b_{\mathbf{m}_{j,i}} \qquad \forall j \in \{1, ..., N\}, \ \forall i \in \{2, ..., |MCS_j|\} \tag{8}$$

$$q_{j,i} \leq p^r_{\mathbf{m}_{j,i}} q_{j,i-1} + \left(1 - b_{\mathbf{m}_{j,i}}\right) \qquad \forall j \in \{1, ..., N\}, \ \forall i \in \{2, ..., |MCS_j|\} \tag{9}$$

$$q_{j,i} \geq p^r_{\mathbf{m}_{j,i}} q_{j,i-1} - \left(1 - b_{\mathbf{m}_{j,i}}\right) \qquad \forall j \in \{1, ..., N\}, \ \forall i \in \{2, ..., |MCS_j|\} \tag{10}$$

In this formulation, $\mathbf{m}_{j,i}$ denotes the $i$:th element of the vector $\mathbf{m}_j$. The constraint (4) restricts the indicator variables $b_i$ to be binary, and the constraint (5) ensures that the overall cost of the portfolio stays within the budget $B$.

The formation of a minimal cut set probability $q_{j,|MCS_j|}$ is accomplished by the conditional multiplying of basic event probabilities in the constraints (6)-(10). The constraints form two either-or constraints: either

$$q_{j,i} = p_{\mathbf{m}_{j,i}} q_{j,i-1},$$

or

$$q_{j,i} = p^r_{\mathbf{m}_{j,i}} q_{j,i-1}.$$

The constraint (6) selects either the original probability $p_{\mathbf{m}_{j,1}}$ or the reduced probability $p^r_{\mathbf{m}_{j,1}}$ to be the first factor of the minimal cut set probability $q_{j,|MCS_j|}$. The constraints (7)-(10) perform the same type of selections for the rest of the basic events in the minimal cut set $j$. The product of the first $i$ basic event probabilities is formed by multiplying the product of the first $i-1$ basic event probabilities either with the original probability $p_{\mathbf{m}_{j,i}}$ or with the reduced probability $p^r_{\mathbf{m}_{j,i}}$. This conditional multiplying is continued until the value of the minimal cut set probability $q_{j,|MCS_j|}$ is finally determined.

## 3.2 Example

A fault tree consisting of only two basic events, 1 and 2, and one AND gate is presented in Figure 1. The failure of this system, i.e., the top event T, is

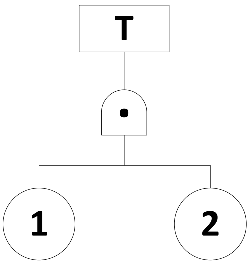

Figure 1: The fault tree of a system consisting of only two basic events, 1 and 2, and one AND gate. The top event T indicates the failure of the system, which occurs if both of the basic events occur.

determined by only one minimal cut set, $MCS_1 = \{1,2\}$ . Thus, the rare event approximation of the system unreliability is the product $p_1 p_2$, where $p_1$ and $p_2$ denote the probabilities of the basic events 1 and 2, respectively.

The ordering vector $\mathbf{m}_1$ of the minimal cut set 1 is $\mathbf{m}_1 = (1,2)$. If the original basic event probabilities $p_1$ and $p_2$ can be reduced to $p_1^r$ and $p_2^r$ with the costs $c_1$ and $c_2$ and a budget $B$ is given, the optimal risk reduction portfolio $P$ for this system can be solved. This can be accomplished by defining the decision variables

$$\begin{aligned} \mathbf{b} &= (b_1, b_2)\,, \\ Q_p &= \{q_{1,1}, q_{1,2}\}\,, \end{aligned}$$

and solving the MILP problem

$$\begin{aligned} \min_{\mathbf{b},Q_p} \quad & q_{1,2} \\ \text{s.t.} \quad & b_1, b_2 \in \{0,1\} \\ & c_1 b_1 + c_2 b_2 \leq B \\ & q_{1,1} = p_1(1-b_1) + p_1^r b_1 && (11) \\ & q_{1,2} \leq p_2 q_{1,1} + b_2 && (12) \\ & q_{1,2} \geq p_2 q_{1,1} - b_2 && (13) \\ & q_{1,2} \leq p_2^r q_{1,1} + (1-b_2) && (14) \\ & q_{1,2} \geq p_2^r q_{1,1} - (1-b_2)\,. && (15) \end{aligned}$$

The decision variables $b_1$ and $b_2$ indicate whether the basic events 1 and 2 are included in the optimal portfolio $P$, i.e., whether their probabilities

Table 3: All the possible values of the decision variables $q_{1,1}$ and $q_{1,2}$ as a function of the decision variables $b_1$ and $b_2$. In this example, the value of $q_{1,2}$ equals to the value of the objective function.

| $b_1$ | $b_2$ | $q_{1,1}$ | $q_{1,2}$ |
|---|---|---|---|
| 0 | 0 | $p_1$ | $p_1p_2$ |
| 1 | 0 | $p_1^r$ | $p_1^rp_2$ |
| 0 | 1 | $p_1$ | $p_1p_2^r$ |
| 1 | 1 | $p_1^r$ | $p_1^rp_2^r$ |

are reduced. In addition, the decision variables $q_{1,1}$ and $q_{1,2}$ construct the probability of $MCS_1$.

The constraints (11)-(15) form the probability of $MCS_1$. If $b_1 = 0$, the value of the variable $q_{1,1}$ is determined to be $p_1$, which can be seen by substituting $b_1 = 0$ into the constraint (11). Similarly, if $b_1 = 1$, the constraint (11) determines the value of the variable $q_{1,1}$ to be $p_1^r$.

If $b_2 = 0$, the constraints (12)-(13) force the value of the variable $q_{1,2}$ to be $p_2q_{1,1}$ because inequalities $q_{1,2} \leq p_2q_{1,1}$ and $q_{1,2} \geq p_2q_{1,1}$ are both valid if and only if $q_{1,2} = p_2q_{1,1}$. In this case, the constraints (14)-(15) become redundant, because $p_2^r$, $q_{1,1}$ and $q_{1,2}$ are probabilities and, thus, $p_2^rq_{1,1} - 1 \leq 0 \leq q_{1,2} \leq 1 \leq 1 + p_2^rq_{1,1}$. Similar kind of reasoning applies also to the case $b_2 = 1$. All the possible values of the variables $q_{1,1}$ and $q_{1,2}$ as a function of the variables $b_1$ and $b_2$ are listed in Table 3.

The objective function $q_{1,2}$ is the probability of $MCS_1$. Because this example system contains no other minimal cut sets, the probability of $MCS_1$ represents the rare event approximation of the system unreliability, which was to be minimized.

If the costs were $c_i = 1$ for both components, the budget were $B = 1$, the original probabilities were $p_1 = p_2 = 0.1$ and the reduced probabilities were $p_1^r = 0.02$ and $p_2^r = 0.04$, then the optimal solution would be to reduce the failure probability of the component 1. This can be seen in Table 4 that lists the numerical values of the decision variables.

Table 4: The total costs of risk reduction portfolios $P$ and the numerical values of the decision variables $q_{1,1}$ and $q_{1,2}$ as a function of the decision variables $b_1$ and $b_2$. A portfolio $P$ is marked feasible if its total cost is less than the budget $B = 1$. The optimal solution is in bold.

| $P$ | | | | | |
|---|---|---|---|---|---|
| $b_1$ | $b_2$ | $\sum_{i=1}^{2} b_i c_i$ | Feasible | $q_{1,1}$ | $q_{1,2}$ |
| 0 | 0 | 0 | Yes | 0.1 | 0.01 |
| **1** | **0** | **1** | **Yes** | **0.02** | **0.002** |
| 0 | 1 | 1 | Yes | 0.1 | 0.004 |
| 1 | 1 | 2 | No | 0.02 | 0.0008 |

## 3.3 Scaling method to overcome numerical difficulties

MILP solvers may feature a feasibility tolerance parameter to control how much the constraints of a model are allowed to be violated. However, the minimum value of this parameter may be too high for an optimal risk reduction portfolio problem. The probability products $q_{j,i}$ in the constraints (7)-(10) can become smaller than this minimum value, which causes rounding errors in the probability products $q_{j,i}$.

The problem with a feasibility tolerance parameter can be alleviated by scaling minimal cut set probabilities $q_{j,|MCS_j|}$ with a scaling factor $s > 1$. In the MILP problem formulation, this is accomplished by replacing the constraints (6)-(10) with the constraints

$$q_{j,1} = s\left(p_{\mathbf{m}_{j,1}}\left(1 - b_{\mathbf{m}_{j,1}}\right) + p^r_{\mathbf{m}_{j,1}} b_{\mathbf{m}_{j,1}}\right) \qquad \forall j \in \{1, ..., N\} \tag{16}$$

$$q_{j,i} \leq p_{\mathbf{m}_{j,i}} q_{j,i-1} + s b_{\mathbf{m}_{j,i}} \qquad \forall j \in \{1, ..., N\}, \; \forall i \in \{2, ..., |MCS_j|\} \tag{17}$$

$$q_{j,i} \geq p_{\mathbf{m}_{j,i}} q_{j,i-1} - s b_{\mathbf{m}_{j,i}} \qquad \forall j \in \{1, ..., N\}, \; \forall i \in \{2, ..., |MCS_j|\} \tag{18}$$

$$q_{j,i} \leq p^r_{\mathbf{m}_{j,i}} q_{j,i-1} + s\left(1 - b_{\mathbf{m}_{j,i}}\right) \qquad \forall j \in \{1, ..., N\}, \; \forall i \in \{2, ..., |MCS_j|\} \tag{19}$$

$$q_{j,i} \geq p^r_{\mathbf{m}_{j,i}} q_{j,i-1} - s\left(1 - b_{\mathbf{m}_{j,i}}\right) \qquad \forall j \in \{1, ..., N\}, \; \forall i \in \{2, ..., |MCS_j|\} \tag{20}$$

The constraint (16) is responsible for multiplying a minimal cut set probability $q_{j,|MCS_j|}$ with a scaling factor $s$, and the constraints (17)-(20) work in the similar manner as the constraints (7)-(10) because $s \geq sq_{j,i}$ $\forall j \in \{1, ..., N\}$ $\forall i \in \{1, ..., |MCS_j|\}$. Now, all the minimal cut set probabilities and, thus, the objective function becomes scaled by the scaling factor $s$. Consequently, the value of the optimal solution returned by a MILP solver must be multiplied with $s^{-1}$ to cancel out scaling.

# 4 Optimal redundancy allocation

The unreliability of a system can be reduced by allocating redundancy [4]. This can be accomplished by securing a component with a parallel configuration of two or more components identical to the secured one. For example, the first level of redundant arrays of inexpensive disks (RAID) technology specifies that a hard disk is mirrored with an identical one to reduce the unreliability of a data storage system [11]. The degree of redundancy $d$ is defined to be the number of components in a parallel configuration.

In fault tree modeling, securing a component with a parallel configuration of identical components can be interpreted as connecting the basic event of the secured component to an AND gate with new basic events that all have the same probability as the original basic event. For example, redundancy can be allocated in the fault tree of Figure 1 by connecting the basic event 2 to an AND gate with a new basic event 3 that has the same probability as the basic event 2. As a result, the original probability $p_2$ is reduced to $p_2^r = p_2 \cdot p_2 = (p_2)^2$. The effect of this redundancy allocation for the fault tree is illustrated in Figure 2. However, in the case of connecting a basic event to an AND gate with new basic events, the failures of the components in a parallel configuration are assumed to be independent.

Redundancy can be allocated optimally by utilizing the optimal risk reduction portfolio problem. Assume that the degrees of redundancies $d_i$ are known for each component and the reduced probabilities $p_i^r$ can be computed as a function of the degrees $d_i$. In this case, an optimal risk reduction portfolio can be solved. This yields the set of components that should be secured by allocating redundancy optimally, i.e., in such a way that system unreliability is minimized.

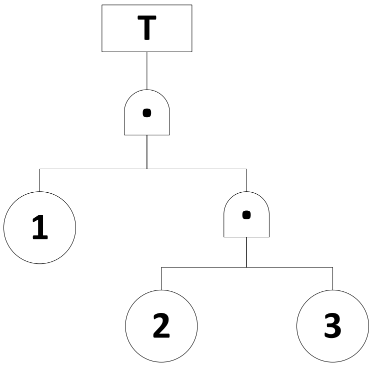

Figure 2: The fault tree of the example in Section 3.2 after the component 2 is secured with the degree of redundancy $d = 2$.

## 4.1 Common-cause failures

The independence of component failures can be an unrealistic assumption. This is because, e.g., identical components manufactured in the same production process are likely to share the same defects. These types of dependencies can be modeled with common-cause failure (CCF) models.

A widely utilized CCF model is the beta factor model [12]. This single-parameter model assumes that all the components in a redundant system (e.g., a parallel configuration of identical components) fail when a CCF occurs. In this model, the probability that $k$ out of $d$ components fail is defined as

$$p_k = \begin{cases} (1-\beta)\,p & , \quad k = 1 \\ 0 & , \quad 1 < k < d \\ \beta p & , \quad k = d \end{cases} , \tag{21}$$

where $p$ is the failure probability of a component, $p_1$ is the probability that a component fails independently, $p_d$ is the probability that all components in a configuration fail because of a CCF, and $\beta$ estimates the proportion of common cause failures to all failures. The beta factor can be expressed as the fraction

$$\beta = \frac{\lambda_c}{\lambda_c + \lambda_i},$$

where $\lambda_c$ is the rate of common cause failures and $\lambda_i$ is the rate of independent failures. Statistical data can be utilized to estimate the value of the parameter $\beta$. For instance, a typical value for equipment in industrial process control is 1-10 % [13].

Assume that a component is secured by replacing it with a parallel configuration of $d$ identical components. The failure probability of the secured component is derived in the following way. Let event $A$ denote the event that the secured component fails, and let $p$ be the probability of this event. Similarly, let event $A_k$ denote the event that the component $k$ in the parallel configuration fails. After the component is secured, i.e., redundancy is allocated with the degree $d$, the secured component fails iff all the components in the parallel configuration of $d$ identical components fails. That is, $A$ occurs iff all of the events $A_1, ..., A_d$ occur. Thus, the probability of event $A$ is reduced to

$$p^r = P\left(\bigcap\nolimits_{k=1}^{d} A_k\right), \tag{22}$$

where $P\left(E\right)$ denotes the probability of an event $E$. Let $C$ denote the event of a CCF. Consequently, the probability of a failure event $A_k$ due to an independent failure is

$$P\left(A_k \,|\, C^C\right) = \left(1 - \beta\right) p, \tag{23}$$

where $C^C$ is the complement event of $C$, and the probability of a failure event $A_k$ due to a CCF is

$$P\left(A_k \,|\, C\right) = 1. \tag{24}$$

The value $\left(1 - \beta\right) p$ in Equation (23) is derived from Equation (21), and Equation (24) results from the fact that in the beta factor model all components will fail with absolute certainty if a CCF occurs. By the law of total probability, the reduced probability of event A is

$$P\left(\bigcap_{k=1}^{d} A_k\right) = P\left(\bigcap_{k=1}^{d} A_k \,|\, C\right) P\left(C\right) + P\left(\bigcap_{k=1}^{d} A_k \,|\, C^C\right) \left(1 - P\left(C\right)\right). \tag{25}$$

With similar reasoning as in Equation (24), it follows that

$$P\left(\bigcap\nolimits_{k=1}^{d} A_k \,|\, C\right) = 1, \tag{26}$$

and the probability of a CCF

$$P\left(C\right) = \beta p \tag{27}$$

is equal to the probability that all components fail because of a CCF. This probability is presented in Equation (21). In the event $\bigcap\nolimits_{k=1}^{d} A_k$ with the condition $C^C$ all components fail independently. For this reason, the probability of the conditional event can be computed with the help of Equation (23)

$$P\left(\bigcap\nolimits_{k=1}^{d} A_k \,|\, C^C\right) = \left(P\left(A_k \,|\, C^C\right)\right)^d = \left(\left(1 - \beta\right) p\right)^d. \tag{28}$$

Finally, by substituting equations (25)–(28) into Equation (22), the reduced probability of event $A$ and, thus, the failure probability of the secured component becomes

$$p^r = \beta p + \left( \left( 1 - \beta \right) p \right)^d \left( 1 - \beta p \right). \tag{29}$$

## 4.2 Example

Consider the two-component example system in Section 3.2 with the original probabilities $p_1 = p_2 = 0.1$. Assume that redundancy can be allocated by securing the component 1 with a parallel configuration of $d_1 = 2$ identical components and the component 2 with a parallel configuration of $d_2 = 3$ identical components.

In addition, if the proportion of common-cause failures to all failures were $\beta = 0.1$, the reduced probabilities would be $p_1^r = 0.01802$ and $p_2^r = 0.01072$. These probabilities are computed from Equation (29).

Now, assume that it were cheaper to acquire three components identical to the component 2 than two components identical to the component 1. In this case, the optimal way of allocating redundancy would be to secure the component 2 with a parallel configuration of $d_2 = 3$ identical components. This is because $p_2^r = 0.01072 < 0.01802 = p_1^r$.

# 5 Analysis of epistemic uncertainties

In probabilistic risk assessment, failure probabilities are often based on expert opinions [2]. However, these opinions are prone to biases, such as overconfidence and anchoring. Also, expertise is often gathered from multiple experts from different fields, which results in a need of combining the opinions of these experts. Furthermore, the failure probabilities to be estimated are related to events that are typically rare, and, thus, estimation using statistical methods is based on only a few observations. For these reasons, estimating a failure probability by aggregating the information and expertise available to a single point estimate may exaggerate the current knowledge of the probability.

Epistemic uncertainties are uncertainties that originate from the lack of knowledge [14]. In contrast, aleatory uncertainties are uncertainties that originate from inherent variation (contingencies) in a system. While aleatory uncertainties are irreducible, epistemic uncertainties can be reduced by obtaining new observations.

Epistemic uncertainties in failure probabilities can be modelled with probability intervals. The end points of an interval define the range in which the probability is estimated to locate. Consequently, a point-estimate probability $p$ can be converted to a probability interval, e.g., by defining the interval $[p - \epsilon, p + \epsilon]$, where the parameter $\epsilon$ describes the uncertainty in the failure probability.

Obtaining new observations can result in the change of probability intervals. For example, if a failure probability is estimated to locate in the interval $[0.03, 0.06]$ and new knowledge is obtained, the interval may be reduced to $[0.04, 0.05]$. After this interval reduction, the failure probability is estimated to be known more accurately than before. However, the opposite could occur equally well. That is, the interval may be changed to $[0.02, 0.07]$ if new knowledge reveals that the originally estimated interval was too narrow to describe the confidence on the failure probability.

## 5.1 Dominance relation

With probability intervals, risk reduction portfolios can be compared through dominance relations. These relations are determined by system unreliability $Q$, which is approximated by the rare event approximation

$$Q\left(\mathbf{p}, \mathbf{b}\right) \approx \sum\nolimits_{j=1}^{N} \prod\nolimits_{i \in MCS_j} \left(p_i\right)^{1-b_i} \cdot \left(p_i^r\right)^{b_i},$$

where $\mathbf{p}$ is a vector containing basic event probabilities $p_i$, $\mathbf{b}$ is the binary indicator vector of a portfolio $P$ defined in Equation (1) and (2), $N$ is the number of minimal cut sets and reduced probabilities $p_i^r < p_i$ are computed as a function of original probabilities $p_i$, e.g., from Equation (29).

**Definition 1** *Portfolio $P_1$ ($\boldsymbol{b}_1$) dominates portfolio $P_2$ ($\boldsymbol{b}_2$), denoted, $P_1 \succ P_2$, with budget level $B$ if and only if $\sum_{i=1}^{n} c_i b_{k,i} \leq B \; \forall k \in \{1, 2\}$ and*

$$\begin{array}{ll} \text{(i)} & \forall \mathbf{p} \in [0,1]^n: \quad \mathbf{p}_{lb} \leq \mathbf{p} \leq \mathbf{p}_{ub}, \quad Q\left(\mathbf{p}, \mathbf{b}_1\right) \leq Q\left(\mathbf{p}, \mathbf{b}_2\right) \\ \text{(ii)} & \exists \mathbf{p} \in [0,1]^n: \quad \mathbf{p}_{lb} \leq \mathbf{p} \leq \mathbf{p}_{ub}, \quad Q\left(\mathbf{p}, \mathbf{b}_1\right) < Q\left(\mathbf{p}, \mathbf{b}_2\right) \end{array},$$

where $n$ is the number of components, $c_i$ is the cost incurred by reducing original probability $p_i$ to $p_i^r$, the vector $\mathbf{p}_{lb}$ contains the lower bounds of the intervals and the vector $\mathbf{p}_{ub}$ the upper bounds.

Definition 1 implies that dominance relations form a partial order. That is, they are irreflexive, asymmetric and transitive. Irreflexivity means that a portfolio cannot dominate itself, i.e., $P_i \not\succ P_i \; \forall i$. Asymmetricity implies that $P_i \succ P_j \Rightarrow P_j \not\succ P_i \; \forall i \neq j$. Transitivity gives: $P_i \succ P_j$ and $P_j \succ P_k \Rightarrow P_i \succ P_k \; \forall i, j, k$. From these properties it follows that such pairs of portfolios may exist that neither of the portfolios dominates the other. Especially, the set of portfolios that are not dominated by any other portfolio may contain more than one portfolio. These non-dominated portfolios are interesting for a decision maker because no other portfolio can yield lower unreliability for any probabilities $\mathbf{p}$: $\mathbf{p}_{lb} \leq \mathbf{p} \leq \mathbf{p}_{ub}$ [15].

The set of non-dominated portfolios can be approximated by optimal risk reduction portfolios with point-estimate probabilities. If a risk reduction portfolio $P_o$ is the unique optimum with the probabilities $\mathbf{p}_0$, i.e., no other portfolio yields equally low unreliability with $\mathbf{p}_0$, it follows that the condition (i) in Definition 1 cannot hold for any dominance comparison where it is investigated if some other portfolio dominates $P_o$. However, if $P_o$ is not unique, then it may not be a non-dominated portfolio because another portfolio $P_1$ may exist that dominates $P_0$. In that case, also $P_1$ would be optimal with the probabilities $\mathbf{p}_0$ because otherwise the condition (i) in Definition 1 would not hold for the dominance $P_1 \succ P_0$. In addition, it is noteworthy that a non-dominated portfolio may not be optimal for any fixed $\mathbf{p}_0 \in [0,1]^n : \mathbf{p}_{lb} \leq \mathbf{p}_0 \leq \mathbf{p}_{ub}$ [16].

However, in this thesis it is not investigated whether an optimal risk reduction portofolio is the unique optimum (if such exists), and for this reason, an optimal portfolio is called a potentially non-dominated portfolio and the set of them is said to be approximative with respect to the set of non-dominated portfolios. Potentially non-dominated portfolios are computed by selecting point estimates of failure probabilities randomly from their respective intervals and solving the corresponding optimal risk reduction portfolios.

## 5.2 Core index

Basic events under probability intervals can be analysed with core indices. The concept of core index is defined in [16] as a part of robust portfolio modeling (RPM) methodology. The core index $CI$ of a basic event $BE$ denotes the proportion of non-dominated portfolios containing the event to all non-dominated portfolios and is denoted as

$$CI\left(BE, \mathbf{p}_{lb}, \mathbf{p}_{ub}, B\right) = \frac{\left|\left\{P \in P_N\left(\mathbf{p}_{lb}, \mathbf{p}_{ub}, B\right) \mid BE \in P\right\}\right|}{\left|P_N\left(\mathbf{p}_{lb}, \mathbf{p}_{ub}, B\right)\right|},$$

where $P_N\left(\mathbf{p}_{lb}, \mathbf{p}_{ub}, B\right)$ denotes the set of non-dominated portfolios with the probability intervals $\mathbf{p}_{lb} \leq \mathbf{p} \leq \mathbf{p}_{ub}$ and budget $B$.

The core index $CI$ of a basic event $BE$ can be approximated by solving $N_{pnd}\left(\mathbf{p}_{lb}, \mathbf{p}_{ub}, B\right)$ potentially non-dominated portfolios and by computing the fraction

$$CI\left(BE, \mathbf{p}_{lb}, \mathbf{p}_{ub}, B\right) \approx \frac{\sum_{k=1}^{N_{pnd}\left(\mathbf{p}_{lb}, \mathbf{p}_{ub}, B\right)} \chi_k\left(BE\right)}{N_{pnd}\left(\mathbf{p}_{lb}, \mathbf{p}_{ub}, B\right)}, \tag{30}$$

where $\chi_k$ denotes the characteristic function of the $k$:th potentially non-dominated portfolio. That is, $\chi_k\left(BE\right) = 1$ if the basic event $BE$ belongs to the $k$:th portfolio and $\chi_k(BE) = 0$ in the opposite case. In this thesis, only approximations of core indices are computed. This is accomplished by selecting point estimates of failure probabilities from their respective intervals and solving the optimal risk reduction portfolio problem for $N_{MILP}$ times. This yields a set of $N_{pnd}\left(\mathbf{p}_{lb}, \mathbf{p}_{ub}, B\right) \leq N_{MILP}$ potentially non-dominated portfolios. The cardinality of the set can be smaller than the number of MILP problems solved because the solutions of several MILP problems can be the same.

Core indices divide basic events into three categories. First, the basic events with core index equal to 1 are called core events. They belong to all non-dominated portfolios and reducing their probabilities should be prioritized. Second, the basic events with core index less than 1 but greater than 0 are called border events. Finally, the basic events with core index equal to 0 are called exterior events. They do not belong to a single non-dominated portfolio and reducing their probabilities should be the last priority.

# 6 Computations and results

Two types of computational experiments are conducted. First, it is studied how budget affects on system unreliability and on the contents of optimal risk reduction portfolios. This is accomplished by solving optimal risk reduction portfolios when budget varies between the maximal value that results in an empty portfolio and the minimal value that results in a portfolio containing all components. This type of an experiment is referred to as a budget experiment. Second, uncertainties on failure probabilities are modeled as probability intervals and non-dominated portfolios and core indices are computed. This type of an experiment is referred to as an interval experiment.

Instead of exact system unreliability, the rare event approximation is utilized. This approximation simplifies the sumproduct expression of system unreliability by reducing the number of terms, and it provides an upper bound that is accurate enough when all basic events have low probabilities [10]. In addition, only potentially non-dominated portfolios are computed by solving optimal risk reduction portfolios when failure probabilities are selected randomly from their respective intervals. Based on potentially non-dominated portfolios, approximative core indices are computed from Equation (30).

Experiments were performed with two data sets: an example system consisting of seven components and a residual heat removal system (RHRS) of a nuclear reactor. Both data sets are the same as in [17], and the latter is said to be representative instead of exact in terms of fault tree structure and failure probabilities. The data sets do not include information on costs of reducing failure probabilities. All costs were set to the value of 1.0, which simplifies the computations. Also, the data sets do not contain any information on reduced failure probabilities. It was assumed that each component can be secured with another component in a parallel configuration, so the degree of redundancy was $d = 2$. The CCFs were taken into account by utilizing the beta factor model with the parameter value $\beta = 0.1$. The reduced failure probabilities were computed from Equation (29).

All MILP problems are solved with CPLEX 12.4 [18]. CPLEX was run on a system with an Intel Core i3-2330M CPU @ 2.20 GHz and 4 GB of RAM.

## 6.1 Example system with seven components

The reliability block diagram of the system is illustrated in Figure 3. The diagram consists of In, Out and component nodes and paths between the nodes. Because the system is functioning when there is a path of working components from In node to Out node, the minimal cut sets of the system can be derived from the diagram. The minimal cut sets are listed in Table 5.

In [17] this system was analysed under interval probabilities, and one choice of intervals was $[0.01, 0.03]$ for each component. The same interval for each component is used also in this thesis in the interval experiment of this system,

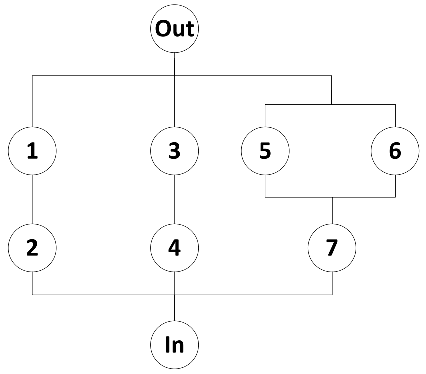

Figure 3: The reliability block diagram of a system with seven components. The system is functioning when there is a path consisting of working components from the In node to the Out node.

Table 5: The minimal cut sets of the example system with seven components.

| | | | |
|---|---|---|---|
| 1. $\{1,3,7\}$ | 3. $\{2,3,7\}$ | 5. $\{1,3,5,6\}$ | 7. $\{2,3,5,6\}$ |
| 2. $\{1,4,7\}$ | 4. $\{2,4,7\}$ | 6. $\{1,4,5,6\}$ | 8. $\{2,4,5,6\}$ |

and in the budget experiment the original probabilities were chosen to be the midpoints of the intervals, i.e., $p = 0.02$. Thus, the reduced probabilities in the budget experiment were $p^r = 2.3234 \cdot 10^{-3}$, which was obtained from Equation (29) with the parameter values $p = 0.02$, $d = 2$ and $\beta = 0.1$.

The optimal risk reduction portfolio MILP problem for this system contains 35 decision variables, of which seven are binary indicator variables and 28 real-valued probability products. In addition, the MILP problem contains 89 constraints.

### Budget experiment

Eight MILP problems were solved in the budget experiment. The total computing time that CPLEX reported was 0.2964 s while the average computing time for one MILP problem was 0.03705 s.

The results of the budget experiment are drawn in Figure 4 and Figure 5. Figure 4 represents system unreliability $Q$ as a function of budget $B$ in both the optimal and the worst case. Figure 5 represents the optimal risk reduction portfolios $P$ as a function of budget $B$.

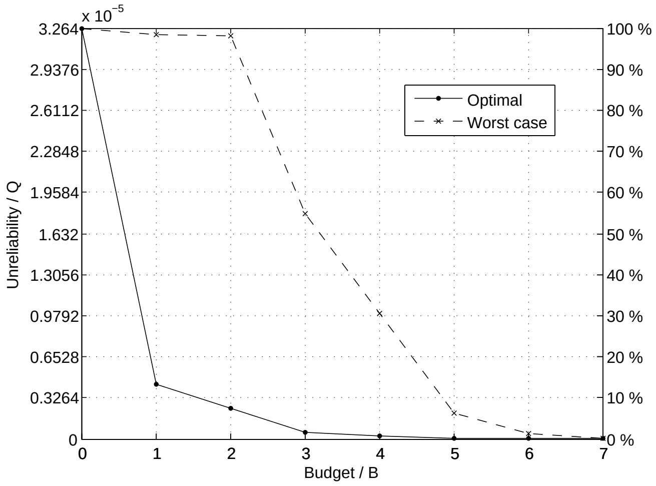

Figure 4: System unreliability $Q$ as a function of budget $B$ in the example system with seven components. Unreliability $Q$ is represented in both the optimal and in the worst case.

Figure 4 shows that unreliability $Q$ can be reduced to less than 15 % of its original value by investing to securing just one component. On the other hand, it can also be seen that investing to securing more than three components would yield at maximum only the reduction of 1.4 percentage points in unreliability compared to the situation where exactly three components were secured. When all the components are secured, unreliability is reduced to $Q = 5.028 \cdot 10^{-8}$, which is 0.1541 % of its original value. Figure 4 shows also that the difference between the optimal solutions and the worst solutions is notable.

Figure 5 shows that when a single component can be secured, the best choice is the component 7. This can be explained as the follows. Table 5 shows that there are four minimal cut sets of both cardinalities three (the minimal cut sets 1-4) and four (the minimal cut sets 5-8). All components belong to four minimal cut sets, and the component 7 belongs to all minimal cut sets of cardinality three. Thus, when failure probabilities are equal, reducing the failure probability of the component 7 reduces the objective function the most. With similar reasoning, it can be inferred that components 1-4 are the next best choices because each of them belongs to two minimal cut sets of cardinality three and two of cardinality four. Finally, components 5 and 6 should be the last choices because they are in all minimal cuts sets of cardinality four. That is, reducing their probabilities reduces the objective

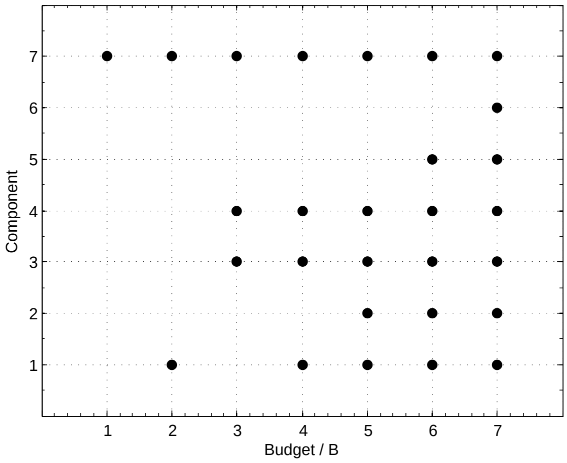

Figure 5: The optimal risk reduction portfolios $P$ as a function of budget $B$ in the example system with seven components. A component is marked with a dot if it belongs to an optimal portfolio $P$ with a budget $B$.

function the least. The described selection order can be observed in Figure 5.

### Interval experiment

In the interval experiment, the budget was fixed to $B = 4$, i.e., four components out of seven could be secured. In total, 200 MILP problems were solved, which yield $N_{pnd} = 4$ potentially non-dominated portfolios. That is, the solutions of the 200 MILP problems contained four different portfolios. The total computing time that CPLEX reported was 8.1901 s while the average computing time for one MILP problem was 0.04095 s.

The frequencies $f$ of the components in the solutions of the 200 MILP problems are presented in Figure 6. The figure shows that the component 7 belongs to all computed portfolios and the remaining three components are selected from the set $\{1, 2, 3, 4\}$ while the components 5 and 6 do not belong to any optimal portfolio.

As Figure 6 implies, the $N_{pnd} = 4$ potentially non-dominated portfolios consist of the component 7 and three of the components 1, 2, 3 and 4. Consequently, the core indices were $CI \approx 3/4$ for the components 1-4, $CI \approx 0$ for the components 5-6 and $CI \approx 1$ for the component 7. Thus, the component 7

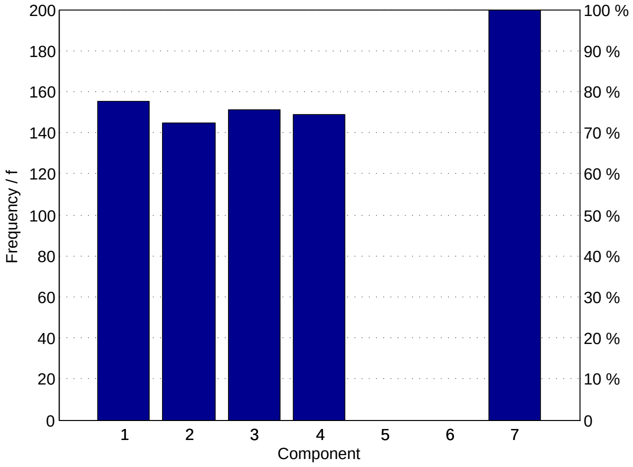

Figure 6: The frequencies $f$ of the example system components in the optimal solutions of the 200 MILP problems. The failure probabilities were taken from probability intervals.

can be called a core component, the components 1-4 border components and the components 5-6 exterior components. The approximations were computed from Equation (30).

## 6.2 Residual heat removal system

The system consists of 31 components and 147 minimal cut sets. The failure probability point estimates and intervals and the minimal cut sets are presented in Appendix A. The optimal risk reduction portfolio MILP problem for this system contains 363 decision variables, of which 31 are binary indicator variables and 332 real-valued probability products. In addition, the MILP problem contains 888 constraints.

### Budget experiment

In the budget experiment, 32 MILP problems were solved. The total computing time that CPLEX reported was 7.0668 s while the average computing time for one MILP problem was 0.2208 s.

The results of the budget experiment are drawn in Figures 7 and 8. Figure 7

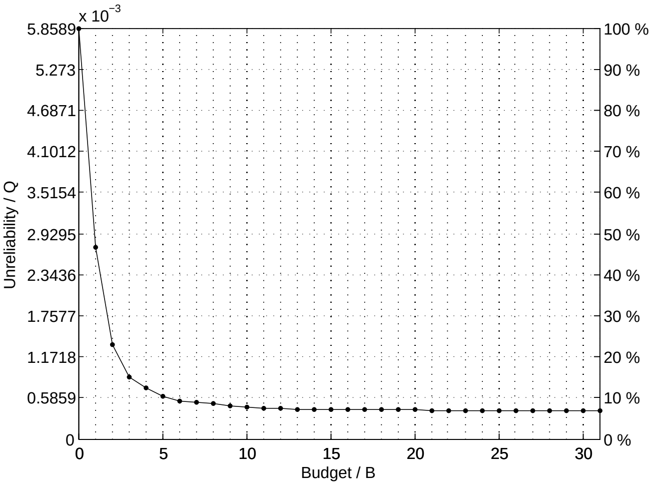

Figure 7: System unreliability $Q$ as a function of budget $B$ in the residual heat removal system.

shows system unreliability $Q$ and Figure 5 optimal risk reduction portfolios $P$ as functions of budget $B$. According to Figure 7, securing one component reduces unreliability to 46.71 % of its original value and securing six components reduces it to 9.34 %. Securing all 31 components reduces unreliability to 6.97 %.

The components in the RHRS data set are sorted according to their Fussel-Vesely risk importance measure values. These values measure the fractional contribution of a component to the overall risk [19]. Figure 8 shows that the selection order of the components roughly resembles the Fussel-Vesely risk importance measure order. That is, first, the component 1 is selected, second, the component 2 is selected etc.

### Interval experiment

In the interval experiment, the budget was fixed to $B = 10$, i.e., ten components out of 31 could be secured. In total, 4000 MILP problems were solved, which yield $N_{pnd} = 97$ potentially non-dominated portfolios. That is, the solutions of the 4000 MILP problems contained 97 different portfolios. The total computing time that CPLEX reported was 967.0 s while the average computing time for one MILP problem was 0.2418 s.

The core indices of the components were computed from Equation (30) and

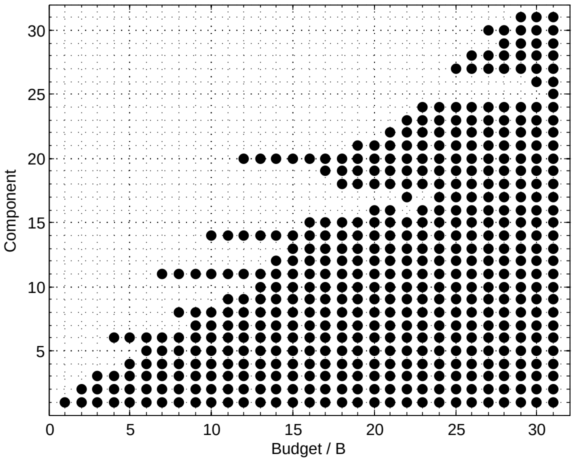

Figure 8: The optimal risk reduction portfolios $P$ as a function of budget $B$ in the residual heat removal system. A component is marked with a dot if it belongs to an optimal portfolio $P$ with a budget $B$.

are presented in Figure 9. The figure shows that the components 1, 2, 3 and 6 can be considered as core components while the components 16, 19 and 21-31 can be considered as exterior components. The remaining components are categorized border components.

The distribution of the 97 portfolios in the 4000 MILP problem solutions is presented in Figure 10, which demonstrates the difference in using probability intervals instead of point estimates. While the optimal portfolio with the highest frequency of 702 is the same as the optimal portfolio with point estimate probabilities and budget $B = 10$ shown in Figure 8, now also other potentially equally good, i.e., non-dominated, alternatives exist.

An interval experiment was repeated for budgets $B = 5, 10, ..., 30$ to see how core indices $CI$ behave as a function of budget. For each budget $B$, 1000 MILP problems were solved and core indices of the components were computed from Equation (30). The results are displayed in Figure 11. The figure shows that for most of the components core index is increasing as a function of budget. The only exception is the component 28, whose core index is $CI \approx 0.0164$ with the budget $B = 10$ and $CI \approx 0$ with $B = 15$. However, this is difficult to observe in Figure 11. Also [15] shows a case in which robust portfolio modeling is applied and not all core indices were monotonous functions of budget.

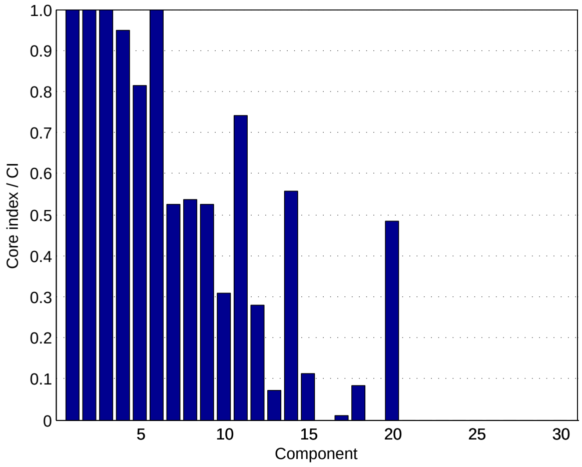

Figure 9: The core indices $CI$ of the components in the RHRS when 4000 MILP problems were solved yielding 97 different portfolios and the point estimates of failure probabilities were taken from probability intervals.

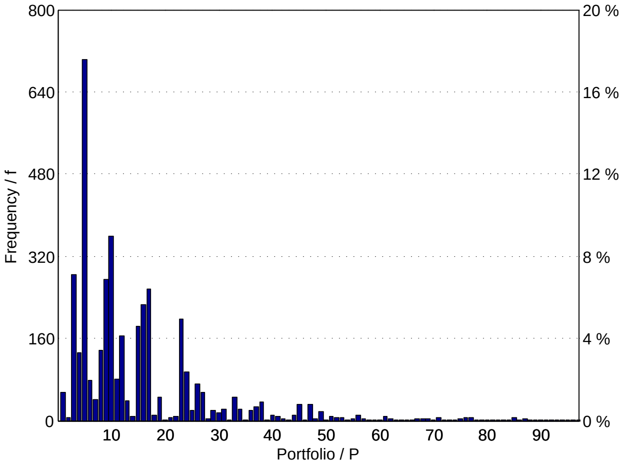

Figure 10: The distribution of optimal portfolios $P$ in the interval experiment of the RHRS. In total, 4000 MILP problems were solved, which yield 97 potentially non-dominated portfolios.

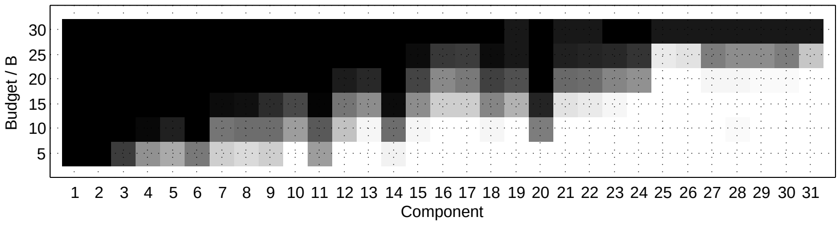

Figure 11: The core indices $CI$ of the components in the RHRS as a function of budget $B$. The darker the rectangle of a component, the closer the core index of the component is to 1.0. That is, the core index of 1.0 is marked as a black rectangle and the core index of 0.0 as a white rectangle. For each budget $B$, 1000 MILP problems were solved.

# 7 Discussion

This thesis develops a MILP model that minimizes unreliability of a system that is presented as a fault tree. In contrast, the reliability optimization models of Cho and Sung [5], Kuo and Prasad [6] and Feizollahi and Modarres [7] assume more on system structure. Fault trees enable a detailed analysis of system failure and are widely applied in different fields of industry.

Minimization in the MILP model of this thesis is subject to two types of constraints. First, the reduction of component failure probability has a cost. Second, the overall cost of risk reduction is not allowed to exceed a budget. This budget constraint is similar to the budget constraint in the problem formulation of Cho and Sung and dissimilar to the formulations of Kuo and Prasad and Feizollahi and Modarres. That is, in this study the costs of reducing failure probabilities are commensurable while risk reduction of a component may consume many different types of resources in the formulations of Kuo and Prasad and Feizollahi and Modarres.

The MILP problem formulation in Section 3.1 contains redundant decision variables. This is because the intersection of minimal cut sets may not be empty. For example, if a system contained the minimal cut sets $MCS_1 = \{1, 2, 3\}$ and $MCS_2 = \{1, 2, 4\}$, then the MILP problem would have six probability product decision variables for the probabilities of these MCSs. However, it would be sufficient to have only four of them because $MCS_1 \bigcap MCS_2 = \{1, 2\}$ and the first two probability product variables could be common for both MCSs.

The MILP model can be applied in optimal redundancy allocation to determine which components should be replaced with parallel configurations of identical components to minimize system unreliability. However, the degrees of redundancy are assumed to be known for each component unlike in the models of Kuo and Prasad and Feizollahi and Modarres. In these models, also the degrees of redundancy are solved. The model in this thesis can take CCFs into account, e.g., with the beta factor model. On the other hand, if the proportion of CCFs to independent failures is large for a parallel configuration of identical components, then it may not be reasonable to allocate redundancy for this type of components at all.

The model of this thesis was utilized with two systems to analyze which components in a system should be secured when a budget is reserved for securing. The model was utilized also in the case where failure probabilities were uncertain. In this case, failure probabilities were modeled as probability intervals instead of point estimates. With probability intervals, the model of this thesis does not yield exact solutions unlike the model of Feizollahi and Modarres.

MILP problems were solved with CPLEX that features a feasibility tolerance parameter to control how much the constraints of a model are allowed to be violated [20]. However, the minimum value of this parameter is $10^{-9}$, which is high for the MILP model. The problem with the parameter was alleviated with the scaling method presented in Section 3.3. Without scaling, it was sometimes observed that probability products were rounded to zeros, which in turn resulted in incorrect results.

CPLEX may terminate optimization if it has found a solution that is provably sufficiently close to the optimal solution [21]. This can cause inaccuracies in the results of computations. For each solution, CPLEX reports a relative optimality gap (ROG) that denotes how close the solution is relatively to the optimal solution. For instance, if the ROG were 0.05, then CPLEX might terminate optimization after it has found a solution that is within five percent of the optimum. For the vast majority of the MILP problem computations CPLEX reported ROGs of 0.00 %. The remaining ROGs were mostly 1.00 %, but in the worst case a ROG of 62.00 % was observed.

# 8 Conclusions

The computations with the seven-component example system show that the MILP model in this thesis is applicable to analyse optimal risk reduction of systems. These computations show also that the model is applicable when uncertainties of failure probabilities are modeled with probability intervals. However, with this model, it is not possible to solve exact solutions when probability intervals are utilized. In addition, the quality of these approximative solutions, i.e., how close they are to the exact solutions, is not analysed in this thesis. In addition, the model can be applied in optimal redundancy allocation.

The MILP model can be utilized with any system that can be described as a fault tree. This set of systems is extensive and includes, e.g., a residual heat removal system of a nuclear reactor that was analysed in this thesis. The optimal risk reduction portfolios for the RHRS were computed as a function of budget in 7.0668 s. This shows that the model can be utilized in a reasonable time with problems based on real-world data. The optimal risk reduction portfolios suggest that the optimal order of securing components in the RHRS is roughly the same order as the Fussel-Vesely risk importance order of the components. With probability intervals, 97 potentially non-dominated portfolios of ten components were found. The core index approximations suggested that the securing of the components 1, 2, 3 and 6 should be prioritized while the securing of the components 16, 19 and 21-31 should be the last priority.

# References

[1] ASN Aircraft accident Boeing 707-328 F-BHSM Paris-Orly Airport (ORY). `http://www.aviation-safety.net/database/record.php?id=19620603-0`. Viewed 26.8.2013.

[2] Bedford, T., Cooke, R. Probabilistic Risk Assessment: Foundations and Methods. Cambridge University Press, 2003.

[3] Keller, W., Modarres, M. A Historical Overview of Probabilistic Risk Assessment Development and Its Use in the Nuclear Power Industry: A Tribute to the Late Professor Norman Carl Rasmussen. Reliability Engineering and System Safety. Volume 89 (2005), Issue 3, Pages 271-285.

[4] Kuo, W., Wan, R. Recent Advances in Optimal Reliability Allocation. IEEE Transactions on Systems, Man and Cybernetics. Volume 37 (2007), Issue 2, Pages 143-156.

[5] Cho, Y.K., Sung, C.S. Reliability Optimization of a Series System with Multiple-Choice and Budget Constraints. European Journal of Operational Research, Volume 127 (2000), Issue 1, Pages 159-171.

[6] Kuo, W., Prasad, V.R. Reliability Optimization of Coherent Systems. IEEE Transactions on Reliability, Volume 49 (2000), Issue 3, Pages 323-330.

[7] Feizollahi, M.J., Modarres, M. The Robust Deviation Redundancy Allocation Problem With Interval Component Reliabilities. IEEE Transactions on Reliability, Volume 61 (2012), Issue 4. Pages 957-965.

[8] Modarres, M. Risk Analysis in Engineering: Techniques, Tools and Trends. CRC Press, 2006.

[9] Larsen, A., Musgrave, G., Sgobba, T. Safety Design for Space Systems. Elsevier, 2009.

[10] Collet, J. Some Remarks on Rare-Event approximation. IEEE Transactions on Reliability. Volume 45 (1996), Issue 1, Pages 106-108.

[11] Gibson, G., Katz, R.H., Patterson, D.A. A Case for Redundant Arrays of Inexpensive Disks (RAID). Proceedings of ACM SIGMOD. Chicago, IL, June 1988.

[12] Fleming, K.N. Reliability Model for Common Mode Failures in Redundant Safety Systems. General Atomic Report, GA 13284, 1974.

[13] Goble, W.M. Estimating the Common Cause Beta Factor. http://www.exida.com/articles/Estimatingthebetafactor1.pdf. Viewed 9.7.2013.

[14] Eldred, M., Jakeman, J., Xiu, D. Numerical Approach for Quantification of Epistemic Uncertainty. Journal of Computational Physics, Volume 229 (2010), Issue 12, Pages 4425-4854.

[15] Liesiö, J., Mild, P., Salo, A. Robust Portfolio Modeling with Incomplete Cost Information and Project Interdependencies. European Journal of Operational Research, Volume 190 (2008), Issue 3, Pages 679-695.

[16] Liesiö, J., Mild, P., Salo, A. Preference Programming for Robust Portfolio Modeling and Project Selection. European Journal of Operational Research, Volume 181 (2007), Issue 3, Pages 1488-1505.

[17] Salo, A., Toppila, A. A Computational Framework for Prioritization of Events in Fault Tree Analysis Under Interval-Valued Probabilities. IEEE Transactions on Reliability. Volume 62 (2013), Issue 3, Pages 583-595.

[18] CPLEX Optimizer. http://www-01.ibm.com/software/commerce/optimization/cplex-optimizer/. Viewed 14.7.2013.

[19] Davis, T.C., Denning, R.S., Saltos, N., Vesely, W.E.. Measures of Risk Importance and Their Applications. NUREG/CR-4377, Washington, D.C., 1985.

[20] CPLEX feasibility tolerance. http://pic.dhe.ibm.com/infocenter/cosinfoc/v12r4/topic/ilog.odms.cplex.help/CPLEX/Parameters_reference/topics/EpRHS.html. Viewed 16.7.2013.

[21] Terminating MIP optimization. http://pic.dhe.ibm.com/infocenter/cosinfoc/v12r4/topic/ilog.odms.cplex.help/CPLEX/User_manual/topics/uss_solveMIP_11.html. Viewed 23.7.2013.

# A Residual heat removal system data

The data of the system is the same as in [17].

The component failure probabilities, both point estimates and intervals, and the Fussel-Vesely risk importance values of the RHRS.

| Component | Point estimate | Lower bound | Upper bound | Fussell-Vesely |
|---|---|---|---|---|
| 1 | 3.48E-03 | 1.45E-03 | 1.31E-02 | 5.97E-01 |
| 2 | 3.13E-02 | 9.28E-03 | 8.35E-02 | 2.72E-01 |
| 3 | 3.13E-02 | 9.28E-03 | 8.35E-02 | 2.37E-01 |
| 4 | 1.00E-02 | 4.58E-03 | 1.83E-02 | 6.97E-02 |
| 5 | 1.00E-02 | 4.58E-03 | 1.83E-02 | 5.86E-02 |
| 6 | 1.68E-04 | 7.00E-05 | 6.30E-04 | 2.88E-02 |
| 7 | 3.35E-03 | 8.93E-04 | 8.04E-03 | 2.54E-02 |
| 8 | 3.35E-03 | 8.93E-04 | 8.04E-03 | 2.54E-02 |
| 9 | 1.51E-03 | 4.48E-04 | 4.03E-03 | 1.31E-02 |
| 10 | 1.51E-03 | 4.48E-04 | 4.03E-03 | 1.14E-02 |
| 11 | 2.40E-03 | 3.84E-04 | 9.60E-03 | 7.13E-03 |
| 12 | 6.00E-04 | 1.60E-04 | 1.44E-03 | 5.21E-03 |
| 13 | 6.00E-04 | 1.60E-04 | 1.44E-03 | 4.54E-03 |
| 14 | 1.92E-05 | 8.00E-06 | 7.20E-05 | 3.29E-03 |
| 15 | 3.36E-04 | 4.17E-05 | 1.04E-03 | 2.92E-03 |
| 16 | 5.79E-02 | 1.71E-02 | 1.54E-01 | 2.82E-03 |
| 17 | 5.79E-02 | 1.71E-02 | 1.54E-01 | 2.66E-03 |
| 18 | 6.43E-03 | 2.68E-03 | 2.41E-02 | 2.64E-03 |
| 19 | 3.36E-04 | 4.17E-05 | 1.04E-03 | 2.54E-03 |
| 20 | 1.20E-05 | 5.00E-06 | 4.50E-05 | 2.06E-03 |
| 21 | 1.73E-04 | 5.12E-05 | 4.61E-04 | 1.50E-03 |
| 22 | 1.73E-04 | 5.12E-05 | 4.61E-04 | 1.31E-03 |
| 23 | 1.08E-04 | 3.20E-05 | 2.88E-04 | 9.38E-04 |
| 24 | 1.08E-04 | 3.20E-05 | 2.88E-04 | 8.18E-04 |
| 25 | 1.00E-02 | 4.58E-03 | 1.83E-02 | 4.45E-04 |
| 26 | 1.00E-02 | 4.58E-03 | 1.83E-02 | 4.19E-04 |
| 27 | 2.40E-05 | 9.00E-07 | 9.00E-05 | 2.08E-04 |
| 28 | 2.40E-05 | 9.00E-07 | 9.00E-05 | 2.08E-04 |
| 29 | 2.40E-05 | 9.00E-07 | 9.00E-05 | 1.82E-04 |
| 30 | 2.40E-05 | 9.00E-07 | 9.00E-05 | 1.82E-04 |
| 31 | 1.00E-07 | 3.93E-10 | 3.54E-07 | 1.72E-05 |

# The minimal cut sets of the RHRS.

| No | Probability | Components | | |
|---|---|---|---|---|
| 1 | 3.48E-03 | 1 | | |
| 2 | 9.81E-04 | 3 | 2 | |
| 3 | 3.13E-04 | 5 | 2 | |
| 4 | 3.13E-04 | 4 | 3 | |
| 5 | 1.68E-04 | 6 | | |
| 6 | 1.05E-04 | 2 | 7 | |
| 7 | 1.05E-04 | 8 | 2 | |
| 8 | 4.73E-05 | 10 | 2 | |
| 9 | 4.73E-05 | 9 | 3 | |
| 10 | 3.35E-05 | 8 | 4 | |
| 11 | 3.35E-05 | 4 | 7 | |
| 12 | 1.92E-05 | 14 | | |
| 13 | 1.88E-05 | 12 | 3 | |
| 14 | 1.88E-05 | 13 | 2 | |
| 15 | 1.54E-05 | 18 | 11 | |
| 16 | 1.51E-05 | 5 | 9 | |
| 17 | 1.51E-05 | 4 | 10 | |
| 18 | 1.20E-05 | 20 | | |
| 19 | 1.05E-05 | 15 | 3 | |
| 20 | 1.05E-05 | 19 | 2 | |
| 21 | 8.03E-06 | 16 | 17 | 11 |
| 22 | 6.00E-06 | 5 | 12 | |
| 23 | 6.00E-06 | 4 | 13 | |
| 24 | 5.41E-06 | 2 | 22 | |
| 25 | 5.41E-06 | 3 | 21 | |
| 26 | 5.06E-06 | 9 | 7 | |
| 27 | 5.06E-06 | 8 | 9 | |
| 28 | 4.34E-06 | 17 | 11 | 2 |
| 29 | 4.34E-06 | 16 | 11 | 3 |
| 30 | 3.38E-06 | 24 | 2 | |
| 31 | 3.38E-06 | 23 | 3 | |
| 32 | 3.36E-06 | 5 | 15 | |
| 33 | 3.36E-06 | 4 | 19 | |
| 34 | 2.28E-06 | 10 | 9 | |
| 35 | 2.01E-06 | 8 | 12 | |
| 36 | 2.01E-06 | 12 | 7 | |
| 37 | 1.73E-06 | 4 | 22 | |
| 38 | 1.73E-06 | 5 | 21 | |
| 39 | 1.39E-06 | 17 | 25 | 11 |
| 40 | 1.39E-06 | 16 | 26 | 11 |
| 41 | 1.39E-06 | 16 | 11 | 5 |
| 42 | 1.39E-06 | 17 | 11 | 4 |
| 43 | 1.13E-06 | 8 | 15 | |
| 44 | 1.13E-06 | 15 | 7 | |
| 45 | 1.08E-06 | 23 | 5 | |
| 46 | 1.08E-06 | 24 | 4 | |
| 47 | 9.06E-07 | 10 | 12 | |
| 48 | 9.06E-07 | 13 | 9 | |
| 49 | 7.52E-07 | 29 | 2 | |
| 50 | 7.52E-07 | 30 | 2 | |
| 51 | 7.52E-07 | 28 | 3 | |
| 52 | 7.52E-07 | 27 | 3 | |
| 53 | 7.51E-07 | 25 | 11 | 3 |
| 54 | 7.51E-07 | 26 | 11 | 2 |
| 55 | 5.79E-07 | 21 | 7 | |
| 56 | 5.79E-07 | 8 | 21 | |
| 57 | 5.07E-07 | 10 | 15 | |
| 58 | 5.07E-07 | 9 | 19 | |
| 59 | 4.65E-07 | 16 | 8 | 11 |
| 60 | 4.65E-07 | 16 | 11 | 7 |
| 61 | 3.62E-07 | 23 | 8 | |
| 62 | 3.62E-07 | 23 | 7 | |
| 63 | 3.60E-07 | 13 | 12 | |
| 64 | 2.61E-07 | 9 | 22 | |
| 65 | 2.61E-07 | 10 | 21 | |
| 66 | 2.40E-07 | 5 | 28 | |
| 67 | 2.40E-07 | 27 | 5 | |
| 68 | 2.40E-07 | 4 | 29 | |
| 69 | 2.40E-07 | 30 | 4 | |
| 70 | 2.40E-07 | 26 | 11 | 4 |
| 71 | 2.40E-07 | 25 | 11 | 5 |
| 72 | 2.10E-07 | 16 | 11 | 10 |
| 73 | 2.10E-07 | 17 | 11 | 9 |
| 74 | 2.02E-07 | 12 | 19 | |
| 75 | 2.02E-07 | 13 | 15 | |
| 76 | 1.63E-07 | 24 | 9 | |
| 77 | 1.63E-07 | 23 | 10 | |
| 78 | 1.13E-07 | 19 | 15 | |
| 79 | 1.04E-07 | 12 | 22 | |
| 80 | 1.04E-07 | 13 | 21 | |
| 81 | 1.00E-07 | 31 | | |
| 82 | 8.32E-08 | 16 | 11 | 13 |
| 83 | 8.32E-08 | 17 | 11 | 12 |
| 84 | 8.05E-08 | 8 | 28 | |
| 85 | 8.05E-08 | 27 | 8 | |
| 86 | 8.05E-08 | 28 | 7 | |
| 87 | 8.05E-08 | 27 | 7 | |
| 88 | 8.04E-08 | 8 | 25 | 11 |
| 89 | 8.04E-08 | 25 | 11 | 7 |
| 90 | 6.48E-08 | 24 | 12 | |
| 91 | 6.48E-08 | 23 | 13 | |
| 92 | 5.80E-08 | 19 | 21 | |
| 93 | 5.80E-08 | 15 | 22 | |
| 94 | 4.66E-08 | 16 | 11 | 19 |
| 95 | 4.66E-08 | 17 | 11 | 15 |
| 96 | 3.63E-08 | 23 | 19 | |
| 97 | 3.63E-08 | 24 | 15 | |
| 98 | 3.63E-08 | 29 | 9 | |
| 99 | 3.63E-08 | 28 | 10 | |
| 100 | 3.63E-08 | 27 | 10 | |
| 101 | 3.63E-08 | 30 | 9 | |
| 102 | 3.62E-08 | 25 | 11 | 10 |
| 103 | 3.62E-08 | 26 | 11 | 9 |
| 104 | 2.99E-08 | 21 | 22 | |
| 105 | 2.40E-08 | 17 | 11 | 21 |
| 106 | 2.40E-08 | 16 | 11 | 22 |
| 107 | 1.87E-08 | 24 | 21 | |
| 108 | 1.87E-08 | 23 | 22 | |
| 109 | 1.50E-08 | 17 | 23 | 11 |
| 110 | 1.50E-08 | 16 | 24 | 11 |
| 111 | 1.44E-08 | 29 | 12 | |
| 112 | 1.44E-08 | 28 | 13 | |
| 113 | 1.44E-08 | 27 | 13 | |
| 114 | 1.44E-08 | 30 | 12 | |
| 115 | 1.44E-08 | 26 | 11 | 12 |
| 116 | 1.44E-08 | 25 | 11 | 13 |
| 117 | 1.17E-08 | 23 | 24 | |
| 118 | 8.06E-09 | 28 | 19 | |
| 119 | 8.06E-09 | 27 | 19 | |
| 120 | 8.06E-09 | 29 | 15 | |
| 121 | 8.06E-09 | 30 | 15 | |
| 122 | 8.05E-09 | 26 | 11 | 15 |
| 123 | 8.05E-09 | 25 | 11 | 19 |
| 124 | 4.15E-09 | 28 | 22 | |
| 125 | 4.15E-09 | 27 | 22 | |
| 126 | 4.15E-09 | 29 | 21 | |
| 127 | 4.15E-09 | 30 | 21 | |
| 128 | 4.14E-09 | 25 | 11 | 22 |
| 129 | 4.14E-09 | 26 | 11 | 21 |
| 130 | 3.33E-09 | 16 | 11 | 29 |
| 131 | 3.33E-09 | 16 | 30 | 11 |
| 132 | 3.33E-09 | 17 | 11 | 28 |
| 133 | 3.33E-09 | 17 | 27 | 11 |
| 134 | 2.59E-09 | 24 | 28 | |
| 135 | 2.59E-09 | 27 | 24 | |
| 136 | 2.59E-09 | 23 | 29 | |
| 137 | 2.59E-09 | 30 | 23 | |
| 138 | 2.59E-09 | 24 | 25 | 11 |
| 139 | 2.59E-09 | 23 | 26 | 11 |
| 140 | 5.76E-10 | 29 | 28 | |
| 141 | 5.76E-10 | 27 | 29 | |
| 142 | 5.76E-10 | 30 | 28 | |
| 143 | 5.76E-10 | 27 | 30 | |
| 144 | 5.75E-10 | 30 | 25 | 11 |
| 145 | 5.75E-10 | 27 | 26 | 11 |
| 146 | 5.75E-10 | 26 | 11 | 28 |
| 147 | 5.75E-10 | 25 | 11 | 29 |

# B Summary in Finnish

Teknisten järjestelmien, kuten liikennevälineiden, tietoverkkojen ja voimalaitosten vikaantuminen voi aiheuttaa merkittäviä materiaalisia ja taloudellisia vahinkoja. Onneksi näiden vahinkojen aiheuttajia voidaan analysoida tulevien vahinkojen ennaltaehkäisemiseksi.

Vikapuumallinnus on menetelmä teknisen järjestelmän vikaantumisen aiheuttajien kvantitatiiviseen analyysiin. Tässä menetelmässä järjestelmä jaetaan komponentteihin, joille arvioidaan vikaantumistodennäköisyys. Koko järjestelmän vikaantuminen puolestaan mallinnetaan yksittäisten komponenttien vikaantumisten funktiona, joka määräytyy järjestelmän rakenteesta. Vikapuumallinnuksessa järjestelmän rakenne esitetään puuna, jonka lehtinä ovat järjestelmän komponentit. Puun juurta kutsutaan järjestelmän epäluotettavuudeksi, ja se vastaa koko järjestelmän vikaantumisen todennäköisyyttä.

Komponenttien vikaantumistodennäköisyyksiä voidaan pienentää toimenpiteillä, esimerkiksi huoltamalla. Komponentteja voidaan varmentaa myös vaihtamalla komponentti usean vastaavanlaisen komponentin rinnankytkentään. Tällöin alkuperäistä komponenttia vastaava järjestelmän osa toimii, kun yksikin rinnankytketty komponentti toimii, ja tämän osan vikaantumistodennäköisyys on siis aiempaa pienempi. Komponentin vaihtamista usean vastaavanlaisen rinnankytkentään kutsutaan redundanssin allokoinniksi. Toimenpiteiden suorittaminen aiheuttaa kuitenkin kustannuksen, jolloin rajallisella budjetilla toimenpiteitä ei voi suorittaa kaikille komponenteille. Budjetin rajoissa varmennettavien komponenttien joukkoa kutsutaan riskinalentamisportfolioksi.

Vikaantumistodennäköisyyksiin sisältyy usein epävarmuuksia. Tämä tarkoittaa, että niitä ei tiedetä mielivaltaisen tarkasti. Näitä epävarmuuksia voidaan mallintaa todennäköisyysintervalleilla, jotka ovat reaalilukuvälejä, joihin vikaantumistodennäköisyyksien arvioidaan kuuluvan.

Todennäköisyysintervalleja käytettäessä riskinalentamisportfolioita voidaan verrata toisiinsa dominanssirelaatioiden avulla. Portfolion sanotaan dominoivan toista portfoliota tietyllä budjetilla, joss kummankaan kokonaiskustannus ei ylitä budjettia ja järjestelmän epäluotettavuus on dominoivalla portfoliolla aina vähintään yhtä hyvä ja joillakin intervallien pistetodennäköisyyksillä parempi kuin dominoidulla portfoliolla. Dominanssirelaatioista seuraa, että on olemassa ei-dominoituja portfolioita, joihin verrattuna yhdelläkään muulla portfoliolla ei ole parempi järjestelmän epäluotettavuus kaikilla todennäköisyysintervallien pistetodennäköisyyksillä.

Todennäköisyysintervalleja käytettäessä komponentteja voidaan puolestaan verrata toisiinsa ydinluvun avulla. Komponentin ydinluku määritellään komponentin sisältävien ei-dominoitujen portfolioiden lukumäärän suhteena kaikkien ei-dominoitujen portfolioiden lukumäärään. Näin ollen jokaiseen ei-dominoituun portfolioon kuuluvan komponentin ydinluku on yksi ja yhteenkään kuulumattoman nolla.

Tässä työssä muodostettiin optimointimalli vikapuulla kuvatun järjestelmän epäluotettavuuden minimoimiseen, kun komponentteja voidaan varmentaa kustannuksia aiheuttavilla toimenpiteillä ja toimenpiteisiin käytettävissä oleva budjetti on rajallinen. Malli muotoiltiin lineaarisena sekalukutehtävänä (engl., mixed-integer linear programming; MILP), jonka ratkaisuna saadaan komponentit, jotka varmentamalla järjestelmän epäluotettavuus minimoituu budjetin sallimissa rajoissa. Näiden komponenttien joukkoa kutsutaan optimaaliseksi riskinalentamisportfolioksi. Lisäksi työssä analysoidaan kahta järjestelmää muodostetun optimointimallin avulla.

Epäluotettavuus on tulosummalauseke, jonka tulontekijöitä ovat komponenttien vikaantumistodennäköisyydet. Kun komponentin vikaantumistodennäköisyys valitaan kahden vaihtoehdon joukosta, joko alkuperäisen tai alennetun todennäköisyyden, voidaan summalausekkeen yksittäinen tulotermi muodostaa ehdollisella kertolaskulla.

Optimointimalli sisältää reaalilukupäätösmuuttujan jokaisen tulotermin jokaiselle saman järjestyksen osatulolle. Esimerkiksi yhden pituista osatuloa kuvaavan päätösmuuttujan arvo on joko ensimmäisen komponentin alkuperäinen tai sen alennettu todennäköisyys. Vastaavasti kahden pituisen osatulomuuttujan arvo on yhden pituisen osatulomuuttujan arvo kerrottuna joko toisen komponentin alkuperäisellä tai sen alennetulla todennäköisyydellä. Järjestelmän komponentit on numeroitu, ja osatulojen järjestykseksi on valittu luonnollisten lukujen järjestys. Lisäksi optimointimalli sisältää binääripäätösmuuttujan jokaiselle komponentille. Komponentin binäärimuuttuja ilmaisee, varmennetaanko komponentti vai ei.

Työssä analysoitiin seitsemän komponentin esimerkkijärjestelmää ja ydinreaktorin jälkilämmönpoistojärjestelmää (engl. residual heat removal system; RHRS). Molemmilla järjestelmillä suoritettiin sekä budjetti- että intervallikoe. Budjettikokeessa ratkaistiin optimaaliset riskinalentamisportfoliot budjetin funktiona. Intervallikokeessa puolestaan mallinnettiin vikaantumistodennäköisyyksien epävarmuuksia todennäköisyysintervalleilla ja approksimoitiin ei-dominoitujen portfolioiden joukkoa ja ydinlukuja simuloimalla. Simulointi suoritettiin valitsemalla pistetodennäköisyydet satunnaisesti todennäköisyysintervalleilta ja ratkaisemalla optimaaliset riskinalentamisportfoliot arvotuilla pistetodennäköisyyksillä. RHR-järjestelmällä tutkittiin lisäksi ydinlukuja budjetin funktiona.

Työssä oletettiin, että järjestelmän komponentti voidaan varmentaa vaihtamalla se kahden vastaavanlaisen komponentin rinnankytkentään. Rinnankytkettyjen komponenttien vikaantumisia ei kuitenkaan oletettu riippumattomiksi. Näiden komponenttien yhteisvikaantumiset huomioitiin betafaktorimallilla.

MILP-tehtävien ratkaisemiseen hyödynnettiin CPLEX 12.4 -ohjelmistoa. Ohjelmistoa suoritettiin tietokoneella, joka sisältää Intel Core i3-2330M -suorittimen 2,20:n GHz kellotaajuudella ja 4 GB keskusmuistia.

Seitsemän komponentin esimerkkijärjestelmän epäluotettavuusfunktio sisältää kahdeksan tulotermiä, ja tälle järjestelmälle muotoillussa MILP-tehtävässä on 35 päätösmuuttujaa ja 89 rajoitetta. Keskimääräinen laskenta-aika yhdelle MILP-tehtävälle oli n. 0,04 s. Järjestelmän rakenne on muotoiltu siten, että tuloksista pystyy tarkistamaan, toimiiko optimointimalli käytännössä. Sekä budjetti- että intervallikokeen tulokset olivat järkeviä.

RHR-järjestelmän epäluotettavuusfunktio sisältää puolestaan 147 tulotermiä, ja tälle järjestelmälle muotoillussa MILP-tehtävässä on 363 päätösmuuttujaa ja 888 rajoitetta. Keskimääräinen laskenta-aika yhdelle MILP-tehtävälle oli n. 0,25 s.

RHR-järjestelmän budjettikokeessa selvisi, että optimaalinen järjestys komponenttien varmentamiseen vastaa karkeasti komponenttien Fussel-Vesely-riskitärkeysmitan mukaista järjestystä. Intervallikokeessa puolestaan ratkaistiin MILP-tehtävä 4000 kertaa budjetilla, joka mahdollisti kymmenen komponentin varmentamisen. Tällöin löytyi 97 approksimatiivisesti ei-dominoidun portfolion joukko. Näistä portfolioista suurin frekvenssi (n. 17 %) oli portfoliolla, joka esiintyi optimaalisena ratkaisuna myös budjettikokeessa. Ydinlukuapproksimaatiot puolestaan paljastivat, että komponenttien 1-3 ja 6 varmentaminen on etusijalla. Näille komponenteille ydinlukuapproksimaatiot olivat siis yksi. Komponenteille 16, 19 ja 21-31 sen sijaan ydinlukuapproksimaatiot olivat nolla. Näiden komponenttien varmentaminen tulisi siis olla viimeinen toimenpide, jos budjetti on rajallinen. Ydinluvut budjetin funktiona olivat enimmäkseen monotonisesti kasvavia.