THESIS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

Risk Assessment and Decision Support for Managing Drinking Water Systems

ANDREAS LINDHE

Department of Civil and Environmental Engineering
Division of GeoEngineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Gothenburg, Sweden 2010

Risk Assessment and Decision Support for Managing Drinking Water Systems
ANDREAS LINDHE
ISBN 978-91-7385-438-2

Doktorsavhandling vid Chalmers tekniska högskola
Ny serie nr 3119
ISSN 0346-718X

Department of Civil and Environmental Engineering
Division of GeoEngineering
Chalmers University of Technology
SE-412 96 Gothenburg
Sweden
Telephone + 46 (0)31 772 10 00
www.chalmers.se

Chalmers reproservice
Gothenburg, Sweden 2010

Risk Assessment and Decision Support for Managing Drinking Water Systems
ANDREAS LINDHE
Department of Civil and Environmental Engineering
Division of GeoEngineering
Chalmers University of Technology

ABSTRACT

The vital importance of a reliable and safe drinking water supply makes efficient risk management necessary for water utilities. Risks must be assessed and possible risk-reduction measures evaluated to provide relevant decision support. The World Health Organization emphasises the use of an integrated approach where the entire drinking water system, from source to tap, is considered when assessing and managing risks. Integrated risk assessments are important in order to avoid overlooking interactions between subsystems and events and to minimise sub-optimisation of risk-reduction measures. Methods for integrated risk assessment are, however, limited. A dynamic fault tree method is presented that enables quantitative, integrated risk assessment of drinking water systems. An approach for approximate dynamic fault tree calculations has been developed to minimise computational demand. It is shown how the method can be used to evaluate uncertainties and provide information on risk levels, failure probabilities, failure rates and downtimes of the entire system and its subsystems. The fault tree method identifies where risk-reduction measures are needed most and different risk-reduction alternatives can be modelled, evaluated and compared. The method is combined with economic analysis to identify the most cost-effective risk-reduction alternative. Integrated risk assessments of drinking water systems are commonly performed using risk ranking, where the probability and consequence of undesired events are assessed using discretised scales. There is, however, no common, structured way of using risk ranking to prioritise risk-reduction measures. Two alternative models for risk-based, multi-criteria decision analysis (MCDA) for evaluating and comparing risk-reduction measures have therefore been developed. The MCDA models are based on risk ranking, they can consider uncertainty in estimates and include criteria related to, for example, different risk types and economic aspects. In summary, this thesis provides methods for integrated risk assessment that make it possible to prioritise risk-reduction measures. It is concluded that the methods provide relevant decision support for efficient risk management in water utilities.

Keywords: drinking water, water supply, risk assessment, decision analysis, dynamic fault tree analysis, multi-criteria decision analysis, water safety plan.

LIST OF PAPERS

This thesis is based on the work contained in the following papers, referred to in the text by Roman numerals:

I. **Lindhe**, **A**., Rosén, L., Norberg, T. and Bergstedt, O. (2009). Fault tree analysis for integrated and probabilistic risk analysis of drinking water systems, *Water Research*, 43 (6), 1641-1653.

II. **Lindhe**, **A**., Norberg, T. and Rosén, L. (2010). Approximate dynamic fault tree calculations for modelling water supply risks, Submitted to *Risk Analysis*.

III. Rosén, L., **Lindhe**, **A**., Bergstedt, O., Norberg, T. and Pettersson, T.J.R. (2010). Comparing risk-reduction measures to reach water safety targets using an integrated fault tree model, *Water Science and Technology: Water Supply*, 10 (3), 428-436.

IV. **Lindhe**, **A**., Rosén, L., Norberg, T., Bergstedt, O. and Pettersson, T.J.R. (2010). Cost-effectiveness analysis of risk-reduction measures to reach water safety targets, Accepted for publication in *Water Research*, doi: 10.1016/j.watres.2010.07.048.

V. **Lindhe**, **A**., Rosén, L., Norberg, T., Røstum, J. and Pettersson, T.J.R. (2010). Risk-based multi-criteria decision models for prioritising water safety measures, Submitted to *Water Research*.

Division of work between the authors

In Paper I, all the authors defined the aim and scope. Lindhe, Norberg and Rosén developed the method and Bergstedt contributed with expert knowledge regarding the function of drinking water systems. Norberg devised the mathematical foundation of the logic gates and Lindhe constructed the generic fault tree model, performed the simulations and was the main author of the paper.

The work presented in Paper II was initiated by Norberg. All authors defined the aim and scope. Lindhe devised the fault tree examples and performed the dynamic fault tree calculations. Norberg performed the Markov simulations. Lindhe and Norberg were the main authors of the paper.

In Paper III, Lindhe construed the fault tree models and performed the calculations with support from Rosén and Norberg. Bergstedt contributed with knowledge of the analysed system and the risk-reduction measures. All the authors analysed the results. Lindhe and Rosén were the main authors of the paper.

In Paper IV, the structure of the analysis was devised by Lindhe, Rosén and Norberg. Lindhe performed the calculations with support from the other authors. Bergstedt contributed with knowledge of the analysed system and the risk-reduction measures. All the authors analysed the results. Lindhe was the main author of the paper.

In Paper V, Lindhe, Rosén and Norberg developed the decision models with support from Pettersson. Røstum contributed with information on the case study site and the effects of risk-reduction measures. Lindhe performed the calculations and was the main author of the paper.

Publications not appended

As part of the doctoral work presented in this thesis, Lindhe (2008) presented a thesis for the degree of licentiate of engineering, see reference in the list below. The licentiate thesis is an important part of the work performed in the doctoral project and is the basis for this doctoral thesis. Parts of the background presented in this thesis are based on Lindhe (2008).

In addition to the work presented in this thesis the author has published or contributed significantly to the following publications, which are not appended to the thesis:

- **Lindhe**, **A**., Rosén, R. and Pettersson, T.J.R. (2006). Risk management in drinking water supply – from source to tap (*In Swedish*), *Cirkulation*, 06 (8), 27-28.
- Rosén, L., Hokstad, P., **Lindhe**, **A**., Sklet, S. and Røstum, J. (2007). *Generic framework and methods for integrated risk management in water safety plans*, Deliverable no. D4.1.3, D4.2.1, D4.2.2, D4.2.3, TECHNEAU.
- Rosén, L. and **Lindhe**, **A**. (2007). *Trend report: Report on trends regarding future risks*, Deliverable no. D1.1.9, TECHEANU.

- Beuken, R., Sturm, S., Kiefer, J., Bondelind, M., Åström J., **Lindhe**, **A**., Machenbach, I., Melin, E., Thorsen, T., Eikebrokk, B., Niewersch, C., Kirchner, D., Kozisek, F., Gari, D.W. and Swartz C. (2008). *Identification and description of hazards for water supply systems – A catalogue of today's hazards and possible future hazards*, Deliverable no. D4.1.4, TECHEANU.
- **Lindhe**, **A**., Rosén, L., Norberg, T., Petterson, T.J.R., Bergstedt, O., Åström, J. and Bondelind, M. (2008). Integrated risk analysis from source to tap: Case study Göteborg, In *Proceedings of 6th Nordic Drinking Water Conference*, Oslo, June 9-11, pp. 231-241, Norsk Vann, Hamar.
- Rosén, L., **Lindhe**, **A**., Hokstad, P., Sklet, S., Røstum, J. and Pettersson, T.J.R. (2008). Generic Framework for Integrated Risk Management in Water Safety Plans, In *Proceedings of the 6th Nordic Drinking Water Conference,* Oslo, June 9-11, pp. 193-203, Norsk Vann, Hamar.
- **Lindhe**, **A**. (2008). *Integrated and Probabilistic Risk Analysis of Drinking Water Systems*, Licentiate Thesis No. 2008:8, Chalmers University of Technology, Göteborg.
- **Lindhe**, **A**., Rosén, L., Bergstedt, O., Norberg, T. and Petterson, T.J.R. (2009). Quantitative risk assessment of water supply systems from source to tap, In *TECHNEAU: Safe Drinking Water from Source to Tap*, van den Hoven, T. and Kazner, C. (Eds.) , pp. 203-215, IWA Publishing, London.
- Norberg, T., Rosén, L. and **Lindhe**, **A**. (2009). Added value in fault tree analyses, In *Safety, Reliability and Risk Analysis: Theory, Methods and Applications*, Martorell, S., Guedes Soares, C. and Barnett, J. (Eds.), pp. 1041-1048, Taylor & Francis Group, London.
- Swartz, C., Pettersson, T.J.R. and **Lindhe**, **A**. (2010). Risk assessment and risk management in water supply systems: State-of-the-art and case studies in southern Africa, Paper presented at the WISA (Water Institute of South Africa) 2010 Biennial Conference & Exhibition, Durban, April 18-22.
- **Lindhe**, **A**., Rosén, L., Norberg T., Åström, J., Bondelind, M., Pettersson, T. and Bergstedt, O. (2010). *Risk assessment case study – Göteborg, Sweden*, Deliverable no. D4.1.5a, TECHNEAU.
- **Lindhe**, **A**., Sturm, S., Røstum, J., Kožíšek, F., Gari, D.W., Beuken, R. and Swartz, C. (2010). *Risk assessment case studies – Summary report*, Deliverable no. D4.1.5g, TECHNEAU.

- Hokstad, P., Røstum, J., Sklet, S., Rosén, L., Pettersson, T.J.R., **Lindhe**, **A**., Sturm, S., Beuken, R., Kirchner, D. and Niewersch, C. (2009*). Method for risk analysis of drinking water systems from source to tap – Guidance report on risk analysis*, Deliverable no. D4.2.4, TECHNEAU.
- **Lindhe**, **A**. (2010). *Risk analysis from source to tap* (*In Swedish*), Report 2010-08, Svenskt Vatten Utveckling, Stockholm.
- Salehpour, Z., Pettersson, T.J.R., Rosén, L., Malm, A. and **Lindhe**, **A**. (2010). Risk-based asset management of potable water distribution systems: case study, In *Proceedings of the 7th Nordic Drinking Water Conference,* Copenhagen, June 7-9, pp. 187-190, DANVA, Skanderborg.
- Rosén, L., **Lindhe**, **A**., Chenoweth, J., Fife-Schaw, C. and Beuken, R. (2010). *Decision support for risk management in drinking water supply – Overview and framework*, Deliverable no. D4.4.1, TECHNEAU.

The publications related to the Techneau project can all be downloaded from www.techeanu.org.

ACKNOWLEDGMENTS

The work on this thesis has been carried out at the Department of Civil and Environmental Engineering, Division of GeoEngineering, at Chalmers University of Technology. The PhD project that resulted in this thesis has been part of the framework programme for drinking water research at Chalmers, DRICKS. The project has also been linked to the Techneau project, funded by the European Commission (contract no. 018320). The author gratefully acknowledges the financial support provided by the Swedish Water & Wastewater Association, the City of Gothenburg and the Techneau project.

A number of people have in different ways contributed to making the work on this thesis possible. First of all, I am sincerely grateful to my supervisor, Professor Lars Rosén, for valuable and inspiring discussions and for his excellent support. I am also very grateful for the supervisory support from Associate Professor Tommy Norberg and Assistant Professor Thomas Pettersson. Tommy, I very much appreciate your support, which has helped me to broaden my understanding of statistics. Thomas, thank you for your valuable discussions and feedback.

The fruitful collaboration with the City of Gothenburg has been of great importance in this work. I would like to thank Olof Bergstedt, Göteborg Vatten and Chalmers, for providing valuable feedback and in other ways contributing to a successful result. Furthermore, I would like to thank Helena Hallagård, Claes Wångsell and the rest of the staff at Göteborg Vatten who have participated in discussions and provided me with data and comments on the work.

I would also like to express my gratitude to my colleagues within DRICKS and to my colleagues at the Division of GeoEngineering for being good friends and providing an inspiring working climate. Special thanks to Professor Lars O. Ericsson for his constructive comments on this thesis and Karin Holmgren for help with some of the illustrations.

I also wish to thank the people involved in the Techneau project, especially the partners of Work Area 4 *Risk assessment and risk management*.

I am grateful to my friends and my family for their support and encouragement. Special thanks to my beloved wife Therese. Despite marvellous supervisors and colleagues, this thesis would not have been possible to write without you Therese – thank you for your love and patience!

Floda, November 2010

Andreas Lindhe

TABLE OF CONTENTS

1 INTRODUCTION

The first chapter provides the background to the thesis. The aim and objectives are presented and the scope of the work is specified. Important limitations of the thesis are also presented.

1.1 Background

The supply of drinking water is of primary importance in society. Public health and economic development are examples of factors that rely on access to and the quality of drinking water (IWA, 2004). Since drinking water systems include several subsystems, there are many parts where undesired events may occur and cause harm. The water source may, for example, be contaminated and the supply of treated water may be interrupted due to pipe bursts or other failures in the distribution system (e.g. Beuken *et al.*, 2008; Nadebaum *et al.*, 2004). Drinking water systems and the consumers are thus exposed to a wide range of risks. Furthermore, climate changes, societal development and emergence of new contaminants constantly present new risks (AwwaRF, 2006; Rosén and Lindhe, 2007). Within the drinking water sector it has been stated that the goal is to provide *good safe drinking water that has the trust of consumers* (IWA, 2004). To meet this goal and to guarantee consumers a reliable supply of safe drinking water, risks must be assessed and the results used to make well-informed decisions.

The World Health Organization (WHO, 2008) has concluded that a holistic risk assessment and risk management approach, including the entire drinking water system, from source to tap, is the most effective way to ensure a safe drinking water supply. A proactive and risk-based approach that takes into account the entire drinking water system is also advocated in national guidelines in, for example, Australia (NHMRC/NRMMC, 2004) and Canada (CDW/CCME, 2004). Risk management based on a proactive approach cannot be claimed to be completely new for the drinking water sector. However, a more formalised and explicit approach to risk management can now be seen and which has not been used before (Hrudey *et al.*, 2006; MacGillivray *et al.*, 2007a; 2007b; Pollard *et al.*, 2004). Methods and tools available today, and possible future methods and tools,

provide better means than previously for assessing risk and providing useful decision support regarding risk issues.

As part of a risk-based approach, the WHO suggests preparation of Water Safety Plans (WSPs) (WHO, 2008). The basic idea of a WSP is to assess the entire drinking water system, identify possible hazards and plan how to monitor and operate the system so that the risks are controlled. To be able to assess risks suitable methods are of course necessary. A common type of qualitative, or semi-quantitative, risk assessment used in many fields is risk ranking, where the probability and the consequence of undesired events are estimated on discretised scales and the results are presented in a risk matrix. This type of assessment is also suggested as part of a WSP (e.g. Bartram *et al.*, 2009; Davison *et al.*, 2005). Risk ranking can be used to prioritise risks but there is currently no common, structured way of using the approach whereby risk-reduction measures can also be evaluated and compared. Risk ranking is useful in many situations but it has several limitations since, for example, uncertainties are typically not included and chains of events and interactions between events are not easily considered (e.g. Burgman, 2005; Cox, 2008). Consequently, additional methods for integrated risk assessment of drinking water systems, including the entire system, are needed.

The purpose of risk assessment is to provide information so that well-informed decisions can be made (e.g. Aven and Kørte, 2003). A water utility may, for example, be interested in knowing the risk level to decide if risk-reduction measures are required or not. If the risk level is unacceptable, possible measures need to be evaluated to find out what alternative is most suitable. Hence, risk assessments are initiated by an underlying decision problem. Since it is not possible to eliminate all risks, an acceptable risk level must be obtained by balancing risks, benefits and cost. Risk assessment is thus closely linked to decision-making and it is therefore often reasonable to combine risk assessment and decision analysis.

The overall work of risk management includes several steps. Commonly it includes risk assessment, where risks are analysed and evaluated, and a subsequent step where decisions are made, risk-reduction measures are implemented and the effects are monitored (e.g. AZ/NZS, 2004b; IEC, 1995). Risk management is an iterative process which means that the work should be continuously updated and that there are no strict boundaries between the steps. Furthermore, risk and related aspects need to be communicated between decision-makers, scientists, the general public and other stakeholders.

To facilitate risk management within the drinking water sector, including preparation of WSPs, suitable methods for risk assessment and decision analysis are needed. The drinking water sector needs access to several methods and tools to be able to analyse the wide variety of risk-related problems that may exist. Both qualitative risk assessment methods, such as risk ranking, and more advanced quantitative methods that can consider complex systems and uncertainties are needed, but for different situations and purposes. Risk assessment methods are typically used to determine the current risk level to see if it is acceptable or not. However, if the risk is unacceptable, methods for evaluating possible risk-reduction measures are needed. Since not only the risk but also other criteria are important when deciding on risk-reduction measures, risk assessment results must be combined with other information to provide useful decision support. It should be emphasised that the risk assessment result can never be the actual decision but provides important information to be used by the decision-maker (e.g. Kammen and Hassenzahl, 2001). Furthermore, to achieve efficient risk management a water utility needs not only methods for proper risk assessment and decision analysis but also an organisational structure and commitment (e.g. MacGillivray and Pollard, 2008).

Risk management aims of course to protect humans and what is considered of value to humans. It should, however, not be forgotten that risk assessments and decision analyses create opportunities by providing information needed to keep the risk at an acceptable level and at the same time maximise the benefits, in monetary or other contexts.

1.2 Aim and objectives

The overall aim of this thesis is

> *to develop, apply and evaluate methods for integrated risk assessment, from source to tap, that provide decision support for efficient risk management of drinking water systems.*

Based on the background description given above it can be concluded that there is a lack of quantitative methods for integrated risk assessment of drinking water systems. A main reason for applying such methods is the possibility of providing quantitative decision support. A quantitative and probabilistic risk assessment method was developed and is presented in this thesis. The method was combined with an economic analysis to show how to extend the results to further support

decision-making. One type of method cannot be used to assess all risk-related problems a water utility could face. Hence, qualitative methods such as risk ranking are also needed. However, new approaches are required since there is no common, structured way of how to use risk ranking for evaluating and comparing risk-reduction measures. To enable such evaluation and comparison, two decision models were developed that combine risk ranking with multi-criteria decision analysis and take uncertainties into consideration. As a basis for the work presented in this thesis, an overview of risk management and decision-making in the context of drinking water supply is provided.

In addition to the overall aim, the thesis has the following specific objectives:

- Present a generic framework describing risk management and decision-making in the context of drinking water supply.
- Develop a quantitative and probabilistic risk assessment method for analysing entire drinking water systems, from source to tap, and modelling the effects of risk-reduction measures.
- Evaluate the quantitative risk assessment method with regard to its theoretical foundation.
- Evaluate the practical applicability of the quantitative risk assessment method based on case studies and show how risks can be assessed and how risk-reduction measures can be modelled.
- Combine results from quantitative risk assessment with economic analysis to provide decision support, including information on cost-effectiveness and cost-benefit aspects.
- Combine qualitative risk assessment (risk ranking) with multi-criteria decision analysis to enable evaluation and comparison of risk-reduction measures based on several criteria and with consideration of uncertainties.

1.3 Scope of the work

The overall aim of the thesis is achieved through theoretical studies, method development and by applying the methods in case studies. This work is presented in the following five papers appended to the thesis (short titles in parenthesis):

Paper I (*Dynamic fault tree method*):	Fault tree analysis for integrated and probabilistic risk analysis of drinking water systems
Paper II (*Method evaluation*):	Approximate dynamic fault tree calculations for modelling water supply risks
Paper III (*Modelling risk reduction*):	Comparing risk-reduction measures to reach water safety targets using an integrated fault tree model
Paper IV (*Evaluating risk reduction*):	Cost-effectiveness analysis of risk-reduction measures to reach water safety targets
Paper V (*Decision models*):	Risk-based multi-criteria decision models for prioritising water safety measures

The overall problems considered in this thesis and the main outcomes are described in Figure 1.1. The problems are directly linked to the objectives presented in Section 1.2 and the five papers listed above contain most of the outcomes. The illustration in Figure 1.1 indicates where in this thesis the outcomes are presented. The thesis includes a theoretical background to the research area, which is presented in Chapter 2. In Chapter 3 the methods and techniques used to develop new risk and decision support methods are presented. Chapter 4 provides an overview of the five papers and their main findings. The results of the thesis, including the methods developed and their applications, are described in Chapter 5. Chapter 6 contains a discussion and the main conclusions are presented.

This thesis work has partly been performed in Techneau, a drinking water project funded by the European Commission. Within Techneau, the author has been involved in work on risk assessment and decision support that is not presented in this thesis. However, all the knowledge and experience gathered from the work in the Techneau project has or course been an important input to this thesis.

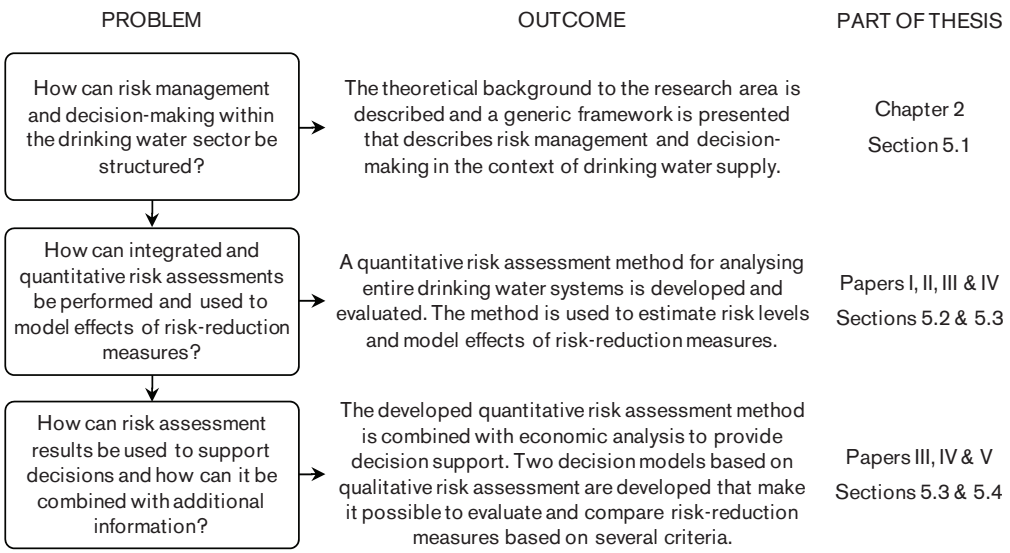


Figure 1.1 *Schematic description of the overall problems considered in this thesis, the main outcomes and the specific parts of the thesis where the outcomes are presented.*

1.4 Limitations

When dealing with risk assessment methods and decision models for drinking water systems, it is impossible to include all aspects. This thesis is focused on integrated risk assessments, including entire systems, and how risk assessment results can be used in decision analysis to evaluate and compare measures for risk reduction. Since an integrated approach is used the aim is to include a wide range of possible scenarios instead of analysing only a specific type of event that may cause harm. The thesis does not deal with designing specific measures for reducing certain risks or the process of implementing and monitoring selected measures. Although risk assessment and decision analysis results provide a necessary basis for risk communication, the aim of the thesis is not to discuss communication issues in detail. Furthermore, the thesis does not focus specifically on crisis management, although risk assessments and decision analyses are important when preparing for a crisis.

2 THEORETICAL BACKGROUND

In this chapter the theoretical background to the contents of the thesis is presented. The chapter includes descriptions of the basis of drinking water supply and concepts related to risk assessment and decision analysis.

2.1 Drinking water supply

Safe drinking water

It is often emphasised that drinking water should be safe, but what does this mean? As described in Section 1.1 it has been stated within the drinking water sector that the goal of water utilities is to provide *good safe drinking water that has the trust of consumers* (IWA, 2004). It is also emphasised that a reliable supply of safe drinking water is fundamental to public health and economic development. The WHO (2008) defines safe drinking water as *does not represent any significant risk to health over a lifetime of consumption, including different sensitivities that may occur between life stages*. Furthermore, the aim of water treatment may be described as producing an adequate and continuous supply of water that is of acceptable quality (e.g. Gray, 2005).

It can be concluded that two key aspects of safe drinking water are the water quality and the ability to deliver water to the consumers. It is, however, not reasonable to say that there should be no, or zero, risk related to safe drinking water (e.g. Hunter and Fewtrell, 2001). It is neither practicable nor affordable to eliminate all risks. Instead, an acceptable risk level should be obtained where benefits and costs, in monetary or other terms, are balanced (e.g. Fischhoff *et al.*, 1981). Hence, safe drinking water means that consumers should have access to a drinking water supply of acceptable reliability and with a high water quality that poses a minimal and acceptable risk to human health. However, what is considered to be an acceptable level of reliability and risk differs. Hrudey *et al.* (2006) suggest that safety is described as *a level of risk so negligible that a reasonable, well-informed individual need not be concerned about it, nor find any rational basis to change his/her behaviour to avoid such small, but non-zero risks*. It should be stressed that the trust and confidence of consumers are also

important aspects for water utilities to consider (e.g. Fife-Schaw *et al.*, 2008; Morrison *et al.*, 2009).

The above description of safe drinking water is based on a consumer perspective. When managing risks a water utility may also need to deal with factors such as financial and environmental effects. Furthermore, there may be competing interests in using the water source for purposes such as irrigation and energy production instead of as a raw water source.

Drinking water systems

The principal structure of drinking water systems is similar and typically includes a raw water source, a treatment plant and a distribution system (Figure 2.1). Sometimes the consumer is considered as a separate and fourth part of the system. Due to variations in natural conditions, water demand, economic resources and other factors, the overall structure and the different subsystems may appear very different.

Possible raw water sources include surface water, groundwater (artificial or induced recharge may be used) or combinations of these (e.g. HDR Engineering, 2001). The type of treatment and the number of treatment steps depend on the raw water quality (e.g. Gray, 2005). When water sources are scarce, treated wastewater may be used to produce drinking water as well as seawater desalination (e.g. Rygaard *et al.*, 2011; Van der Bruggen, 2010). In addition to pipes the distribution system includes pumps and service reservoirs needed to manage variations in water demand and to ensure adequate hydraulic pressure in the service areas. However, the layout of the distribution system differs between systems. Drinking water systems commonly have a physically distributed layout with different types of interaction between subsystems and components.

To achieve a safe supply, drinking water systems are typically designed to include redundant subsystems and components. This gives the systems an inherent ability to compensate for failures. Failure of a pump in the distribution system, for example, may not affect delivery to the consumers if there are reserve pumps. Furthermore, unacceptable raw water quality may be compensated for by the treatment plant, and an interruption in the supply of raw water does not automatically affect the consumers since water stored at the treatment plant and in the distribution system can be used. These conditions need to be identified and understood when analysing a drinking water system. A good understanding of the

analysed systems is a basic requirement for proper risk assessments that provide useful results.

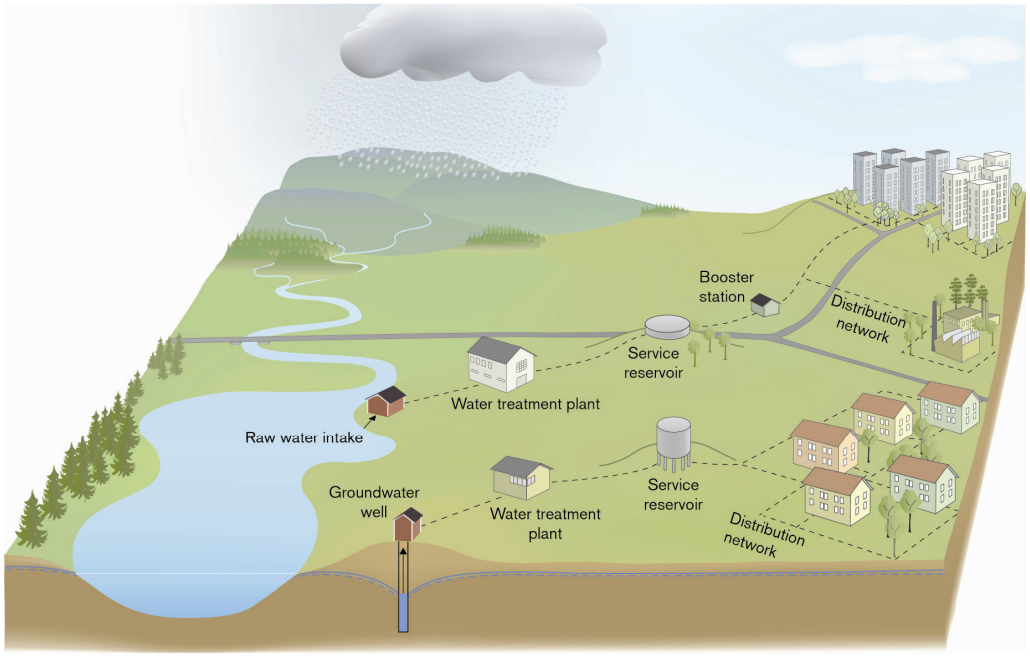


Figure 2.1 *Schematic illustration of two drinking water systems, one using a surface water source and one using a groundwater source.*

2.2 Risk and related concepts

Risk

The term *risk* includes several dimensions and it is not easy to provide a universal definition suitable for all contexts. A vast number of definitions can be found in the literature (e.g. Aven and Renn, 2009) and they differ slightly depending on, for example, if they are based on an engineering or socio-scientific perspective and if the considered risk is related to human health problems, environment problems or purely technical problems. Here, the aim is to present some of the most common views of risk and describe what definition is used in this thesis. Due to the many different definitions, it can be concluded that it is important to describe clearly how the term is used in the specific application.

Sometimes risk is used as a synonym for the probability of an undesired event occurring. However, a common description of risk is that it is a combination of

the probability and the consequence of an undesired event (e.g. EC, 2000; IEC, 1995; ISO/IEC, 2002). Kaplan and Gerrick (1981) state that the question "What is risk?" actually comprises the following three questions (also discussed by Kaplan, 1997; Kristensen *et al.*, 2006):

- What can happen?
- How likely is it?
- What are the consequences?

The answer to the first question describes what could go wrong and can be called a scenario (S). How likely (L) it is that the scenario happens is described using a probability or a frequency and the consequence (X) describes the damage. Together the answers to these three questions describe the risk and can be written as a triplet $\left(S_i, L_i, X_i\right)$, $i = 1, 2, \ldots, n$. Index i specifies that more than one scenario may be of interest to describe the risk. If curly brackets are used to describe a set of answers and index c, meaning *complete*, is added to indicate that all possible scenarios of interest are considered, then risk (R) can be expressed as $R = \{\langle S_i, L_i, X_i \rangle\}_c$. This quantitative definition describes risk as a combination of the probability, or frequency, of occurrence and the consequence of *all* scenarios of interest. When analysing a drinking water system one scenario may, for example, be a pipe burst (S) that is estimated to occur with a probability of 0.05 (L) and cause an interruption in the delivery of drinking water to 100 people for a period of 8 hours (X).

Risk is in some applications expressed as the probability multiplied by the consequence, i.e. as the expected value of consequence (or expected value of damage). Kaplan and Garrick (1981) argue that this definition may be misleading in some cases and prefer to say that risk is probability *and* consequence. Although a common description of risk should not state that risk is equal to the expected value of consequence, it may in some applications be suitable to express risk in this way. Aven (2010) argues that the probability component of risk should be replaced by *uncertainty* since important uncertainty aspects may be overlooked when focusing on probability. To stress that uncertainty should be used rather than focusing on probabilities when discussing risk, Aven and Renn (2009) define risk as *uncertainty about and severity of the consequences of an activity*.

In the new international standard for risk management, issued by the International Organization for Standardization (ISO, 2009), risk is defined as

effects of uncertainty on objectives. It is further explained that risk is the consequence of an organisation setting and pursuing objectives against an uncertain environment. This definition is further used to describe risk management as an optimisation process that makes the achievement of objectives more likely (Purdy, 2010). Leitch (2010) criticises the new standard, including the definition of risk, since he thinks that it is unclear, is not mathematically based and has little to say about probability, data and models. It should be stressed that irrespective of what risk definition is used, it is important to consider uncertainties.

Quantitative definitions of risk, such as the one by Kaplan and Gerrick (1981) described above, are sometimes subject to criticism. It is argued that these definitions do not consider the social amplification of risk and do not take value judgement into account (Slovic, 2001; 2002). Klinke and Renn (2002) define risk as the possibility that human actions or events lead to consequences that harm aspects of things that human beings value. Kaplan and Garrick (1981) however, emphasise that a clear and quantitative way of expressing risk is essential to rational decision-making. If this kind of definition does not exist, it is not possible to weight properly the risk along with costs and benefits in the decision process. Although risk is expressed quantitatively, human perception of risk should also be taken into consideration in the decision process. Risk perception and its role in risk management is discussed by Renn (1998), see also Slovic (1987).

In this thesis, the definition by Kaplan and Garrick (1981) is used as a basis for risk but uncertainties regarding probabilities, consequences and other aspects are included to describe the risk properly. Furthermore, risk assessment results are seen as an input in decision-making that can and should be combined with additional information to facilitate well-informed decisions.

Uncertainty

As stated in the description of risk, uncertainty is an important part of risk and must thus be considered in risk assessments and decision analyses. Although the probability component of risk can to some extent be seen as a description of uncertainty, this is not what is referred to here as uncertainty. Proper risk assessment and decision analysis should consider uncertainties of probabilities as well as uncertainties of consequences and other aspects.

Different sources of uncertainty exist and typically uncertainties due to natural variation (aleatory uncertainty) and lack of knowledge (epistemic uncertainty)

are discussed (e.g. Aven, 2003; Back, 2006; Norrman, 2004). Further categorisation of uncertainties is possible and French (1995), for example, presents ten different sources of uncertainty that may be expressed during modelling, during exploration of the model and when model results are interpreted. There are different techniques for including uncertainties when risks are analysed and evaluated (Paté-Cornell, 1996). Point estimates, for example, can be replaced by probability distributions to describe uncertainties in variables (see Section 3.5).

A Bayesian approach is commonly applied when analysing risks (Bedford and Cooke, 2001; Kaplan, 1993). This means that probability is seen as a degree of belief and the Bayesian approach makes it possible to combine hard data, e.g. measurements and statistics on events, in a mathematically formal manner with expert judgements. Since hard data is often lacking, expert judgements become an important component of risk.

Hazard and event

Hazard is a common term used when risk issues are discussed. In water quality applications hazard is sometimes defined as, for example, a biological or chemical agent (e.g. WHO, 2008). Here, not only hazardous agents are considered and a broader definition of hazard found in international standards is thus used. Hazard is defined as *source of potential harm or a situation with a potential of harm* (AZ/NZS, 2004b; CSA, 1997; IEC, 1995; ISO/IEC, 2002). Consequently, hazard does not include any information about the probability of occurrence, whereas risk is based on the hazard as well as the probability. Burgman (2005) emphasises that the conversion of hazard assessment to risk assessment involves a probabilistic element, i.e. that the probability of the hazard having an effect is assessed. In addition to hazard, *undesired event* or simply *event* is also used in this thesis to describe the scenario part in risk.

Vulnerability

A term often used in combination with risk is *vulnerability*. Similar to risk there are different definitions of vulnerability in the literature. Haimes (2006) states that vulnerability is the manifestation of the inherent states of the system (e.g. physical, technical, organisational, cultural) that can be exploited to adversely affect (cause harm or damage to) that system (see also Haimes, 2009). Typically, vulnerability is used to stress that not only external hazards should be considered but also the inherent qualities of a system. Johansson and Hassel (2010) point out

that in the literature, vulnerability is viewed both as an overall property of a system and as a specific aspect or a component of a system.

Aven (2007) describes vulnerability as being one component of risk. When analysing risks to drinking water systems it is necessary to consider system vulnerabilities to obtain a relevant description of the risk. In this thesis, when the term *risk assessment* is used it also includes the concept of vulnerability. Imagine, for example, a situation where two drinking water systems use the same water source, one has a treatment plant with multiple barriers and the other only includes one barrier. Since the treatment plants have different vulnerabilities due to differences in their ability to reduce contaminants in the raw water, a situation with reduced raw water quality does not pose the same risk to the consumers in the two systems. For a system with multiple barriers, the probability of having drinking water of unacceptable quality reaching the consumer is lower compared to the other system. Consequently, the risk is also lower for the system with multiple barriers.

2.3 Risk management and decision-making

The processes

In the literature, separate descriptions of risk management and decision-making are often found. In this section the two topics are presented to show that they are strongly linked to each other.

The task of managing risks includes several steps that may start with an identification of a problem and end with an action aimed at reducing the risk to an acceptable level. Although the process of risk management is illustrated in a vast number of ways in the literature, they commonly share certain basic steps (e.g. AZ/NZS, 2004b; IEC, 1995; ISO, 2009; Schaub, 2004). However, the terms used to describe these steps vary and the same terms are used to describe different steps. One main reason for these differences is that both the terminology and the descriptions have been developed within different fields with a different focus, e.g. engineering, human health, ecology and economics.

The illustration in Figure 2.2 shows an example of how risk management can be divided into steps and how these are linked. This outline is rather generic since it does not include specific steps relevant only to certain applications. Here, risk management refers to the entire process, including the initial description of scope

and purpose of risk management, the identification of hazards and the estimation of risks, through to the evaluation of risk acceptance, identification of possible risk-reduction measures and an analysis of the alternatives, to the selection, implementation and monitoring of appropriate actions.

The arrows in Figure 2.2 represent how results and other information are transferred between the different steps. Hence, the results from risk analysis are used as input for the risk evaluation where it is determined if the risk is acceptable or not. If the risk is unacceptable possible risk-reduction measures are identified and analysed, and these results are used to decide what actions to take. The task of risk analysis and risk evaluation is referred to as risk assessment. It should be noted that risk management is an iterative process and there are now clear boundaries between the different steps. The feedback arrow in Figure 2.2 illustrates that each step should be updated when new information becomes available and when the conditions change. This is especially true for the steps included in risk assessment. It is also important to communicate information on risk properly to affected stakeholders (e.g. Davidsson *et al.*, 2003; Owen *et al.*, 1999).

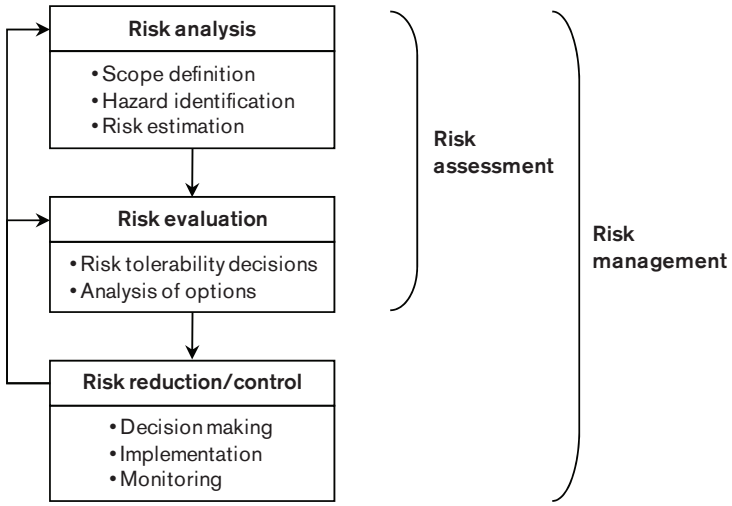


Figure 2.2 Illustration of the risk management process according to IEC (1995).

The aim of risk assessment can be described as providing information so that good decisions can be made. In the risk management context the decision problems typically relate to whether the risk is acceptable or not and what action to take. What constitutes a good decision depends on what aspects are considered important for the specific decision problem. When evaluating and comparing possible measures for risk reduction, decisions are made before the actual

outcomes can be observed. Hence, decisions need to be made under uncertainty. Aven (2003) presents two possible approaches for reaching a good decision (see also Aven and Kørte, 2003):

- Establish an optimisation model of the decision-making process and choose the alternative that maximises (minimises) certain specific criteria.
- See decision-making as a process with formal risk and decision analyses to provide decision support, followed by an informal managerial judgement and review process resulting in a decision.

Aven (2003) recommends the latter strategy to be most suitable since an optimisation model can only include a limited number of dimensions and thus not provide the full basis for decision-making. There may, however, be situations where the first strategy is most applicable. Based on the second strategy the process of choosing from a set of decision alternatives can be described as in Figure 2.3. As illustrated in the figure, the results from various analyses are used as input when making decisions although the decision-makers need to perform a managerial review and judgement of relevant factors that are not included in the applied models. The decision problem, the development of decision alternatives and the other steps in the process are affected by goals, criteria and preferences based on stakeholder values.

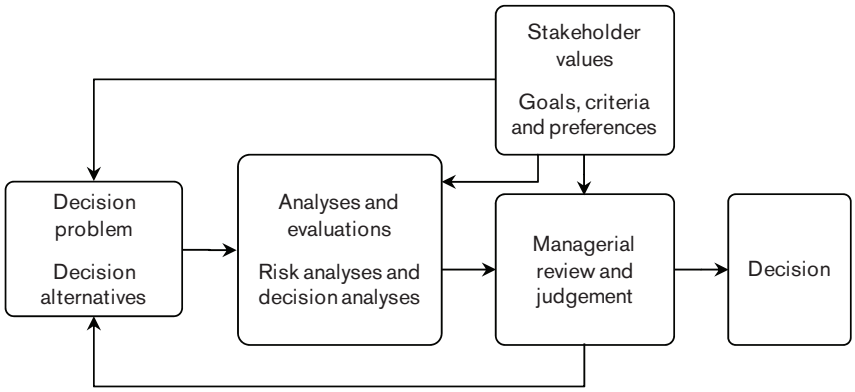


Figure 2.3 Basic structure of the decision-making process (Aven, 2003).

Motives for risk management

When discussing the concept of safe drinking water (Section 2.1) it was concluded that it is neither practicable nor affordable to eliminate all risks. Kaplan and Garrick (1981) emphasise that we cannot avoid risks but only choose between

risks. In the Australian/New Zealand standard on risk management (AZ/NZS, 2004a; 2004b), it is stated that risk management is about achieving an appropriate balance between realising opportunities for gains while minimising losses. Hence, risk management is about providing necessary information so that this balance can be achieved. Risk management is thus not only about protecting humans and what we value but also about creating opportunities. Knowledge about what constitutes a risk and what does not facilitates a proper selection between possible actions.

Egerton (1996) describes a simplified example of how a risk analysis can provide information that enables a reduction in both risk and cost. By identifying which areas of a treatment plant contribute most to the risk, measures can be taken to reduce the risk. At the same time that unsafe components are identified, areas of over-design can also be identified, making it possible to reduce the costs with little impact on the overall reliability.

2.4 Approaches in the drinking water sector

The WHO (2008) concludes that the most effective way to ensure the safety of a drinking water supply is by means of a comprehensive risk assessment and risk management approach. According to Pollard *et al.* (2004) the drinking water sector is formalising and making explicit approaches to risk management and decision-making that were previously implicit. Furthermore, MacGillivray *et al.* (2007a; 2007b) emphasise that a significant shift in the drinking water sector's approach to risk management is ongoing. Risk management is becoming increasingly explicit and better integrated with other business processes compared to the historical implicit approach, which focused on treatment plant design and operation (Hrudey *et al.*, 2006). One example of the increased awareness of risk-related issues within drinking water supplies is the Water Safety Plan (WSP) approach suggested by the WHO (2008). The WSP approach is described further below.

Risks can be managed on different levels in an organisation depending on what kind of decision needs to be made. Pollard (2008) describes the different levels as *strategic*, *programme* and *operational* (Figure 2.4) (see also MacGillivray *et al.*, 2006). On the strategic level regulatory, commercial and financial risks are included while risks linked to, for example, asset and catchment management are considered on the programme level. Risks associated with specific operations, such as failure of process components, are managed on the operational level.

Strategic decisions are supposed to be transferred into actions on the programme level and implemented on the operational level.

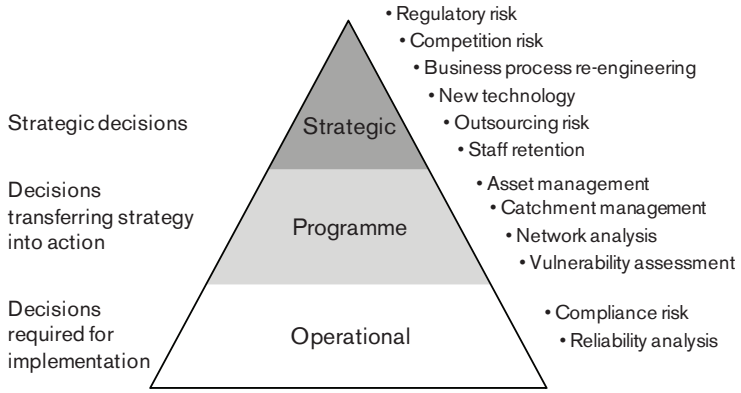


Figure 2.4 *The hierarchy of decisions in risk management within the drinking water sector (Pollard, 2008).*

National guidelines and frameworks for risk management of drinking water systems have been developed in many countries, such as Australia (NHMRC/NRMMC, 2004), New Zealand (Ministry of Health, 2005a; 2005b), Sweden (SNFA, 2007; SWWA, 2007), Denmark (DWWA, 2006) and Norway (NFSA, 2006). Dalgleish and Cooper (2005) point out that it can be a difficult task for water utilities to adopt a management approach that focuses on avoiding losses and taking advantage of opportunities.

Although efforts are made to manage risks efficiently, possibilities for further improvements exist. This not only includes water utilities but also other stakeholders such as governmental authorities. The Swedish National Audit Office (SNAO) has scrutinised the preparedness for severe crises in the Swedish water supply. Some of the main conclusions are that limitations in the ability to manage crises exist, the quality of risk and vulnerability analyses is not good enough and governmental support is insufficient (SNAO, 2008). Positive trends have also been identified, such as increased collaboration between municipalities and local awareness of issues related to crisis management.

Water Safety Plans

As already noted the WHO (2008) emphasises a risk-based approach when managing drinking water systems. A guidance framework for safe drinking water has been described (Figure 2.5). A key element in the framework is the WSPs, in

which risks in source waters, treatment plants and distribution networks should be assessed and managed in an integrated, from source to tap, manner. The WSPs should be guided by health-based targets and independent surveillance should ensure the quality of the work and promote improvements.

Bartram *et al.* (2009) describe the WSP approach as a risk management strategy that aims to consistently ensure the safety and acceptability of a drinking water supply. The WSPs include system assessment, monitoring and management plans (Figure 2.5). The system should be assessed to determine whether it is capable of delivering water that meets the health-based targets. The system assessment should include the entire system and consider interactions between elements. The purpose of monitoring is to assess control measures in order to ensure that the system is operating properly. Management plans should be developed to document and communicate relevant information. As part of WSPs the use of risk ranking for assessing risks is suggested by the WHO (2008), Bartram *et al.* (2009), Davison *et al.* (2005) and others. Risk ranking is described in Section 3.1.

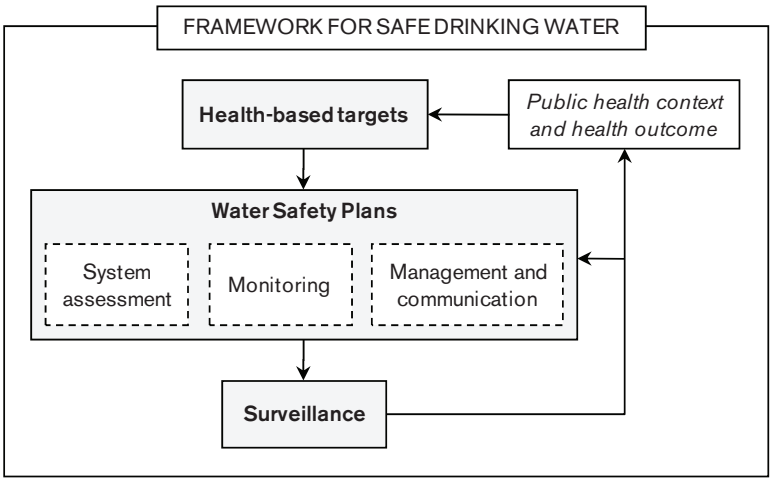


Figure 2.5 The framework for safe drinking water as presented by the WHO (2008).

The WSP approach includes principles and concepts from the multi-barrier approach (described further below) and the Hazard Analysis and Critical Control Point (HACCP) system. The HACCP system originates from the food industry and can be described as a systematic way of identifying specific hazards and measures for their control (Codex, 2003). Havelaar (1994) presented the first application of HACCP to drinking water and the principles have afterwards been used in different ways within the drinking water sector (e.g. Damikouka *et al.*, 2007; Dewettinck *et al.*, 2001; Gunnarsdóttir and Gissurarson, 2008; Hamilton *et*

al., 2006; Howard, 2003; Jagals and Jagals, 2004; Mullenger *et al.*, 2002; Yokoi *et al.*, 2006). However, it has been pointed out that HACCP is most suitable to apply in the treatment part of a drinking water system, and is not applied as easily to the important areas of source water and distribution system (e.g. Hamilton *et al.*, 2006; Hrudey, 2004; NHMRC/NRMMC, 2004).

The Bonn Charter for Safe Drinking Water (IWA, 2004) is a complementary document to the guidelines provided by the WHO (2004; 2008) and emphasises the WSP approach. The document includes key principles that are considered essential in order to create a management framework for a reliable supply of safe drinking water. WSPs are currently being implemented in countries around the world and are thus an important part of risk management of drinking water systems (e.g. Breach and Williams, 2006; Garzon, 2006; McCann, 2005; Vieira, 2007). Furthermore, the ongoing revision of the Drinking Water Directive 98/83/EC (EC, 1998) will most likely lead to a stepwise implantation of the WSP approach in the Directive.

Two contrary but also complementary approaches

One of the basic ideas in risk management is to work proactively to avoid or reduce risks to an acceptable level. If actions are taken only after failures and near mishaps a reactive approach is used, which can be considered as the opposite to proactive risk management. Within the drinking water sector, end-product testing (compliance monitoring) is used to monitor the water quality. End-product testing can be seen as a reactive approach but is a necessary part of water quality management. However, end-product testing cannot be used as the only means to guarantee safe drinking water (e.g. WHO, 2008). Weaknesses of end-product testing include the limited number of pathogens and contaminants that can be analysed and the time it takes to complete analyses (CDW/CCME, 2004; Sinclair and Rizak, 2004; Vieira, 2007). Rizak *et al.* (2003) point out that experience of waterborne disease threats and outbreaks have shown that end-product testing is not sufficient to guarantee safe water quality. If unacceptable water quality is detected in the drinking water distributed to the taps, at least some consumers will use the water before the analysis is completed and corrective action has been taken. End-product testing should be used as a tool for verifying that the water is/was safe to drink but not as the only means of guaranteeing safe drinking water. Note that the current version of the Drinking Water Directive 98/83/EC is based on end-product testing (EC, 1998).

Instead of relying solely on end-product testing, the use of a multi-barrier approach is advocated by many (e.g. CDW/CCME, 2004; WHO, 2008). The multi-barrier approach is based on implementation of multiple barriers throughout the drinking water system, from source to tap. The barriers are supposed to block or control hazards to prevent them from causing any unacceptable harm (Figure 2.6). Since multiple barriers are used, failure of one or more barriers can be compensated for by the others. Reason (1990) described the concept of multiple barriers using a *Swiss cheese model*, where the holes in the cheese slices illustrate that the barriers cannot stop all hazards (Figure 2.6). In a drinking water system it is not only the treatment plants that should include barriers. Protection of source waters and distribution systems, as well as training of personnel, is important to achieve an efficient multi-barrier approach.

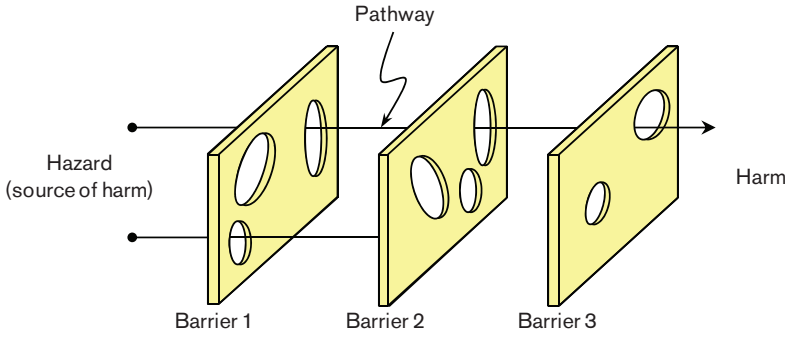


Figure 2.6 *Illustration of how a hazard may cause harm if existing barriers are unable to prevent a pathway (after Reason, 1990).*

The integrated approach

A drinking water system may be described as a supply chain, including a water source, a treatment plant and a distribution system. However, the system actually consists of a large number of subsystems and components that interact in different ways. Events at the water source may, for example, affect treatment and distribution. As described in Section 2.1, drinking water systems typically have an inherent ability to compensate for failures in different ways. A drinking water system can thus not be described as a traditional series system where failure in one part automatically leads to failure of the whole system. Hence, as stated in, for example, the Australian guidelines on drinking water (NHMRC/NRMMC, 2004) and by the WHO (2008), efficient management of drinking water systems requires that consideration is given to the entire supply chain. This means that all parts, from source to tap, or even more comprehensively from catchment to consumer, should be considered.

An integrated *from source to tap* approach can be used in risk assessments to minimise sub-optimisation of risk-reduction measures and, consequently, enable more efficient use of available resources. Sub-optimisation may arise if, for example, only the treatment system is analysed and considered when selecting risk-reduction measures. It might be more efficient to take actions to protect the water source or spend money on maintenance and upgrading the distribution network. It should, however, be noted that integrated analyses cannot replace analyses of specific parts of the system or specific hazardous events. The different types of analysis should complement each other in efficient risk management.

2.5 Risk assessment

Risk assessments are initiated by decision problems and the aim is to provide relevant and accurate information to support decisions (Section 2.3). The basic steps included in risk assessment are to estimate the risk level based on identified hazards, determine whether or not the risk is acceptable and, if necessary, identify and analyse risk-reduction measures (Figure 2.2). The identification of hazards can be based on experiences from the past, brainstorming, checklists (e.g. Beuken *et al.*, 2008; Nadebaum *et al.*, 2004; Olofsson *et al.*, 2001)and structured methods such as *What if* analysis, Hazard and Operability Analysis (HAZOP), Failure Modes and Effects analysis (FMEA) and Hierarchical Holographic Modelling (HHM) (e.g. Haimes, 2009; Hokstad *et al.*, 2009; Kletz, 2001; Mannan and Lees, 2005; Nolan, 1994). A large number of methods are available for use when estimating risk levels and modelling risk-reduction measures. Most methods can be categorised as either qualitative or quantitative. Qualitative methods aim to describe the risk in words or using classes, whereas the quantitative methods express the risk in numerical values. The term semi-quantitative is sometimes used to describe methods that are mainly qualitative but where, for example, probability and consequence classes are assigned numerical values (Section 3.1). The values represent a relative difference but they are not probabilities, physical measures of consequences or similar. When referring to qualitative methods in this thesis, however, both strictly qualitative and semi-quantitative methods are considered. An example of a method that can be strictly qualitative but also semi-quantitative is risk ranking, including risk matrices, which is describe further in Section 3.1. Another example of a qualitative methods used within the drinking water sector is DRASTIC, which is used to assess groundwater vulnerability (Aller *et al.*, 1987; Rosén, 1994; 1995).

Quantitative methods are typically used when the analysed system is complex and to facilitate comparison with other risks and acceptable levels of risk in absolute terms. Kaplan (1991) explains some basic ideas linked to quantitative risk assessment. A wide range of quantitative methods exist. Some are comprehensive with a wide field of application while others are used only to assist in specific parts of an analysis. Examples of methods are quantitative microbial risk assessment, quantitative chemical risk assessment, fault tree analysis, event tree analysis, reliability block diagrams, Bayesian belief networks and Markov models (e.g. Haas *et al.*, 1999; Hokstad *et al.*, 2009; Rausand and Høyland, 2004; Rosén *et al.*, 2007; van Leeuwen and Vermeire, 2007). Fault tree analysis and Markov models are described in Section 3.2.

System analysis

When analysing a system in order to identify possible undesired events and estimate the risk, it is necessary to have a good understanding of the system. To estimate risks and determine the effect of risk-reduction measures, models of a system or parts of a system are often required. It should be stressed that a model is always just a model and does not represent truth (West and Harrison, 1997). However, by creating a model based on a good understanding of the analysed system and a solid theoretical foundation, it is possible to achieve a useful model that can assist decision-making. The illustration in Figure 2.7 shows how a model can be built based on investigations of the truth. The model is affected by our perception of reality and can, if it is built and used properly, work as a decision aid.

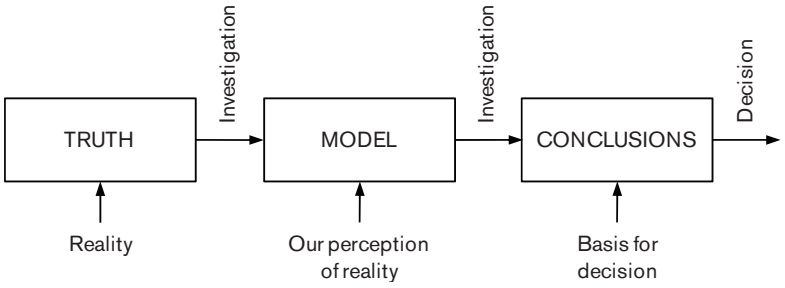


Figure 2.7 *Illustration of how a model can be used to represent the truth and provide information to decision-makers (Vesely et al., 1981).*

The outline of a technical system can be described as in Figure 2.8. This is a generic description of a system but illustrates important aspects of, for example, a drinking water system and can be used to describe the origin of risks. As with the

system in Figure 2.8, a drinking water system is built up of subsystems such as raw water sources, treatment plants and distribution networks. The subsystems interact and use different types of input and support to produce wanted outputs. The wanted output of a drinking water system is of course a reliable supply of safe drinking water. To obtain this output, inputs such as raw water of sufficient quality, power supply to run pumps and chemicals for the treatment plant are needed. If the inputs needed are unavailable it may not be possible to supply drinking water to the consumers. Unwanted inputs can also enter the system and cause problems. For example, microbial contaminants in the raw water can cause an unwanted output in terms of drinking water of unacceptable quality. Failures may occur in the system, e.g. failure of technical components, and can also be caused by external threats, such as flooding. Hence, the origin of risks to a drinking water system, and consequently also the consumers, can be problems of wanted inputs, unwanted inputs, failures in the system or events caused by external threats. Factors such as the technical condition of the system and existing problems constitute the boundary conditions that define the system and affect the risk.

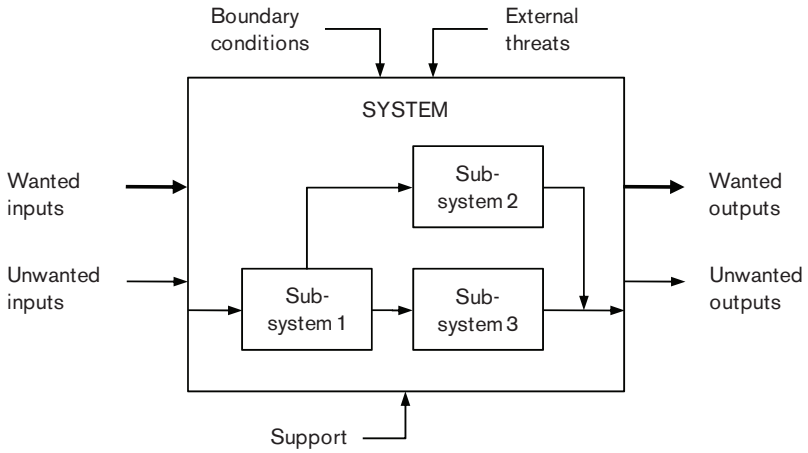


Figure 2.8 Generic illustration of a technical system (Rausand and Høyland, 2004).

Risk evaluation

The main purpose of risk evaluation is to determine whether or not the risk, before and after risk-reduction measures are implemented, is acceptable. The risk can be compared to predefined acceptance criteria or based on other approaches. A principle commonly used to evaluate risks is the As Low As Reasonable Practicable (ALARP) principle, see Figure 2.9 (e.g. CAN/CSA, 1997; Melchers, 2001). The ALARP principle implies that a risk can be: unacceptable, i.e. must be

reduced or eliminated under any circumstances; acceptable, i.e. can be left without further action; or between acceptable and unacceptable and *may* be accepted if it is economically and/or technically unreasonable to reduce it (the ALARP region).

Other possible approaches in risk evaluation are the principles of reasonableness, proportionality, allocation, and avoidance of disasters (Davidsson *et al.*, 2003). What is an acceptable risk depends on several factors. Examples of factors affecting how humans perceive risk are personal control, voluntariness and familiarity (Renn, 1998; 2008). Havelaar and Melse (2003) point out similar factors relevant specifically to drinking water safety. Hunter and Fewtrell (2001) presented a possible approach that can be used when determining whether or not risks related to drinking water are acceptable. Furthermore, Murphy and Gardoni (2008) present a set of criteria to be considered when choosing a proper approach to determining acceptable risk.

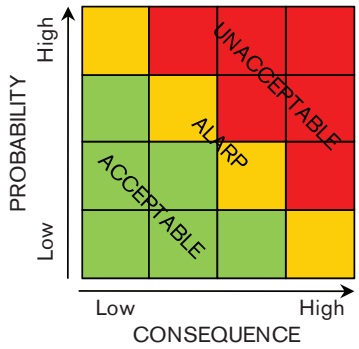


Figure 2.9 *Risk matrix used to illustrate the ALARP (As Low As Reasonable Practicable) principle. The green, orange and red represent acceptable risk, the ALARP region and unacceptable risk respectively. Risk matrices are described further in Section 3.1.*

Risk-reduction measures

In order to treat risks in a proper manner suitable risk-reduction measures must be designed (e.g. Rosness, 1998). In some situations it may be possible avoid the risk and sometimes it is sufficient to monitor the risk. However, most often a strategy for reducing the risk to an acceptable level is needed. If risk is viewed as a combination of the probability and the consequence of an event (Section 2.2), three categories of measures can be described: (i) those reducing the probability of the undesired event; (ii) those reducing the consequences of the events; and (iii) those reducing both the probability and the consequences. In reality, the

effect of risk-reduction measures may be much more complex but this categorisation can help in discussions on strategies for risk reduction.

A risk-reduction measure may affect the risk related to several different events and more than one measure may be required to reduce one specific risk to an acceptable level. Different safety measures exist, such as installation of an additional treatment step or training of water utility personnel, but they all aim to reduce the risk. When analysing risk-reduction alternatives it is important, especially when the risk is within the ALARP region, to consider that *no action* may also be a possible course of action.

2.6 Decision analysis

To make well-informed decisions about, for example, risk-reduction measures, information about possible alternatives must be evaluated in a structured manner. Keeney (1982) describes decision analysis as *"a formalisation of common sense for decision problems which are too complex for informal use of common sense."* Hence, decision analysis is about helping decision-makers to evaluate and compare alternatives using necessary models and tools so that relevant and informative results can be provided.

To analyse a decision problem can be compared to solving a puzzle (Figure 2.10). The problem can be simple, i.e. a puzzle with a few pieces, or complex, i.e. a puzzle with many pieces. You may have little knowledge or be quite sure about what the puzzle will look like in the end, just like you may have different amounts of information about the alternative actions before the analysis is started. In the end you may have the full picture of the problem or there may be parts missing and these pieces may be difficult or impossible to find. Hence, subjective information, e.g. expert judgements, may be needed to fill in the missing gaps. The overall aim of solving a puzzle/analysing a decision problem is to put the pieces/the information together correctly.

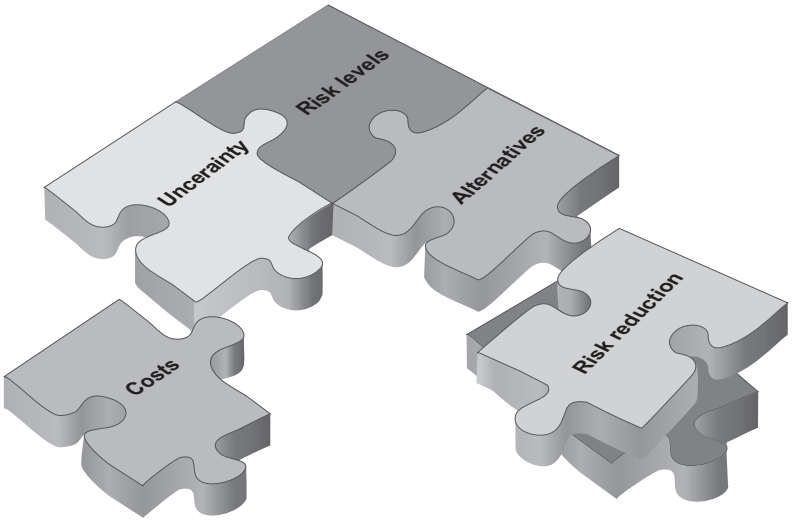


Figure 2.10 *Illustration of a decision problem as a puzzle. The pieces represent information relevant to the decision problem.*

The context of decision problems may look very different. However, Keeney (1982) lists five generic aspects relevant to decision problems:

- A perceived need to accomplish some objectives.
- Several alternatives, one of which must be selected.
- The consequences associated with alternatives are different.
- Uncertainty, usually about the consequences of each alternative.
- The possible consequences are not valued equally.

To deal with the above five aspects Keeney (1982) describes decision analysis based on the four steps: (1) structure the decision problem; (2) assess the possible impacts of each alternative; (3) determine the preference (values) of decision-makers; and (4) evaluate and compare the alternatives. This structure is very much in line with the decision-making process as presented by Aven (2003), see Figure 2.3. Different decision criteria can be used to evaluate alternatives and one of the most common is to maximise expected utility.

There are basically three disciplines of decision theory: (1) descriptive, (2) normative and (3) prescriptive. Descriptive decision models aim to describe *how decisions are made* by people. The purpose of normative models, in contrast, is to describe *how decisions should be made* to be rational according to predefined rules. The prescriptive models aim to support decision-making by providing a

structure that avoids typical pitfalls and makes sure the decision-maker considers aspects identified as relevant. Prescriptive models can be seen as an aid to make decisions more in line with the normative theory. The decision models presented in this thesis are of a prescriptive nature and decision analysis here is used to refer to normative/prescriptive decision analysis.

The work of von Neumann and Morgenstern (1947) and Savage (1954) is often considered to be the basis of normative decision theory. They presented a set of axioms that should be fulfilled for a decision to be rational. Keeney (1982) concludes that according to these axioms the attractiveness of alternatives should be determined by the likelihood of possible consequences and the decision-makers' preference for those consequences. Some decision problems require that consideration is given to several criteria and Keeney and Raiffa (1993) describe decisions with multiple objectives (see Section 3.4).

3 METHODS

This chapter includes a description of the underlying methods and techniques used in the risk assessment method and in the decision models developed and presented in this thesis.

3.1 Risk ranking

A common way to assess risks is to identify the events that may cause harm, assign to each event a probability and a consequence based on discretised scales, and present the results in a risk matrix (Figure 3.1). This kind of assessment is referred to here as *risk ranking*. The aim of risk ranking is to determine the relative severity of the risks. Methods for risk ranking are applied in many fields (Burgman, 2005) and, as described in Section 2.4, risk ranking is suggested as a means of assessing risks in WSPs. The decision models presented in Paper V and Section 5.4 are based on a risk ranking approach to evaluate risk-reduction measures.

The main steps in risk ranking are to: (i) identify undesirable events; (ii) define discretised probability and consequence scales, i.e. the axes in the risk matrix; (iii) define risk tolerability criteria, i.e. what risks (combinations of probability and consequence) are acceptable, unacceptable and within the ALARP (As Low As Reasonable Practicable) region; (iv) assess the probability and consequence of each event using the scales; and (v) plot the risks in the matrix and evaluate them based on their position. An example of a risk matrix is presented in Figure 3.1. A key part of risk ranking is to define the probability and consequence scales. To include all relevant probabilities and consequences the scales are often not linear but rather of a logarithmic nature. The scales can be ordinal, i.e. comparative, and the classes expressed as high, medium, low, etc. However, the classes can also be assigned numerical values on an interval scale representing the severity in relation to the other classes. An example of how a set of classes ($x = 1, 2, ..., n$) can be translated into values is

$$v_x = A^{x-1} \tag{3.1}$$

where v_x is the value representing the relative severity of class x and A is a factor determining the difference between the values (Paper V). The matrix in Figure 3.1 includes four probability and consequence classes and the value of each class has been calculated using Equation (3.1) with $A = 2$. The reason for assigning values to the classes is typically to calculate risk priority numbers/risk scores Figure 3.1. If the events in a risk ranking are described using a probability (p) and a consequence (c) a risk priority number (R) can, for example, be calculated as

$$R = p^a \cdot c^b \tag{3.2}$$

where a and b are weights representing the relative importance of the probability and the consequence respectively (Paper V). The risk priority numbers in Figure 3.1 are calculated using Equation (3.2) with $a = b = 1$. The probability and consequence are thus considered to contribute equally to the risk. When risk priority numbers are calculated in a risk ranking it is sometimes referred to as a semi-quantitative method instead of qualitative. However, to simplify, all risk ranking methods are here referred to as qualitative methods (Section 2.5).

As shown in Figure 3.1, the ALARP principle (Section 2.5) is often used in risk matrices to distinguish between different risk levels. For further descriptions of risk ranking and risk matrices, see e.g. the Australian/New Zealand standard on risk management (AZ/NZS, 2004a). The use of risk ranking in WSP is presented by e.g. Bartram *et al.* (2009).

The reason why risk ranking is commonly applied is most likely because it is easy to perform and the results are relatively easy to understand and communicate. The method has, however, limitations that are important to be aware of. An event may, for example, have several possible outcomes but in risk ranking this is typically not considered. It is often not an isolated event that causes a problem but rather a chain of events. Chains of events and interaction between events are not easily considered in risk ranking, where a discrete approach for events is used. Furthermore, there is no common procedure for uncertainty analysis in risk ranking. The limitations of risk ranking and risk matrices are discussed further by e.g. Burgman (2005) and Cox (2008).

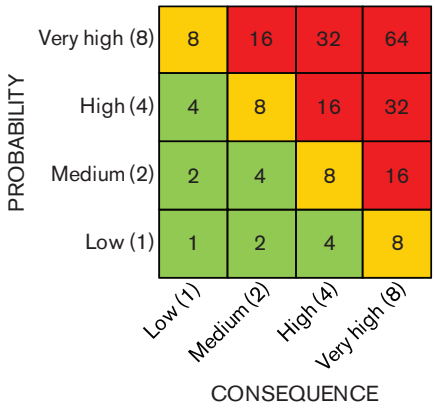


Figure 3.1 *Example of a risk matrix with four classes of probability and consequence. The probability and consequence classes are assigned relative values and a risk priority number is calculated for each combination. The green, orange and red represent acceptable risk (1-4), the ALARP region (8) and unacceptable risk (16-64) respectively.*

3.2 Logic tree models

Analyses of causes and consequences of events can be performed using logic models such as fault trees, event trees, Bayesian networks and Markov models. The quantitative risk assessment method presented and evaluated in Papers I and II and Section 5.2, and further used in Papers III and IV and Section 5.3, is based on fault tree analysis and Markov models.

Fault tree analysis is used in reliability applications to analyse the causes of system failure (e.g. Bedford and Cooke, 2001; Rausand and Høyland, 2004; Vesely *et al.*, 1981; Vesely *et al.*, 2002). A fault tree model is constructed based on the interaction between events and is typically used to calculate the probability of system failure. System failure is represented by the *top event* in the fault tree (Figure 3.2). By using logic gates it is described how the occurrence or non-occurrence of other events may cause the top event to occur. Hence, the top event is divided into its underlying events until a suitable level of detail is obtained. Events at the lowest level of the fault tree are called *basic events* and are the ones that initiate system failure. The logic gates represent interactions between events and are based on Boolean logic. The two most common gates are the OR- and the AND-gate, which are illustrated in Figure 3.2. In the OR-gate the output event occurs if at least one of the input events occurs. In the AND-gate the output event occurs if all input events occur simultaneously. The probability of

the top event (P_F) is calculated based on the probability of the basic events (P_i) using Equations (3.3) and (3.4) for the OR- and AND-gate respectively.

$$P_F = 1 - \prod_i (1 - P_i) \tag{3.3}$$

$$P_F = \prod_i P_i \tag{3.4}$$

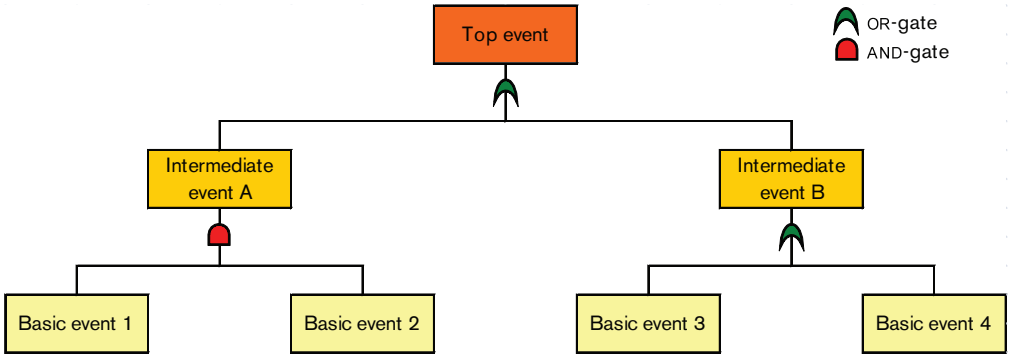


Figure 3.2 Example of a fault tree including the OR- and AND-gates.

Traditional fault trees are often referred to as static fault trees since they are not easily used to model systems where the order of events affects the outcome (Vesely *et al.*, 2002). In addition, dynamic fault trees have been developed to model events in fault-tolerant systems including, for example, spare components and dynamic redundancy (Dugan *et al.*, 1992). What characterises dynamic fault trees are the logic gates designed to model spares and redundancy (Cepin and Mavko, 2002; Durga Rao *et al.*, 2009). Dynamic fault trees are more computationally demanding compared to traditional static fault trees and different techniques for solving them have been developed (e.g. Amari *et al.*, 2003; Boudali *et al.*, 2007; Durga Rao *et al.*, 2010).

A possible way of solving dynamic fault trees is to replace each basic event by a Markov process and translate the fault tree into a Markov model. Using a Markov model a system's transition between different states can be modelled and illustrated. The state diagram in Figure 3.3 can be used to model the OR-gate as well as the AND-gate in Figure 3.2, both of which include two basic events. If the basic events in Figure 3.2 correspond to component failures, then each component may either work (1) or be in a failed state (0). The transition between the two states (0 and 1) is in a Markov model described using a failure rate (λ) and a repair rate (μ) (e.g. Rausand and Høyland, 2004; Ross, 1996). The rates

may also be used to express the mean time to failure ($1/\lambda$) and the mean downtime ($1/\mu$). As illustrated in the Markov model in Figure 3.3 both components may work (11), both may be in a failed state (00) or one of the components may work while one is in a failed state (01 and 10). For the OR-gate the output event (Intermediate event A) occurs in states 10, 01 and 00. For the AND-gate the output event (Intermediate event B) occurs only in state 00. By solving a Markov model the failure rate and repair rate (or the mean time to failure and mean downtime) can be calculated for all states. The probability of failure (P_F) is calculated as

$$P_F = \frac{\text{MDT}}{\text{MTTF} + \text{MDT}} = \frac{1/\mu}{1/\lambda + 1/\mu} = \frac{\lambda}{\lambda + \mu} \tag{3.5}$$

where MDT and MTTF are short for mean downtime and mean time to failure respectively. Note that the probability P_F may also be referred to as the unavailability.

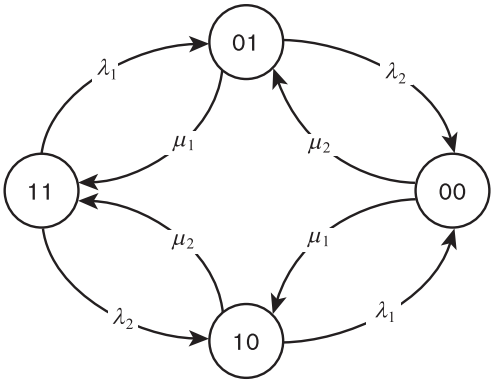


Figure 3.3 *State diagram illustrating a Markov model that can be used to model an OR-gate or an AND-gate, including two basic events. For the OR-gate, system failure occurs when at least one component/basic event is in a failed state (10, 01 and 00). For the AND-gate, system failure occurs when both components/basic events are in a failed state (00).*

A stochastic process is considered to be a Markov process, i.e. have Markov properties, if the future development only depends on the present state and is independent of previous states. Translating dynamic fault trees into Markov models makes it possible to model systems correctly (Dugan *et al.*, 1992) and calculate not only probabilities of failure but also failure rates and repair rates. However, Dugan *et al.* (1992) and others advocate that when the analysed system is not simple the construction of Markov models is tedious and error-prone. The

risk assessment method presented in Section 5.2 and Papers I and II includes approximate dynamic fault tree calculations which are based on Markov models but are less computationally demanding compared to complete Markov simulations.

3.3 Economic analysis

The economic resources of every organisation are limited and economic analyses are consequently important when, for example, evaluating risk-reduction measures. In Papers IV and V and Sections 5.3 and 5.4, economic analysis is included and the results are combined with risk assessment results to facilitate well-informed decision-making.

Depending on the decision problem, different methods can be used in economic analysis. Examples of methods are cost-effectiveness, cost-benefit, cost-utility and cost-feasibility analysis (Levin and McEwan, 2001). A cost-feasibility analysis simply aims to determine the cost of an alternative to see if it can be carried out within a given budget. Cost-effectiveness analysis, however, provides a combined assessment of both the costs and the effects of a safety measure. The effect is expressed in non-monetary units, such as a reduced risk level. Cost-utility analysis is similar to cost-effectiveness analysis but the effect is measured based on subjective assessments rather than objective measureable outcomes. Both cost-effectiveness and cost-utility analysis are tools to identify which alternative provides a specific level of effect/utility at the lowest cost or yields the highest effect/utility at a specific cost. Since the costs (C_{jt}) of, for example, a risk-reduction measure occur over several years (t) the costs can be discounted and the present value (C_j) calculated as

$$C_j = \sum_{t=1}^{T} \frac{C_{jt}}{(1+r)^{t-1}} \tag{3.6}$$

where T is the time horizon and r is the discount rate. Using the present value the total cost of different alternatives can be compared. The effects of alternatives studied in a cost-effectiveness analysis may also be discounted if they occur over several years (Section 5.3). In a cost-effectiveness analysis the cost required to obtain a single unit of effect is represented by a cost-effectiveness ratio (CER) calculated as

$$CER_j = \frac{C_j}{E_j} \tag{3.7}$$

where E_j is the effect of measure j.

Cost-benefit analysis differs from the other methods by measuring both costs and effects as well as other benefits in monetary units (e.g. Boardman *et al.*, 2006; Johansson, 1993). By discounting both costs and benefits and calculating the net benefit, it can be concluded whether or not an alternative is desirable, i.e. has a positive net benefit.

3.4 Multi-criteria decision analysis

Multi-criteria decision analysis (MCDA) is a technique for evaluating and comparing possible alternatives based on several criteria. The decision models presented in Paper V and Section 5.4 are based on MCDA.

Although a vast number of different MCDA techniques exist they all aim to help decision-makers to handle information on possible alternatives consistently. In addition to MCDA, the terms multi-criteria analysis (MCA) and multi-attribute decision analysis (MADA) are also used to describe this type of technique. Here, the term MCDA is used to describe analyses where alternative actions are evaluated and compared with each other in order to prioritise them. Some methods provide a ranked list of alternatives whereas others identify the most preferable one or only identify what alternatives are acceptable. A comprehensive description of MCDA is provided by the Department of Communities and Local Government in the UK (Communities and Local Government, 2009) and the theoretical background to decisions with multiple objectives is described in detail by Keeney and Raiffa (1993). A discussion on some of the basic principles and challenges related to MCDA is presented by Roy (2005).

The basic idea of MCDA is to help decision-makers to evaluate and compare a set of alternatives based on their performance using a set of criteria. The overall goal of the decision is divided into objectives representing important dimensions that must be considered. The objectives are further divided into criteria that are used to measure to what extent the analysed alternatives fulfil each objective and thus the overall goal.

The performance for different criteria in respect of an alternative may be measured either qualitatively or quantitatively. To be able to compare the different performances and combine them into a common unit, scales representing relative preference are used. For each criterion the performance is translated into a scale, for example from 0 to 1, where 0 represents the least preferable and 1 the most preferable outcome. Based on a linear additive approach an overall score, a weighted sum, of an alternative (s_j) can be calculated as

$$s_j = \sum_m s_{jm} w_m \tag{3.8}$$

where s_{jm} is the alternative's (j) performance score for each criterion (m) and $w_{jm} \geq 0$ are weighting factors that determine the relative importance of each criterion. The weighted sum is calculated based on the assumption that the criteria are mutually preference independent. This means that the preference scores assigned to the measures for one criterion do not depend on the preference scores for the other criteria (Keeney and Raiffa, 1993).

The results of an MCDA model can be presented in different ways and can also be evaluated based on different approaches. An important aspect to consider is whether or not strong performance for one criterion may compensate for weak performance for other criteria. Hence, a compensatory or non-compensatory approach can be used. In a non-compensatory mode, critical performance levels can be defined and alternatives that do not meet this level are disqualified.

An advantage of MCDA is that it provides transparency so that applied objectives and criteria, as well as the way information is merged, can be scrutinised and updated when necessary. MCDA applications related to drinking water supply are frequently found in the literature (e.g. Bouchard *et al.*, 2010; Joerin *et al.*, 2009). A review of MCDA-related techniques for water resource management was performed by Cohon and Marks (1975) and more recently by Hajkowicz and Collins (2007). In the latter study, the main challenges for water resource MCDA research were identified. One of the main conclusions was that there is a need for improved handling of risk and uncertainty in MCDA models. It was also concluded that there is a need of better means for incorporating risk preferences of decision-makers in MCDA models. The MCDA models presented in Section 5.4 and Paper V are devised to consider uncertainties in a formalised manner. An overview of how uncertainties can be taken into consideration in MCDA is presented by Stewart (2005).

3.5 Monte Carlo simulation

Monte Carlo simulation is a technique for including uncertainties in model results based on uncertainties in input variables. This technique is used in the work presented in Papers I-V.

Monte Carlo simulation uses random numbers to sample values from probability distributions representing the input variables (e.g. Ang and Tang, 2007; Bedford and Cooke, 2001). In a model with *n* input variables one value from each probability distribution is selected and used to calculate the result. This is performed iteratively, 10,000 times for example, in order to select values representing the entire probability distribution and obtain a probability distribution that represents the result (Figure 3.4).

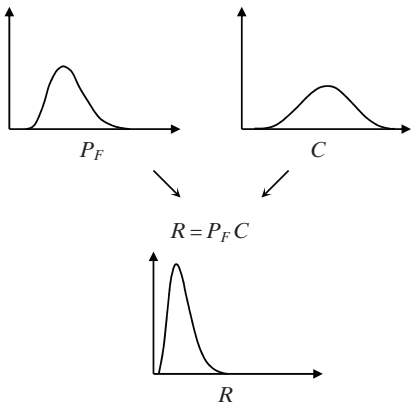


Figure 3.4 *Illustration of how Monte Carlo simulations can be used to include uncertainties in input variables (P_F and C) and the result (R).*

4 THE PAPERS

This chapter is made up of summaries of the five papers that are part of this thesis. The main findings are presented here and in Chapter 5 the outcome of the papers is further presented in combination with additional analyses.

4.1 Overview of the papers

An overview, including the title and the type of work presented in each of the five papers, is presented in Table 4.1. In Paper I, a quantitative risk assessment method for considering entire drinking water systems is presented and applied. The theoretical foundation of the method is evaluated in Paper II and in Paper III the method is used to model and analyse possible risk-reduction measures in a case study. In Paper IV, results from the quantitative risk assessment method is combined with economic analysis to provide decision support for prioritising risk-reduction measures. To facilitate the use of risk ranking, i.e. qualitative risk assessment, to not only prioritise risks but also to evaluate risk-reduction measures, two models for multi-criteria decision analysis (MCDA) are described and applied in Paper V. The MCDA models make it possible to (1) use risk ranking to provide decision support similar to the results from the quantitative risk assessment method and (2) to perform formalised uncertainty analysis of the MCDA outcomes.

4.2 Paper I: Dynamic fault tree method

A quantitative and probabilistic risk assessment method based on the fault tree technique is presented in Paper I. The method was developed because of the identified need of quantitative methods that can be used to analyse an entire drinking water system, form source to tap. The reason the method was based on fault tree analysis is that drinking water systems are often complex with interactions between subsystems and components. It is thus important that chains of events can be modelled. A probabilistic approach is used so that uncertainties of estimates can be included. A generic fault tree model is presented which shows the main failure categories and how the system structure can be reflected in a

Table 4.1 Overview of the five papers included in this thesis.

PAPER	TITLE	SHORT TITLE	TYPE OF WORK
I	Fault tree analysis for integrated and probabilistic risk analysis of drinking water systems	Dynamic fault tree method	Method development and case study
II	Approximate dynamic fault tree calculations for modelling water supply risks	Method evaluation	Evaluation work
III	Comparing risk-reduction measures to reach water safety targets using an integrated fault tree model	Modelling risk reduction	Case study
IV	Cost-effectiveness analysis of risk-reduction measures to reach water safety targets	Evaluating risk reduction	Method development and case study
V	Risk-based multi-criteria decision models for prioritising water safety measures	Decision models	Method development and case study

fault tree model. The method is designed to model two main types of failure: (1) quantity failure, i.e. no water is delivered to the consumer; and (2) quality failure, i.e. water is delivered but does not comply with water quality standards. Traditional fault trees calculate the probability of failure. This method, however, is based on a Markovian approach with dynamic fault tree calculations which provides information on risk levels, probabilities of failure, failure rates and downtimes of the entire system and its subsystems. The risk is expressed as Customer Minutes Lost (CML), i.e. the number of minutes per year the average consumer is not supplied with drinking water (quantity risk) or supplied with drinking water of unacceptable quality (quality risk). The two risk types are presented separately. In Paper I, the drinking water system in Gothenburg, Sweden, is used to exemplify method application.

The main findings of the paper are:

- The complexity of drinking water systems, including the inherent ability to compensate for failure, makes fault tree analysis a suitable tool to model and analyse failures.
- Traditional (static) fault tree calculations are not always informative enough when analysing drinking water systems. Dynamic fault tree calculations based on a Markovian approach provide more useful results and can be used to analyse the entire system as well as the different subsystems.

- CML is showed to be a useful measure for expressing the risk and in combination with the failure rate and mean downtime also the dynamic behaviour of the system can be analysed.
- The probabilistic approach used in the method makes it possible to calculate, for example, the probability of not meeting acceptable risk levels and to analyse what input data contributes most to the uncertainties in the results. This type of information makes it possible to better understand the system and the risk, compared to if only point estimates are used.
- Integrated risk assessment, including the entire system, is important to avoid overlooking important interactions between subsystems.

4.3 Paper II: Method evaluation

The theoretical foundation of the fault tree method (Paper I) is presented and thoroughly evaluated in Paper II. To provide useful results and enable modelling of complex drinking water systems, a Markovian approach is suggested in the fault tree method. To simplify model building and calculations, the fault tree method uses approximate dynamic fault tree calculations and Monte Carlo simulations instead of complete Markov simulations. For three parts of the fault tree model presented in Paper I, the approximate dynamic fault tree calculations are compared to complete Markov simulations. The comparison is made with respect to the probability of failure, the failure rate and the downtime. The three fault tree examples include different types of logic gates and number of events. In addition to the traditional OR- and AND-gates, the examples included two variants of the AND-gate, which makes it possible to model fault-tolerant systems including spare components and dynamic redundancy. The results showed that when only the traditional OR- and AND-gates are used the dynamic fault tree calculations are consistent with the Markov simulations. For the two variants of the AND-gate, small errors were observed for one of them and for the other the error increase with the number of compensating events included. The possible error must, however, be viewed in relation to the sometimes substantial uncertainty caused by uncertainty of input data.

The main findings of the paper are:

- The errors that may occur in the approximate dynamic fault tree calculations are in most cases acceptable with respect to the large uncertainties of input data. If only traditional logic gates are used the errors are negligible.

- The variants of the traditional AND-gate are necessary to model correctly the dynamic behaviour of fault-tolerant systems including, for example, spares and dynamic redundancy.
- The approximate dynamic fault tree calculations facilitate model building and calculations that are less computationally demanding compared to Markov simulations. Hence, the approximate calculations in combination with Monte Carlo simulations make the method applicable in practice.

4.4 Paper III: Modelling risk reduction

An application of the dynamic fault tree method to model risk-reduction measures is presented in Paper III. The drinking water system in Gothenburg is used as a case study site and a structured and thorough analysis of risk-reduction measures is performed. The risk-reduction measures included increased production capacity at the treatment plants and new raw water sources. It is the quantity-related risk that is analysed, i.e. interruptions in the supply. Based on the effect each measure is assumed to have on the specific components of the system, the fault tree model is updated. The possible measures are compared based on the risk reduction they provide and the uncertainty in this effect. It is showed how risk-reduction measures and combinations of measures can be evaluated and compared to provide decision support.

The main findings of the paper are:

- Risk-reduction measures can in a logical manner be modelled by updating input data and restructuring, adding and/or deleting events in a fault tree model. By comparing the results between the original and the new models, risk reduction and other effects resulting from the measures can be quantified.
- Uncertainties are important to consider when analysing the effects of risk-reduction measures. One aspect to consider is the probability of not meeting predefined safety targets What is considered to be a highest acceptable probability of not meeting a safety target may affect the prioritisation of risk-reduction measures.
- By using a model of the entire system when analysing possible changes, it is possible to identify effects that could otherwise have been ignored. For example, changes in one part of the system may affect the interaction with

other parts. Although a measure is intended to reduce the risk it may increase the risk in some part of the system.

- The fault tree method enables structured and thorough analysis of risk-reduction measures.

4.5 Paper IV: Evaluating risk reduction

In Paper IV, the results of the fault tree method are combined with economic analysis and it is shown how the results can be used to support decision-making. The same approach as applied in Paper III is used to model the effect of risk-reduction measures. The Gothenburg drinking water system is used as a case study site and the focus is on interruption in the supply. The measures are also analysed from an economic point of view to identify the most cost-effective alternative and highlight important aspects using cost-benefit calculations. Advantages and limitations with cost-effectiveness analysis are discussed and recommendations are provided regarding how it can be combined with results from quantitative risk assessments. For the Gothenburg system it is shown which alternatives that reduce the risk most and which are considered most cost-effective. The study further identifies aspects not included in the analysis but which may affect the final decision.

The main findings of the paper are:

- Cost-effectiveness analysis provides useful results by combining information on costs and effects. In this case the effect is related to risk reduction. There are, however, limitations that must be known in order to avoid misinformed decision-making.
- If a set of measures are compared solely based on their cost-effectiveness ratios, it may cause a risk reduction that is too low and inefficient use of resources for risk reduction. Instead, the main focus should be on identifying the measures that meet the acceptable risk level at the lowest cost.
- Risk-reduction measures affect the system in many different ways. Consequently, it is important to identify if the measures analysed have important effects not included in the fault tree model and cost-effectiveness analysis.
- Combining quantitative risk assessment results and economic analysis provides a structured and thorough analysis of risk-reduction measures

that facilitates transparency and long-term planning of drinking water systems.

4.6 Paper V: Decision models

Two models for multi-criteria decision analysis (MCDA) are presented and applied in Paper V to evaluate and compare risk-reduction measures for the drinking water system in Bergen, Norway. The decision models are developed to enable the use of risk ranking results, i.e. qualitative risk assessment, to evaluate and compare risk-reduction measures. Both models provide a stepwise procedure for prioritising safety measures based on MCDA. Results from a previously performed risk ranking are used to identify severe risks and risk-reduction measures are identified for four of these. The measures are evaluated based on the effect on three risk types: (1) water quality risks; (2) water quantity/delivery risks; and (3) risks related to loss of reputation/economy. In addition, the cost of implementing the measures is included as a criterion. The differences between the models are: (1) how the benefit of risk reduction is calculated; and (2) how uncertainties are included. Both models consider uncertainties and the probability of not meeting the acceptable risk level. The two MCDA models are evaluated with respect to their theoretical foundation and practical functionality.

The main findings of the paper are:

- A risk-reduction measure is often designed to reduce the risk related to a specific event. It may, however, also impact several other events and this benefit should be included when comparing the costs and benefits of alternative measures.
- It is important to consider the ALARP region (Section 2.5) when evaluating alternative measures. There may be risks that are not reasonable to reduce to an acceptable level but only to the ALARP region.
- Risk ranking is commonly performed but not often used to evaluate risk-reduction measures. The results of a risk ranking can, however, be further used to provide useful decision support regarding risk-reduction measures.
- Uncertainties of estimates can in a practical way be considered in MCDA models and this provides useful information to the evaluation and comparison of risk-reduction measures.

- The two MCDA models presented are examples of how qualitative risk assessment results can be used to evaluate and compare risk-reduction measures in a structured and transparent manner. The models can be adjusted to fit the perception and consider the judgments of the decision-maker.

5 RESULTS AND APPLICATIONS

In this chapter the results in terms of methods developed and case study applications are described. Recommendations and key aspects to consider when applying the methods are also presented.

5.1 A generic framework

As shown in Section 2.3, risk management and decision-making may be described in different ways. The framework in Figure 5.1 was devised by the author and colleagues within the Techneau project to provide a combined structure and a generic description of risk management and decision-making in the context of drinking water supply (Rosén *et al.*, 2010). Here, the aim is to provide an overview of the most important steps and aspects included in water supply risk management and decision-making. The framework is based on the descriptions of risk management produced by the International Electrotechnical Commission (IEC, 1995) and decision-making by Aven (2003), see Section 2.3. The purpose is not to describe a *new* framework but rather to stress the close link between the two processes and clearly illustrate the role of risk assessment results as decision support. Additional components and aspects have been added to the original descriptions to stress, for example, the importance of considering uncertainties, to acquire new information when available, to update models and analyses and to communicate results to the consumers and other stakeholders.

The framework (Figure 5.1) outlines risk management and decision-making as a proactive process where an underlying decision problem initiates a risk assessment and the results are reviewed by the decision-maker before a decision is made. Decision problems initiating risk assessments are often based on the need to prioritise possible alternatives such as risk-reduction measures. A drinking water utility may, for example, want to know the risk a new chemical facility within the watershed would pose to the water source and in the end to the consumers. Questions linked to such a problem could be wheter the risk is acceptable or not, and if not what measure should be taken to reduce the risk? When managing a drinking water system it is important to consider risk related to both water quantity, i.e. supply interruptions, and water quality, i.e. health problems. There may of course also be other risk types important to consider.

As illustrated in the framework, stakeholder values reflected in goals, criteria and preferences affect the decision problems as well as the risk assessment and the subsequent review. Examples of stakeholders are the water utility, the consumers, industries located within the watershed and government authorities. A typical example of criteria used within the drinking water sector is health-based targets defined by authorities. However, water utilities may also define their own performance targets and similar criteria that affect how prioritisations are made. Furthermore, there may be competing interests in society that affect the use of water sources. For example, new roads and railroads within the watershed of a groundwater source may be needed for improved transport, although this also introduces new risks to the water supply due to possible accidents, including hazardous goods.

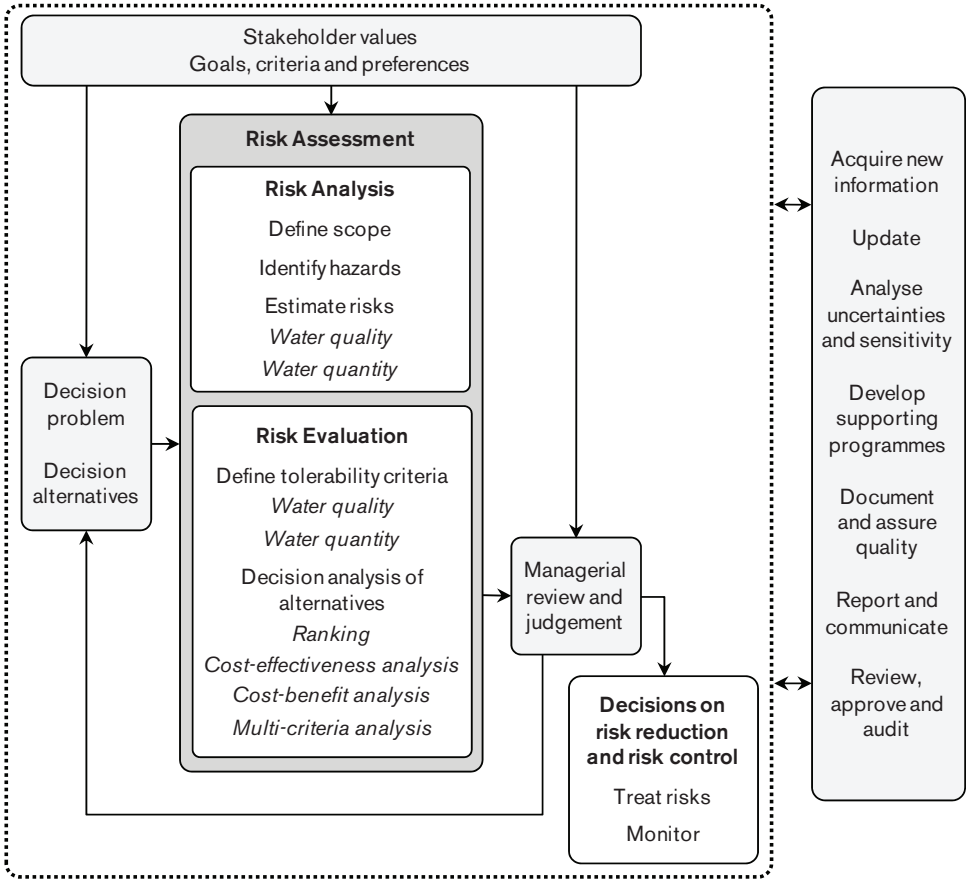


Figure 5.1 *A generic framework illustrating the main steps in risk management and how it is interconnected with decision-making (Rosén et al., 2010).*

Based on the decision problem, suitable methods and tools should be selected and used in the risk assessment to provide useful results that can support decision-making. A decision problem includes a vast number of different dimensions that can be perceived in different ways. In most cases it is not possible to consider all these aspects in a risk assessment. Hence, the risk assessment results provide decision support although a subsequent managerial review and judgement is necessary to consider aspects not possible to include in the risk assessment.

To support the performance of a risk assessment a team of people should be put together. The team should include people with knowledge of the system being analysed as well as people with knowledge of risk assessment and other aspects that may be relevant.

The arrows in Figure 5.1 illustrate the exchange of information between different steps as well as communication with relevant stakeholders. The task of communicating risk is important and carefully performed risk assessments may provide useful results that facilitate communication with decision-makers, consumers and other stakeholders. It is important to emphasise that risk assessment and decision-making should be a continuous and iterative process that is updated when new information becomes available and preconditions change. Furthermore, the framework emphasises that risk assessments and other work need to be reviewed in order to assure the quality.

In addition to the framework (Figure 5.1), tools and guidance documents to support water utilities have been developed within the part of the Techneau project dealing with risk assessment and risk management. Reports have been prepared describing risk management in general and more specifically risk assessment and decision-making (Hokstad *et al.*, 2009; Rosén *et al.*, 2007; Rosén *et al.*, 2010). Furthermore, tools for identifying and analysing risks have been developed, such as databases that include possible hazards and risk-reduction measures (Beuken *et al.*, 2008; Pettersson *et al.*, 2010). Based on the approach to risk management and decision-making presented in Figure 5.1, risk assessment case studies were performed in South Africa, the Czech Republic, Germany, the Netherlands, Norway and Sweden (Lindhe *et al.*, 2010). The aim of the case studies was to evaluate the methods and tools that had been developed and to provide good examples. The method and model applications presented in the subsequent sections of this chapter are examples of these case studies.

5.2 The dynamic fault tree method

A quantitative and probabilistic risk assessment method for considering entire drinking water systems, from source to tap, was developed to overcome the current lack of such methods. The method is based on dynamic fault tree analysis and is presented in Paper I and evaluated in Paper II. The basics of the method are presented below and it is shown how to apply the method and use the results. In Section 5.3 and Papers III and IV there is a description of how to use the fault tree method to model risk-reduction measures.

Method development

The importance of considering the entire drinking water system, from source to tap, when assessing risks is emphasised within the drinking water sector (Section 2.4) although quantitative risk assessments of entire drinking water systems are rare. It was therefore decided to develop a method that could be employed when making such risk assessments. A key requirement for such a method is that it must be able to model the complex structure of a drinking water system, including interactions between subsystems and the ability to compensate for failures (Section 2.1). Furthermore, it was concluded that the method should be quantitative so that risk levels and other results are expressed numerically can thus be compared easily to acceptable risk levels and other performance targets. Since risk is related to uncertainty a probabilistic approach should be applied to enable uncertainty analysis.

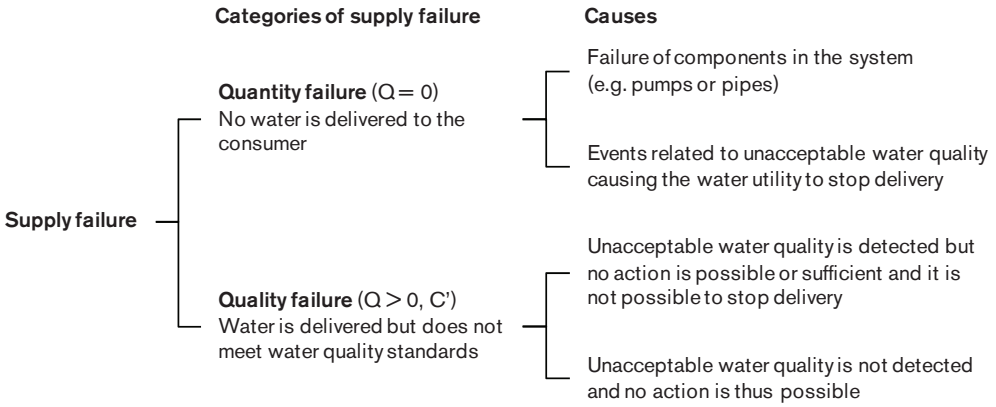
Based on the requirements listed above, fault tree analysis (Section 2.3) was identified as a suitable basis for the method. Using fault tree analysis it is possible to model failures as chains of events and thus consider interactions between components and events. However, it was concluded that traditional fault tree analysis was not sufficient to model drinking water systems correctly and provide sufficiently informative results. Consequently, a Markovian approach was used to consider the dynamic behaviour of a drinking water system (Section 3.2). The main differences between the dynamic fault tree method presented in this thesis and traditional fault tree analysis are: (1) the logic gates that make it possible to model fault-tolerant systems with an ability to compensate for failures; (2) the possibility to calculate not only the probability of failure but also the failure rate and downtime for each event in the fault tree; and (3) the risk levels that are calculated as a function of the probability of failure and information on the proportions of consumers affected by different failures.

Fault tree analysis has previously been applied by, for example, Li (2007) to analyse cause-effect relationships in water supply systems. Beauchamp *et al.* (2010) used it to identify hazards in water treatment and Risebro *et al.* (2007) structured events of quality-related failure using a fault tree.

To facilitate the development of the dynamic fault tree method, it was applied simultaneously to the drinking water system in Gothenburg, Sweden. The Gothenburg system was thus used to identify conditions specific to drinking water systems that needed to be considered in the method. The method is, however, generic and can be applied to any type of drinking water system. A team made up of both researchers and water utility personnel contributed to the task of specifying the scope of the method and then developing and applying it.

Failure types and conceptual model

Failures in a drinking water system may affect the consumers in different ways (Section 2.1). The overall failure event included in the fault tree method is termed *supply failure* and is defined as including: (1) *quantity failure*, i.e. no water is delivered to the consumer; and (2) *quality failure*, i.e. water is delivered but does not meet water quality standards (Figure 5.2). Note that the failure types are defined based on how the consumers are affected. Quantity failure may occur due to failure of technical components such as pipes and pumps, making it impossible to transfer water. However, quantity failure can also be caused by events resulting in an unacceptable raw water or drinking water quality which, in turn, cause the water utility to stop delivery. Quality failure occurs if unacceptable water quality is not detected or if no actions are possible or sufficient and delivery is not stopped.



Q = Flow (Q = 0, no water is delivered to the consumer; Q > 0, water is delivered)
C' = The drinking water does not comply with water quality standards

Figure 5.2 Categories of supply failure and their main causes.

The fault tree method was developed to consider entire systems so that interactions between subsystems could be considered and also to identify how much the different subsystems contribute to the risk. As illustrated in Figure 5.3, the system is divided into its three main subsystems (raw water, treatment and distribution) and it is considered that failure in one part may be compensated for by the subsequent parts. For example, if no raw water can be supplied to the treatment plant, stored water at the treatment plant and service reservoirs within the distribution system can be used and the consumers are not affected until all stored water is used. Spare components, such as reserve pumps, as well as the ability to compensate for failure within a specific subsystem, should of course also be considered.

The above-described failure types and the conceptual view of how failures may occur are of help when constructing fault tree models. Which failure types are included and how the system is divided should of course be adjusted to suit the specific application.

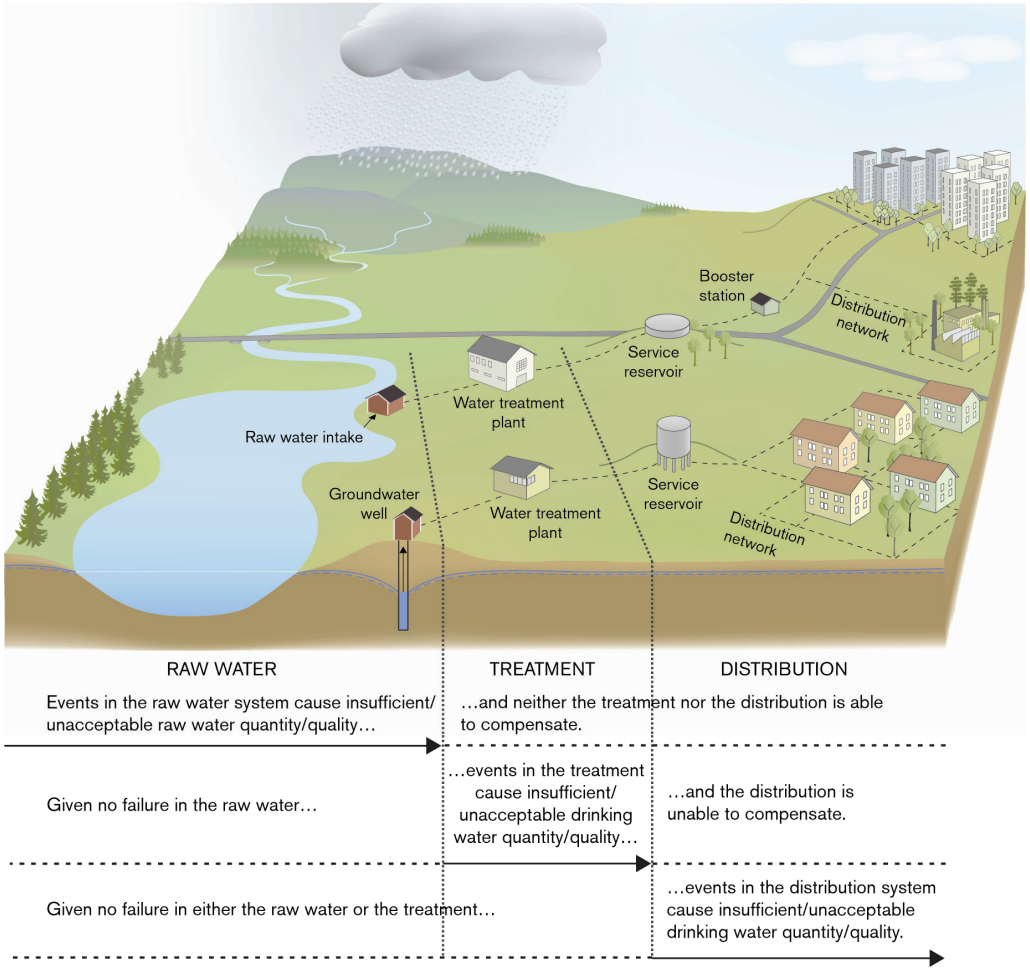


Figure 5.3 *Conceptual model of how quantity and quality failures may occur in a drinking water system and affect the consumers.*

Logic gates and dynamic calculations

To model the dynamic function of drinking water systems a Markovian, dynamic fault tree approach (Section 3.2) is used in the method presented here. Based on the function of drinking water systems and how failures may originate, four logic gates needed to be included. In addition to the traditional OR- and AND-gates, two variants of the AND-gate have been developed (Papers I and II). The variants of the AND-gate have been devised to model a system's ability to compensate for failures and are similar to what in dynamic fault tree applications are referred to as SPARE-gates (e.g. Durga Rao *et al.*, 2010). The traditional OR- and AND-gates are described in Section 3.2 and in Table 5.1 examples are presented of the type

of conditions each of the four logic gates can model. The variants of the AND-gate model how a system, given an initial failure, may prevent the failure from affecting the consumers. Using the first variant, one or more compensating components/events can be included in the model and they are described using a failure rate (λ) and a probability of failure on demand (q). The failure rate corresponds to the time the component may compensate for failure ($1/\lambda$). The probability of failure on demand is included since compensation may not be available at all when needed, due to different reasons such as maintenance.

The second variant of the AND-gate is similar to the first variant but can include only one compensating component/event. The important difference is, however, that the second variant can model the ability of the compensating component to recover after failure, i.e. the downtime ($1/\mu$) is considered. Since a Markov approach is used the events are described using a failure rate (λ), or a mean time to failure ($1/\lambda$), and a mean repair rate (μ), or a mean downtime ($1/\mu$) (Section 3.2). It has been found most suitable to use the failure rate and the mean downtime when discussing the characteristics of events in drinking water systems. These are therefore the variables mainly referred to in this thesis when characterising events. However, the rates λ and μ are used in the calculations. The Markov models for all logic gates are described in detail in Paper II, see also in Norberg *et al.* (2009).

Table 5.1 Examples of conditions in a drinking water system that the different logic gates can model.

LOGIC GATE	EXAMPLE
OR-gate	A raw water source may be contaminated by microbiological, chemical or other contaminants.
AND-gate	To be unable to supply the treatment plant with raw water, all water sources need to be unavailable simultaneously.
First variant of AND-gate	If no drinking water can be transferred from the treatment plant to the distribution system, water stored in reservoirs in the distribution system may compensate for failure for a limited period. Failure on demand may occur if the reservoir is not in use due, for example, to maintenance work.
Second variant of AND-gate	Unacceptable raw water quality may be compensated for by the treatment. If the quality deviation cannot be compensated for at all, the treatment fails on demand. If there is no failure on demand, the quality deviation is compensated for until the treatment efficiency is affected by a failure. When the treatment recovers after the failure compensation is possible again.

To reduce the computational demand, approximate dynamic fault tree calculations are used that do not require Markov simulations. By replacing each basic event in the four logic gates with a Markov process (Section 3.2), equations for calculating the probability of failure, failure rate and mean downtime have been developed, see Table 5.2 (Paper II and Norberg *et al.*, 2009).

Table 5.2 *Equations used for calculating the output of the logic gates. For the variants of the AND-gate $i=1$ corresponds to the failure that may be compensated for by events $i=2, \ldots, n$. For the second variant only one compensating event is considered, $i=2$. Variable P_F is the probability of failure, λ_i the failure rates, μ_i the repair rates ($1/\mu_i$ the mean downtimes) and q_i the probabilities of failure on demand.*

OR-gate	AND-gate
$\lambda = \sum_{i=1}^{n} \lambda_i$	$\mu = \sum_{i=1}^{n} \mu_i$
$\mu = \sum_{i=1}^{n} \lambda_i \cdot \frac{\prod_{i=1}^{n} \mu_i}{\prod_{i=1}^{n} (\lambda_i + \mu_i) - \prod_{i=1}^{n} \mu_i}$	$\lambda = \sum_{i=1}^{n} \mu_i \cdot \frac{\prod_{i=1}^{n} \lambda_i}{\prod_{i=1}^{n} (\lambda_i + \mu_i) - \prod_{i=1}^{n} \lambda_i}$
$P_F = \frac{\lambda}{\lambda + \mu} = 1 - \prod_{i=1}^{n} \frac{\mu_i}{\lambda_i + \mu_i}$	$P_F = \frac{\lambda}{\lambda + \mu} = \prod_{i=1}^{n} \frac{\lambda_i}{\lambda_i + \mu_i}$
First variant of AND-gate	**Second variant of AND-gate**
$\mu = \mu_1$	$P_F = \frac{\lambda_1}{\lambda_1 + \mu_1} \cdot \frac{\lambda_2 + q_2(\mu_1 + \mu_2)}{\lambda_2 + \mu_1 + \mu_2}$
$P_F = \frac{\lambda_1}{\lambda_1 + \mu_1} \cdot \prod_{i=2}^{n} \frac{\lambda_i + q_i \mu_1}{\lambda_i + \mu_1}$	$\lambda = \frac{\mu_1 \lambda_1 q_2 (\lambda_2 + \mu_1 + \mu_2) + \lambda_1 \lambda_2 (1 - q_2)(\mu_1 + \mu_2)}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_1 + \mu_2)(1 - P_F)}$
$\lambda = \frac{P_F}{1 - P_F} \cdot \mu$	$\mu = \frac{\mu_1 \lambda_1 q_2 (\lambda_2 + \mu_1 + \mu_2) + \lambda_1 \lambda_2 (1 - q_2)(\mu_1 + \mu_2)}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_1 + \mu_2) P_F}$

Generic fault tree structure

It is not possible to provide one fault tree model that can be applied to all systems since they all look slightly different and are exposed to different risks. However, a generic fault tree structure is presented in Figure 5.4, which is in line with the conceptual model in Figure 5.3. The system is divided into its three main subsystems: raw water, treatment and distribution. Note that both quantity and quality failure are included in the same fault tree to provide one model that gives

an overview of the entire system. However, the results are presented separately for the two failure types, i.e. two different top events are used. Although the final fault tree model for a system must be more detailed than the example in Figure 5.4 the figure shows a basic structure.

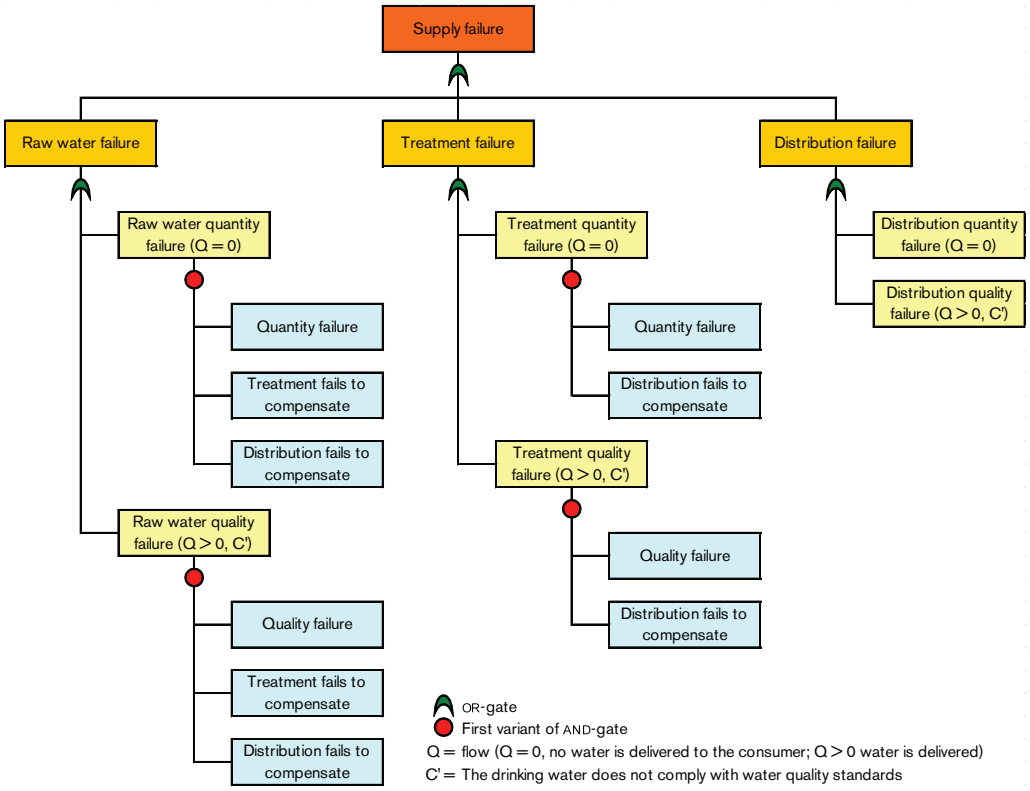


Figure 5.4 *Generic fault tree structure illustrating quantity and quality failure in the three main subsystems.*

Risk

The risk should be calculated and expressed using a unit that reflects properly the unwanted effects. Slovic (2001) also emphasises that the choice of risk measure can affect how risky a particular form of technology appears. In the fault tree method the risk related to both quantity and quality failure is determined by how often failure occurs (failure rate λ), the duration of failure (downtime $1/\mu$) and the number of people affected. The risk is expressed as the expected value of Customer Minutes Lost (CML), which corresponds to the number of minutes per year the average consumer is: (1) not supplied with water (quantity-related risk); and (2) supplied with water that does not comply with water quality standards

(quality-related risk). Whilst the same unit is used for both risk types they must be presented separately to retain transparency. The risk may be calculated approximately by multiplying the failure rate (λ) by the downtime ($1/\mu$) and the proportion of consumers affected (C). However, to take into account that the system cannot fail when already in failure mode the risk (R) should be calculated as

$$R = P_F C \tag{5.1}$$

where P_F is the probability of failure and C the proportion of consumers affected (Paper I). The proportion of consumers affected is used since the risk is expressed for the average consumer. The dynamic fault tree calculations provide information on the probability of failure but not the proportion of consumers affected. Hence, the proportion of consumers affected must be defined for the main failure events in the fault tree. It cannot be defined for the top event since it may include failures that affect a very different number of people. The total risk is thus calculated as

$$R = \sum_i P_{Fi} C_i \tag{5.2}$$

To be able to calculate the risk in this way there can only be OR-gates between the top event and the level where C_i is defined.

The use of CML within the drinking water sector is discussed by, for example, Blokker *et al.* (2005). It should be noted that the quality-related CML does not include any information about the possible health effects and not all drinking water is used as plain drinking water or for cooking. This is further discussed in Section 6.3.

Input data and uncertainties

The dynamic fault tree calculations are combined with Monte Carlo simulations (Section 3.5) to enable uncertainty analysis. The probabilistic approach makes it possible to: (1) analyse the uncertainties in each variable; (2) calculate rank correlation coefficients, providing information on how much the uncertainty of each variable in the fault tree contributes to the uncertainty in the results; and (3) calculate the probability of the risk exceeding specified criteria, i.e. acceptable risk levels.

All input variables in the fault tree model are thus replaced by probability distributions. Variables λ and μ are modelled as exponential rates using Gamma distributions and the proportion of consumers affected (C) as well as the probability of failure on demand (q) are modelled using Beta distributions (Papers I and II). The distributions can be defined based on measurements and event statistics, i.e. hard data, or by using expert judgements. The Gamma distribution has one shape parameter (r) and one scale parameter (σ). Hard data used to define the Gamma distribution for variables λ can be presented as the total number of registered events (r-1) and the specific time period ($1/\sigma$). For μ the data can be presented as the total number of registered events (r-1) and the total duration of failures ($1/\sigma$).

Expert knowledge is often an important source of information in risk assessments since the amount of hard data is often scarce (Paté-Cornell, 1996). The elicitation of expert judgments is facilitated in the fault tree method since the events are seen as Markov processes defined using failure rates and mean downtimes. This means that no direct estimates of the probability of failure are required which was considered an advantage in the method application in Gothenburg. Events and the function of components are described more easily using rates or times and existing data is often available in this format. Possible experts are water utility personnel or other persons with knowledge of the specific event studied. The expert can be asked to estimate a probable highest and lowest value of the failure rate (λ), the downtime ($1/\mu$) and other variables. This information can be used as, for example, as 5- and 95-percentiles to define a probability distribution. What percentiles the values are assumed to correspond to should be based on the expected accuracy in the judgements. It is possible in a fault tree application to use different percentiles for different judgements.

The probability distribution types used in the method (Gamma and Beta) facilitate Bayesian updating. This means, for example, that a distribution defined based on expert judgements can be updated when hard data from measurements or other observations becomes available. The Gamma and Beta distribution families are conjugate, which means that the initial (prior) distribution and the updated (posterior) distribution are of the same distribution class (Gamma or Beta). The use of conjugate distributions therefore simplifies Bayesian updating since the new data can be used to update directly the parameters defining the prior distribution. For example, if a number of pump failures are observed during a specific time period this information can be used to define a new shape parameter (r) and a new scale parameter (σ) for the Gamma distribution representing the pump's failure rate (λ). The Bayesian approach thus provides a

structured way of updating probability distributions and consequently also the results of a fault tree model when new information becomes available.

Case study site

The fault tree method was used to analyse the drinking water system in Gothenburg, Sweden (Paper I). The Gothenburg system supplies approximately 500,000 people with drinking water and includes several forms of interaction between events and subsystems. The system is based solely on surface water and the main water source is the Göta Älv river. An overview of the raw water supply in Gothenburg is presented in Figure 5.5. Two water treatment plants are included in the system and treatment plant number 1 is under normal conditions supplied with water from the river. Water from the river is also pumped via a 12 km rock tunnel to two interconnected lakes (main reservoir lakes), which in turn supply treatment plant number 2 with raw water. Due to variable water quality in the river, the river water intake is closed regularly for about 100 days per year (e.g. Åström *et al.*, 2007). During these periods the reservoir lakes supply both treatment plants with raw water (Figure 5.5). When the intake needs to be closed for longer periods an additional water source (additional reservoir lakes) can also be used to supply the main reservoir lakes, or treatment plant number 2 directly, with water.

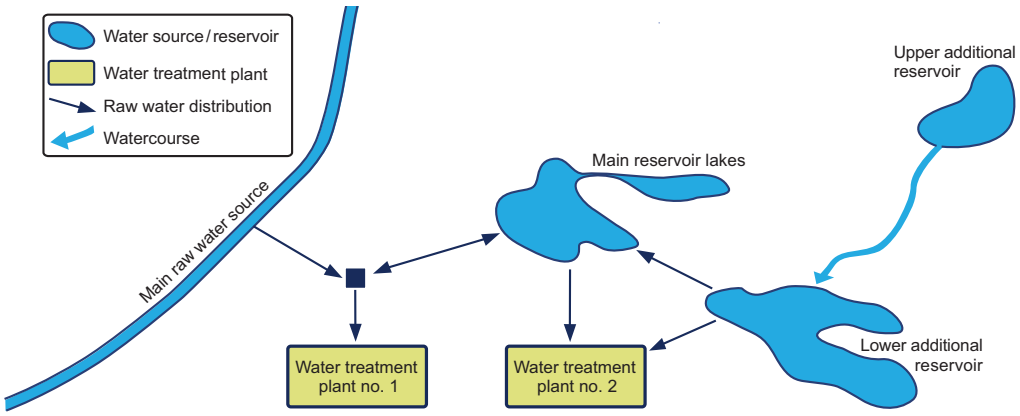


Figure 5.5 *Schematic description of the raw water system in Gothenburg.*

Both treatment plants include similar treatment processes and contribute in approximately equal parts to meeting an average water demand of 165,000 m^3/d (normally demand varies between 120,000 and 210,000 m^3/d). To handle variations in the water demand and production capacity, service reservoirs in the distribution system and at the treatment plants are used. In addition, the

distribution system is divided into different pressure zones and booster stations are used to ensure sufficient pressure in elevated zones.

The water quality is monitored online and by means of regular additional measurements throughout the system. The decision to close the river water intake is based on the online monitoring and reports from operating bodies upstream, such as companies and municipalities.

Fault tree model

The risk assessment of the Gothenburg system included both quantity and quality failures and the drinking water quality was considered unacceptable when *unfit for human consumption*, a criterion defined by the Swedish quality standards for drinking water (SLVFS 2001:30). The task of identifying undesired events, structuring the fault tree and evaluating and updating the fault tree structure was carried out jointly by researchers and water utility personnel. The model building and calculations were performed using Microsoft Excel© and the add-in Software Crystal Ball© was used for running Monte Carlo simulations.

The fault tree model of the Gothenburg system was based on the generic structure presented in Figure 5.4 and in total it included 116 basic events and 101 logic gates. An OR-gate was used to model that failures may occur in any of the three main subsystems (raw water, treatment and distribution). The first variant of the AND-gate was used to model that failure in one subsystem may be compensated for in the subsequent subsystems. The raw water part of the model included the water sources, the raw water supply system (i.e. pumps, siphons, pipes, tunnels etc.) and all components up to the points where the raw water enters the two treatment plants. Everything between the points where the raw water enters the treatment plants, throughout the plants and up to the points just before the treated water is pumped out into the distribution network, was included in the treatment part of the fault tree. The distribution system included all components (pumps, pipes, service reservoirs etc.) from the point where the treated water is pumped out from the treatment plants to the consumers' taps.

An OR-gate was used to separate failures in each of the three main subsystems into quantity and quality failures. In doing so it was possible to calculate the results for quantity and quality failures separately and thus retain transparency.

It is not only possible for one subsystem to compensate for failure in other parts of the system; interactions between parts within the same subsystem also provide

opportunities for compensation. Both variants of the AND-gate were used to model different kinds of compensation within the three subsystems. The first variant of the AND-gate was used to model situations where the ability to compensate was limited in time, for example due to limited reservoir volume. The second variant was used to model the ability of the treatment to compensate for unacceptable raw water quality, see Table 5.1.

To make it possible to calculate risk levels expressed as CML, a suitable level in the fault tree for defining the proportions of people affected needed to be identified. In the Gothenburg fault tree, quantity failure as well as quality failure under each of the three main subsystems were divided into main failure events and the proportion of people affected was defined for these events. Quantity failures in the raw water system, for example, were divided into two events illustrating which of the two treatment plants that may not be supplied with raw water. Quality failures in the distribution system were divided into events such as quality deterioration and contaminant intrusion. These events were also divided into major and minor events in order to avoid mixing events with considerably different consequences.

Hard data as well as expert judgments were used as input data for the fault tree model. The expert judgments were used as estimates of the 5- and 95-percentiles when defining probability distributions describing the uncertainties of the input data.

Case study results

In addition to the quantitative results of the fault tree analysis the actual fault tree model and the process of constructing it are also important results. The structure of the fault tree model illustrates how the system functions and it shows the interactions between subsystems and events. Furthermore, when constructing a fault tree model aspects of a system that may otherwise be ignored are discussed.

The Monte Carlo simulations were performed using 10,000 iterations and the risk levels, failure probabilities, failure rates and downtime were calculated at all levels in the fault tree. In Figures 5.6 and 5.7 the expected CML per year (risk), probability of failure, failure rate and mean downtime are shown for quantity and quality failure respectively. For each failure type the results are presented for the entire system as well as for the raw water, treatment and distribution parts

separately. Since uncertainties are considered in the analysis the mean, 5- and 95-percentiles are presented for all variables.

By studying the risk levels it can be concluded that for both quantity and quality failure the raw water system contributes most to the total risk level (Figures 5.6 and 5.7). However, when comparing the probabilities of failure it is clear that failures in the distribution system are the most probable for both quantity and quality failures. Hence, by studying the CML values together with information on probabilities it can be concluded that the raw water system contributes most to the total risk level due to more severe consequences and not because of a high probability of failure, cf. Equation (5.2). The probability of failure is determined by the failure rate and mean downtime and these two variables provide additional information on the dynamic behaviour of the system.

The failure rates and downtimes show that the high probability of distribution failure (quantity and quality) is due to frequent failures, i.e. a high failure rate, because the downtime is short. It is also shown that the raw water system, in contrast to the distribution system, has a low failure rate but a long downtime. The long downtime in combination with the fact that many consumers are affected when something happens in the first part of the supply chain, explains why the raw water system contributes most to the total risk level. Failure in the treatment may also affect many consumers, but since the failure rate is low and the downtime is short for these events, they only have a minor influence on the total risk. It should be noted that although a quality failure has a low failure rate and short downtime, the consumers affected may be subject to severe health effects.

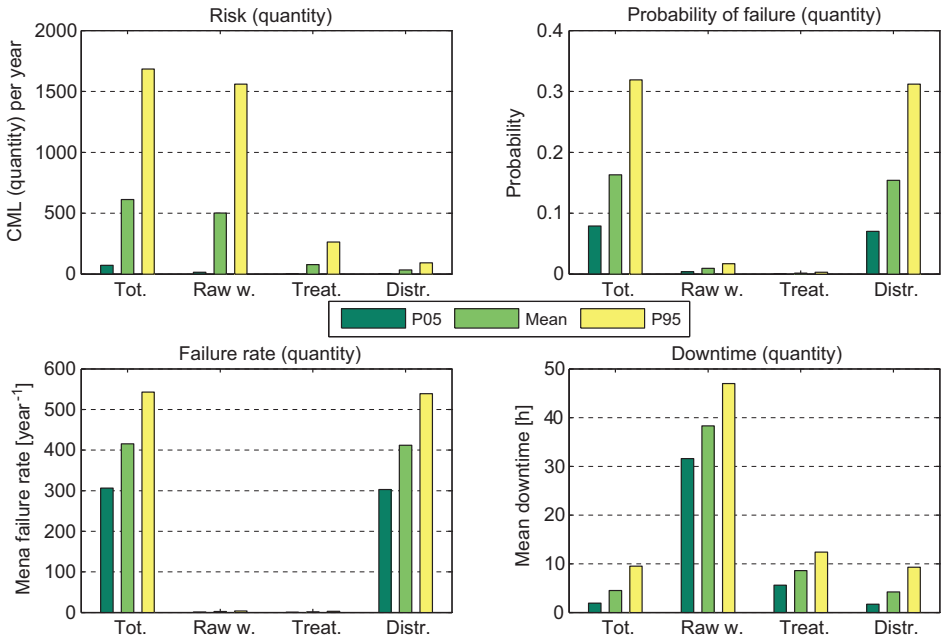


Figure 5.6 *Histograms showing the risk (expected value of CML), probability of failure, failure rate and mean downtime for quantity failure. The mean, 5- and 95-percentiles are presented for the entire system (Tot.) as well as the three main sub-systems.*

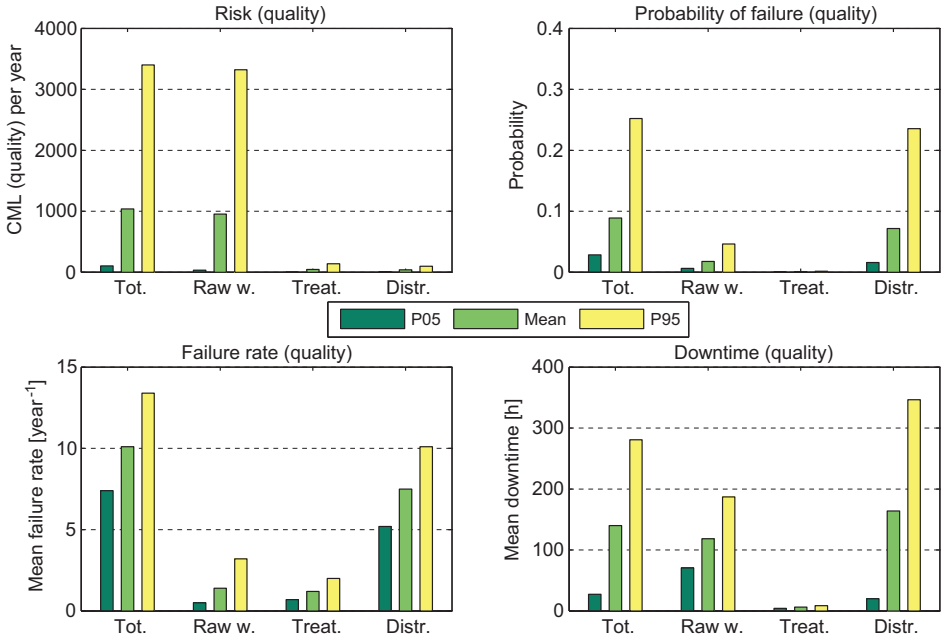


Figure 5.7 *Histograms showing the risk (expected value of CML), probability of failure, failure rate and mean downtime for quality failure. The mean, 5- and 95-percentiles are presented for the entire system (Tot.) as well as the three main sub-systems.*

The histograms in Figures 5.6 and 5.7 show that the failure rate is higher for quantity failure compared to quality failure although the downtime is shorter for quantity failure. Quantity failures are therefore most common whilst quality failures have a longer duration. The percentiles in Figures 5.6 and 5.7 show that the uncertainties in some of the variables are high. One example is the total risk level related to quantity failure, the uncertainties of which are analysed further below.

To evaluate the results the calculated total risk level related to quantity failure was compared with a politically established safety target that can be regarded as being an acceptable level of risk. The safety target is defined by the City of Gothenburg as: *duration of interruption in delivery to the average consumer shall, irrespective of the reason, be less than a total of 10 days in 100 years* (Göteborg Vatten, 2006). The uncertainty distribution in Figure 5.8 represents the calculated risk level (Figure 5.6) and it is compared with the performance target, translated into 144 CML per year. The probability of exceeding the target value was calculated at 0.84. To be able to say whether the risk is unacceptable or not one needs to decide to what level of certainty the target should be fulfilled. This is further discussed in Section 5.3 where risk-reduction measures are modelled and evaluated.

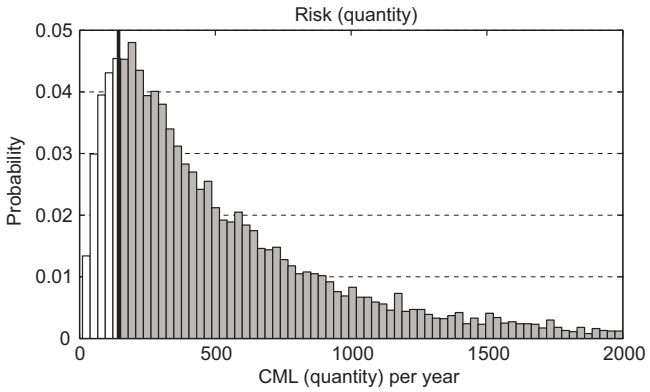


Figure 5.8 *Uncertainty distribution of quantity-related risk, including the entire system, compared with the performance target (144 CML per year) indicated by the solid vertical line. The probability of exceeding the performance target (grey area) is 0.84.*

When the uncertainties are analysed, rank correlation coefficients can be calculated and studied. To illustrate how rank correlation coefficients may be used, Figure 5.9 shows the six variables in the fault tree model contributing most to the uncertainties in the result of *probability of quantity failure in the distribution system*. Note that in Figure 5.9 the repair rate (μ) is presented and not

the mean downtime ($1/\mu$). This is because the repair rate is used as an input variable in the fault tree model. However, since both variables correspond to the same information this does not affect the uncertainty analysis. All failure rates (λ) have a positive rank correlation coefficient since an increase in the failure rate means that failure becomes more frequent and the probability of failure thus increases, cf. Equation (3.5). In the opposite way, all mean repair rates (μ) have a negative rank correlation coefficient since an increase in the repair rate means that the mean downtime ($1/\mu$) decreases and consequently the probability of failure decreases.

The results in Figure 5.9 show that the failure rate and repair rate of *failure of distribution pipe*, *failure of service connection* and *quantity failure in building* are the six variables in the fault tree that contribute most to the uncertainties in the probability of distribution failure. To reduce the uncertainties in this specific probability value most effectively, these six variables should be studied further to acquire more accurate estimations. This kind of information may thus act as a guide in further studies.

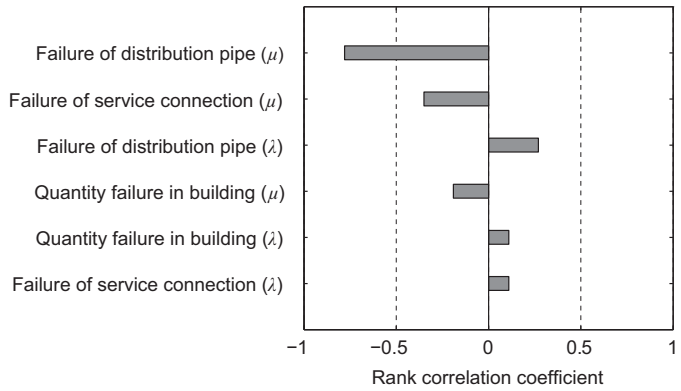


Figure 5.9 *Uncertainty analysis of the probability of quantity failure in the distribution system. The rank correlation coefficients of the six variables contributing most to the uncertainties in the probability of distribution failure are presented.*

The rank correlation coefficients were used to analyse how the input data affects the results for the top events (quantity and quality failure) in the fault tree model of the Gothenburg system. It was concluded that the uncertainties in both the quantity- and quality-related risk levels are mainly caused by uncertainties in the consequences, i.e. proportions of affected consumers. One reason why the consequences have a large impact on the uncertainties is that they are included in the calculations at a high level in the fault tree model. Besides the consequences,

some of the events in the raw water part of the model had relatively high correlation coefficients. For the probability of failure as well as the rates λ and μ, events in the distribution part of the fault tree contributed most to the uncertainties. Compared to the raw water and treatment part of the fault tree model, the distribution part has more basic events at a high level in the structure. This makes the results more sensitive to changes in the variable for these events compared to events at a lower level in the fault tree.

Evaluation of the approximate dynamic fault tree calculations

To evaluate the approximate dynamic fault tree calculations thoroughly, they were compared with complete Markov simulations for three parts of the Gothenburg fault tree model. The evaluation is presented in Paper II and the main results are summarised here.

Two of the analysed fault tree examples in Paper II are presented in Figure 5.10. Example A models how raw water of insufficient quality is supplied to one of the treatment plants and the fault tree includes the traditional OR-gate and the second variant of the AND-gate. The second AND-gate variant is used to consider a situation where although an insufficient raw water quality is used the treatment may be able to provide drinking water that meets the quality standards. The quality deviation in this example refers to measureable parameters, i.e. quality parameters that are analysed routinely by the water utility. Example B includes the traditional OR- and AND-gates but also the first AND-gate variant. This example illustrates how quantity failure may occur due to failure at one of the treatment plants. The first AND-gate variant is used to model the ability to compensate for failure by means of stored water at both treatment plants and in the distribution system and also increased production at the non-affected plant.

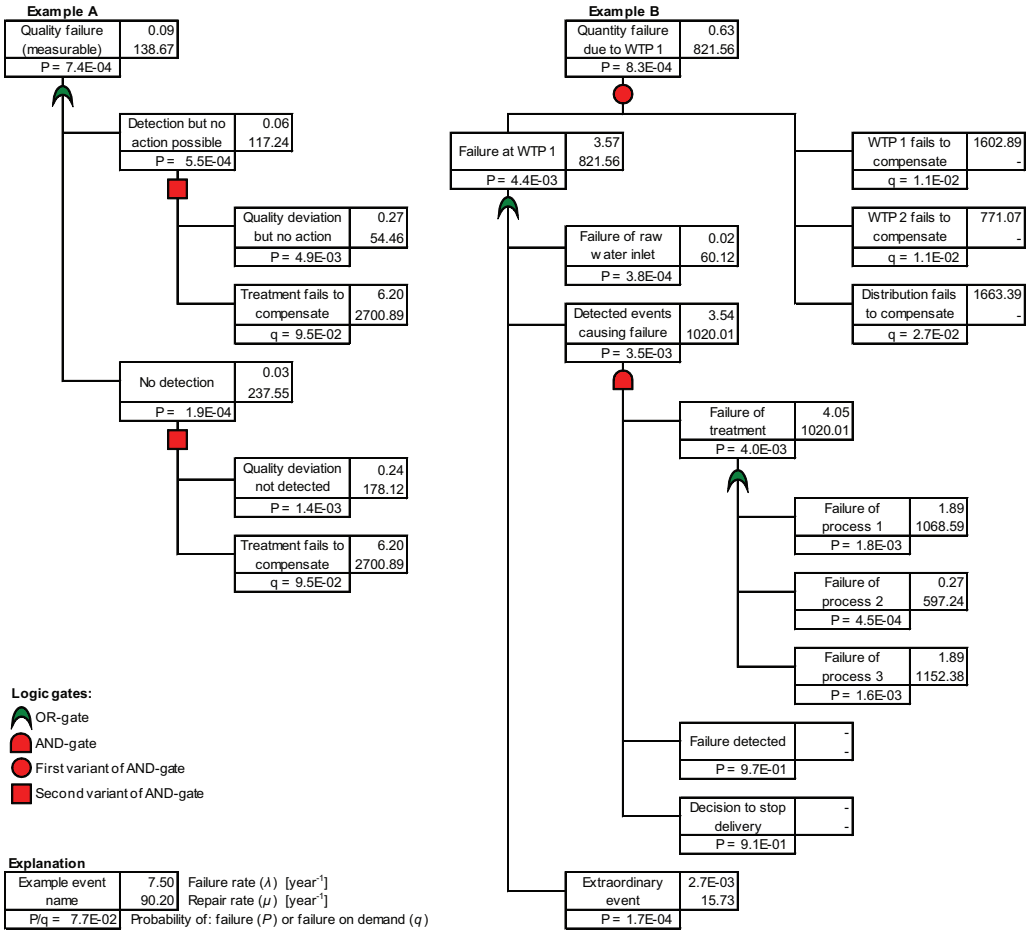


Figure 5.10 *Examples of parts of the fault tree model for the Gothenburg system. The values presented in the fault trees are expected values, for details see Paper II.*

The approximate dynamic fault tree calculations for the two fault tree examples were compared to the results of Markov simulations. Monte Carlo simulations based on 5,000 iterations were performed for the approximate calculations and the Markov simulations were repeated 5,000 times. For each Markov simulation values for the input variables were sampled from the corresponding uncertainty distribution (Paper II). In Figure 5.11 the densities for the approximate dynamic fault tree calculations and the Markov simulations are presented for the results at the top event in example A. Almost no differences can be seen in the densities for the probability of failure (P_F) and the rates λ and μ. In Paper II it is shown that similar results are obtained for fault trees that include only the traditional OR- and AND-gates. Hence, for the traditional logic gates and the second AND-gate variant the errors in the approximate dynamic fault tree calculations are negligible.

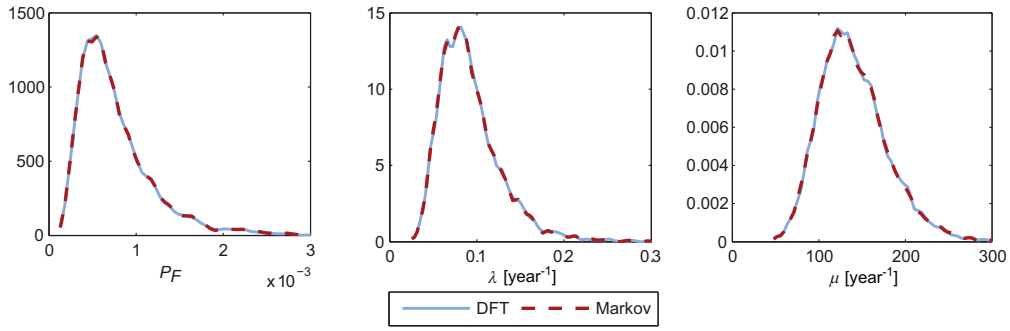


Figure 5.11 *Densities for the results of the approximate dynamic fault tree (DFT) calculations and the Markov simulations for example A. The results are presented for the probability of failure P_F and rates λ and μ.*

Example B includes three compensating events and to see how the number of compensating events affects the results the calculations were performed including one compensating event only, including two of the events and including all events. When one compensating event is included the results of the dynamic fault tree calculations are in good agreement with the Markov simulations (Figure 5.12a-c). The error increases when two, and in particularly three, compensating events are included (Figure 5.12d-f and g-i respectively). However, the uncertainties in the results, caused by uncertainties in input data, should be considered when analysing the errors in the results. Considering the overall uncertainties of the model it was assumed that the errors can be accepted, both for the two small examples presented here but also for the entire model of the Gothenburg system (Paper II). The entire fault tree model includes fifteen second-variant AND-gates and seven first-variant AND-gates. Of the first variant three include one compensating event, two include two compensating events and two include three compensating events. All first-variant AND-gates are placed at a high level in the fault tree. The analysis of rank correlation coefficients showed that the input parameters for these gates are not the ones that contribute most to the uncertainties in the results at the top level.

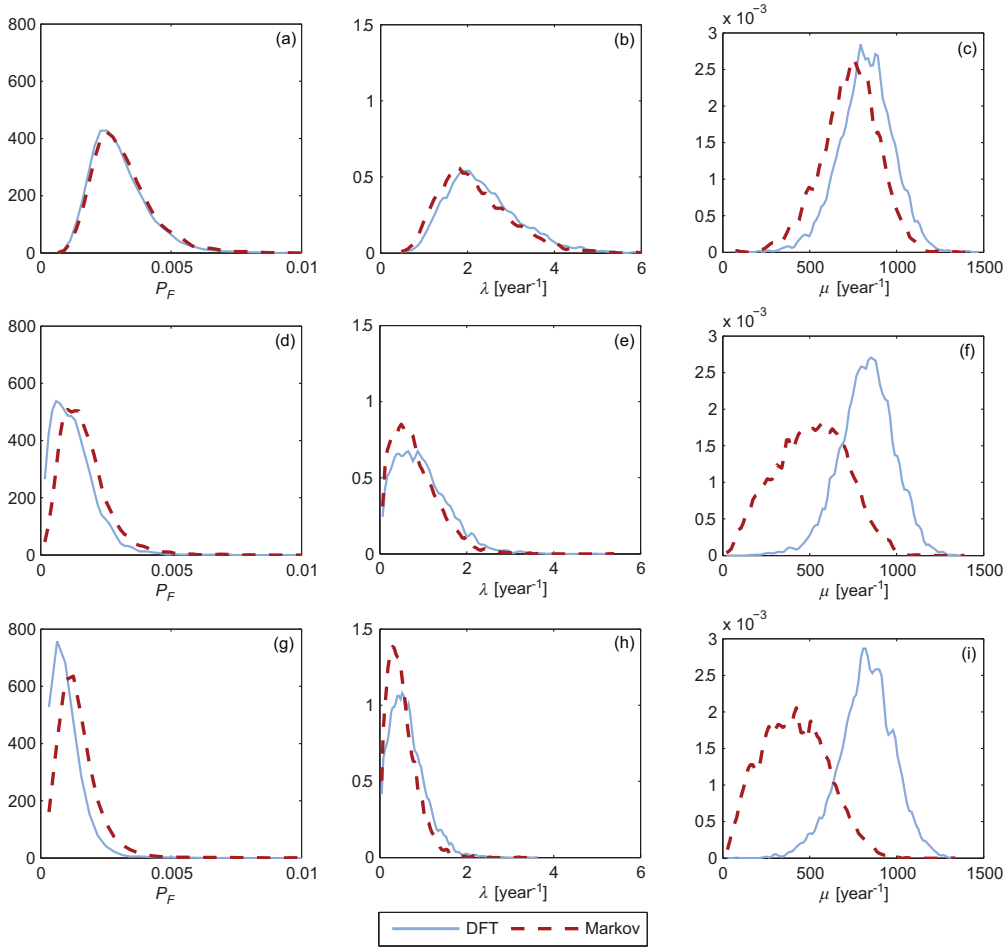


Figure 5.12 *Densities for the results of the approximate dynamic fault tree (DFT) calculations and the Markov simulations for example B. The results are presented for P_F, λ and μ. Figures a-c represent the case when only one compensating event was included in the model, for d-f the model included two compensating events and for g-i all three events were included.*

In Paper II it is shown that the rates λ and μ cannot be assumed to be exponentially distributed at the top event in a fault tree. Consequently, the rates cannot be used to calculate, for example, the probability of failure during a specific time period.

Key aspects when applying the fault tree method

Based on the method development and the case study application, the following key aspects have been identified as being important to consider when using the fault tree method:

- The top events should be defined to fit the specific risk assessment and do not need to be the ones used in the model applications presented here. For example, here an overall type of quality deviation was analysed. It is also possible to use a more narrow definition of quality failure related to, for example, a specific contaminant.
- The identification of undesired events/hazards and the fault tree construction are preferably performed simultaneously. It is an iterative process where events are identified and developed further until a suitable level of detail is obtained. The fault tree model is detailed enough when it describes the system properly and input data for the basic events can be defined.
- To facilitate the fault tree analysis people with expert knowledge of the different subsystems should be involved in the fault tree construction and evaluation work. Good knowledge of the system is of primary importance to provide accurate results.
- When structuring the fault tree model the system should be divided into subsystems that are relevant in order to be able to evaluate how they contribute to the risk. This is is primary importance in order to identify where risk-reduction measures are needed most.
- Use OR- and AND-gates as well as the variants of the AND-gate to describe the system, see examples in Table 5.1. Although errors may occur when several compensating events are included in the first AND-gate variant, all possibilities of compensation should be included in the model. However, rank correlation coefficients should be calculated and analysed to see to what extent the compensating events contribute to the uncertainties in the results.
- When available, hard data can be used to define the input variables for the basic events. However, since hard data is often missing, expert judgements may be needed. The experts are preferably asked to estimate probable highest and lowest values of the input variables, which are translated into percentiles of relevant uncertainty distributions.
- When new hard data becomes available the input data can be updated using a Bayesian approach. The Gamma and Beta distributions used in the fault tree model make the Bayesian updating easy and straightforward. For example, data from monitoring activities can be used to update information about events.
- The proportion of consumers affected should be defined at a high level in the fault tree that only has OR-gates up to the top event.

- A fault tree model can be used to qualitatively analyse and evaluate a system based on the structure of the fault tree. The model illustrates how events and components are interconnected and by studying the model aspects that would otherwise have been ignored are highlighted.
- Analyse risk levels together with information about the failure probabilities as well as failure rates and downtimes to also see the dynamic function of the system. Furthermore, compare the different subsystems to see which part contributes most to the risk, where failures occur most frequently, what part is associated with failures with a long duration etc.
- Analyse uncertainties by, for example, calculating the probability of exceeding acceptable risk levels and other performance targets. Also calculate rank correlation coefficients to see which basic events contribute most to the uncertainty in the results.

5.3 Quantitative risk assessment and economic analysis

It has been shown how the dynamic fault tree method can be used to estimate risk levels and analyse the dynamic function of drinking water systems (Section 5.2 and Papers I and II). The possibility to also model risk-reduction measures and combine the results with economic analysis to provide decision support is presented here and in Papers III and IV.

Modelling risk reduction

The implementation of risk-reduction measures may affect a drinking water system and the risk in different ways (Section 2.5). Based on how the measure is expected to affect the system, an existing fault tree model can be updated and used to quantify risk reduction and other effects. A fault tree model can be updated with respect to: (1) fault tree structure, i.e. events and logic gates can be added and/or removed; (2) input data, i.e. new input data can be used representing the situation as if the measure has been implemented. Hence, a fault tree model can be updated to consider which events must occur to cause failure (including new possibilities to compensate for failure etc.), the probability of the events occurring (failure rate and downtime) and the consequences they may cause.

The effects of risk-reduction measures can be quantified in terms of reduced risk levels as well as changes in the probability of failure, failure rate and downtime.

The probability of the risk exceeding a tolerable level can also be used when evaluating and comparing alternative measures.

Economic analysis of risk-reduction measures

By combining the fault tree results with economic analysis additional information about the analysed risk-reduction measures is provided. In Section 3.3 the basics of cost-effectiveness analysis (CEA) and cost-benefit analysis (CBA) is described. Basically, a CEA aims to identify which alternative meets a predefined criterion, such as an acceptable risk level, at the lowest cost. In a CBA both the benefits, including the effects in terms of risk reduction, and the costs are expressed in monetary units to investigate whether or not the benefits exceed the costs. In this thesis it is shown how to combine the fault tree results with CEA but also how a CBA approach can be used to further analyse risk-reduction measures.

As a basis for CEA the effect (E_j) of risk-reduction measure j is calculated as

$$E_j = R_0 - R_j \tag{5.3}$$

where R_0 is the initial risk level before any measure is implemented and R_j is the residual risk after measure j has been implemented. The costs of the measure should be calculated with consideration given to cost for planning and constructing as well as maintenance costs. Since the costs (C_{jt}) of measure j occur over several years (t) a time horizon (T) and a discount rate (r) need to be decided so that the present value (C_j) can be calculated, see Equation (3.6).

In CEA the effects are also discounted if they vary over time. However, using the fault tree method the effect of risk-reduction measures is considered to be constant over time and thus no discounting is needed to enable a comparison of different alternatives. Discounting effects in CEA are discussed by e.g. Ramsey *et al.* (2005) and Brouwer and Koopmanschap (2000). As shown in Section 5.2 above, a critical risk level can be used to determine whether or not the effect of a risk-reduction measure is sufficient. Since the fault tree method takes uncertainties of estimates into account, it is possible to also define a criterion representing the highest tolerable probability of not achieving the acceptable risk level. Furthermore, a cost-effectiveness ratio (CER) can be calculated for each measure, which in this application represents the cost required to obtain a reduction of one CML, see Equation (3.7). Based on information about final risk

levels, costs and *CER* it is possible to evaluate and compare risk-reduction measure.

In a CBA the net benefit (Φ_j) of an alternative (j) is calculated as

$$\Phi_j = \sum_{t=1}^{T} \frac{1}{(1+r)^{t-1}} \left(B_{jt} - C_{jt} \right) \tag{5.4}$$

where B_{jt} and C_{jt} are the streams of benefits and costs over time, T is the time horizon and r is the discount rate. The only benefit considered using the fault tree method is the effect on risk levels (E_j) and the benefit can be calculated as

$$B_{jt} = E_j cn = (R_0 - R_j) cn \tag{5.5}$$

where R_0 and R_j represent the same parameters as in Equation (5.3), c is the economic value of 1 minute of additional water supply per year and consumer and n is the total number of consumers. The approach presented here can be used to analyse both quantity and quality failure although the application is focused on analysing measures reducing the quantity-related risk. Hence, c represents the cost an average consumer is willing to pay per year to reduce the time of interruption by 1 minute (CML) per year. If c is not known the objective function Φ_j can be calculated as a function of c, which makes it possible to see how the economic valuation of the risk reduction affects the prioritisation of alternatives. The latter approach is used in this thesis.

Case study

As concluded in Section 5.2 and Paper I the quantity-related risk, i.e. risk related to supply interruptions, to the Gothenburg drinking water system is well above the safety target of 144 CML per year. Possible risk-reduction measures have been identified by the City of Gothenburg and the fault tree method in combination with economic analysis has been used to evaluate and compare the alternatives. Note that this method application is focused on the effect of risk-reduction measures' on the quantity-related risk.

In Paper III it is shown how the existing fault tree model can be used to estimate the effect of risk-reduction measures for the Gothenburg system. In Paper IV the measures are analysed further and the results are combined with an economic analysis. The three basic risk-reduction measures are: (1) increased treatment capacity in the two treatment plants; (2) supply of raw water from small lakes;

and (3) supply of raw water from large lake. By increasing the treatment capacity at the two treatment plants, each plant will be able to produce up to the average water demand. Hence, the treatment plants will acquire an improved ability to compensate for failures, such as interruptions in the raw water supply to the other plant or failures at the other plant affecting the treatment capacity. A schematic illustration of the raw water supply and possible new water sources is presented in Figure 5.13. The purpose of including the small lakes in the system is to regulate them to increase the flow in a small river for transport to the drinking water system. Although the small lakes contain a relatively large amount of water the watershed is too small for a continuous supply. For the large lake the solution of building a pipeline for raw water transfer is analysed. Although the large lake has almost no restrictions in water availability failures may occur due to dry periods, causing a water shortage, problems in the raw water transfer or contamination events.

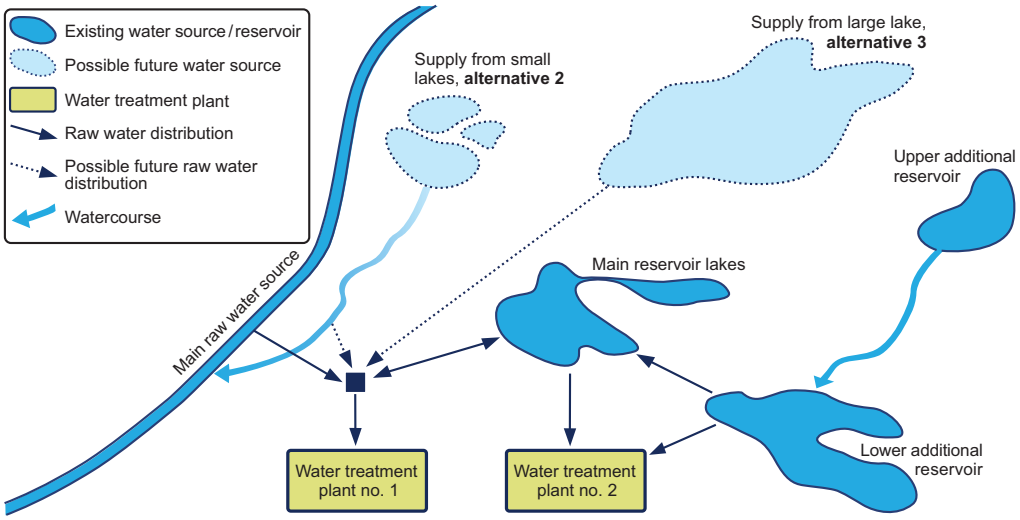


Figure 5.13 *Schematic illustration of the Gothenburg drinking water system and possible new water sources.*

The three main risk-reduction measures are also combined in different ways so that in total seven alternatives are analysed. All alternatives are presented in Table 5.3, including main characteristics used to update the fault tree model.

Table 5.3 Main characteristics of the seven alternatives used to model the risk-reduction measures.

ALTERNATIVE	CHARACTERISTICS
0. Current system	–
1. Increased treatment capacity	Based on statistical data on water demand and estimations regarding the reliability of the treatment plants, the time for compensation (time to failure $1/\lambda$) was estimated to be 3–120 days (90% interval) and the probability of failure on demand 0.0025–0.01 (90% interval). The number of consumers affected was estimated to be 6,500–33,900 for events where one of the treatment plants cannot supply any water.
2. Supply from small lakes	If available and if only treatment plant number 1 needs supply, the source is available (time to failure) 25–35 days (90% interval), whereas if both treatment plants need to be supplied the available time is restricted to 8–18 days (90 %-interval). When the lakes are unavailable, the duration (downtime) is 7–60 days (90% interval).
3. Supply from a large lake	The time to failure is 5–15 years (90% interval) for the three events: water shortage, failures in the transfer of raw water and unacceptable water quality in the lake. When failure occurs the duration (downtime) is estimated to be 1–30 days for water shortage, 0.5–2 days for transfer failures, and 5–30 days for water quality failures (all 90% interval).
4. Combination of alt. 1 and 2	See alternatives 1 and 2.
5. Combination of alt. 1 and 3	See alternatives 1 and 3.
6. Combination of alt. 2 and 3	See alternatives 2 and 3.
7. Combination of alt. 1, 2 and 3	See alternatives 1, 2 and 3.

The risk for the current system and the residual risk levels after the measures have been implemented are presented in Figure 5.14. All alternatives have a significant effect on the risk level but some are more effective than others. The safety target of 144 CML is included in Figure 5.14 and it can be seen that although the mean value is below the target value there may be a non-negligible probability of exceeding the safety target. In Figure 5.15 the probability of exceeding the safety target is presented for all alternatives.

As shown in Section 5.2, failures in the raw water system contribute most to the quantity-related risk for the Gothenburg system. The results presented in Figures 5.14 and 5.15 show that of alternatives 1-3, increased treatment capacity (alt. 1) has the largest effect on the risk. The figures also show that if the treatment capacity is increased the implementation of additional water sources (alt. 3, 4 and 7) does not reduce the risk as significantly as if they are implemented without

increasing the capacity (alt. 2, 3 and 7). In Figure 5.16 the risk is presented for the entire system and its three main subsystems for alternative 1, increased treatment capacity alone, and alternative 7, increased treatment capacity in combination with both the new water sources. The results show that after alternative 1 has been implemented the raw water part and the distribution part contribute almost equally to the total risk. Before any measures, failures in the raw water system were the main cause of the high risk level (cf. Figure 5.6). Consequently, if the treatment capacity is increased, risk-reduction measures within the distribution system are also needed to effectively reduce the risk further. In Figure 5.16 it is also shown that if increased treatment capacity is combined with both the possible water sources (alt. 1) the risk related to the raw water part is further reduced and the distribution part is the main contributor to the overall risk level.

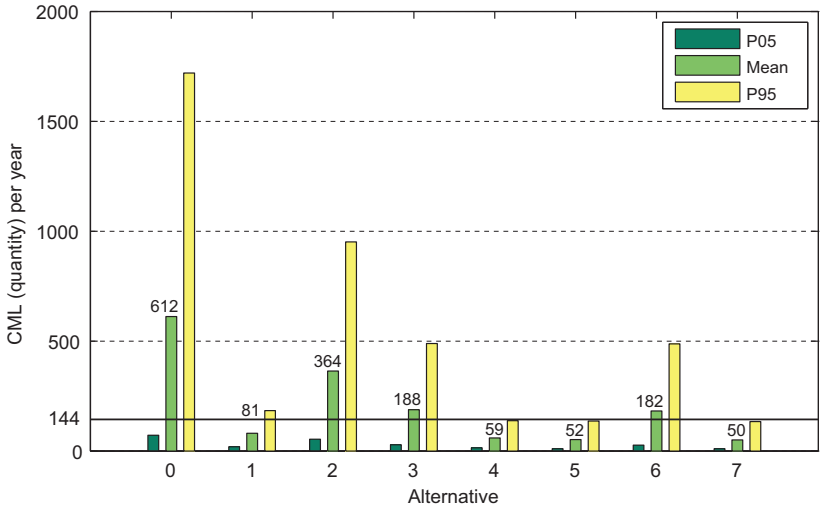


Figure 5.14 *Histograms showing the mean, 5 and 95-percentiles of the risk levels prior to any measure (0) and for the seven alternatives (1-7). The mean values are given at the mean level bars. The solid horizontal line represents the safety target (144 CML).*

Increased treatment capacity seems to be an effective way of reducing the risk related to the raw water supply. Consequently, the risk-reduction measure does not need to be implemented in the subsystem from which failures originates. Aspects such as these are possible to consider in integrated risk assessments. Furthermore, it is the ability to compensate for failure that is increased by alternative 1 and this is modelled using the variants of the AND-gate. Note, however, that these results are case-specific and that risk-reduction measures within the raw water supply system may be more effective in other cases.

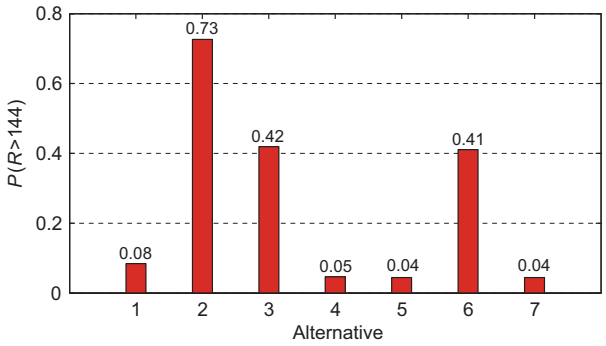


Figure 5.15 *Probabilities of exceeding the safety target (144 CML) for the current system (0) and the seven alternatives (1-7).*

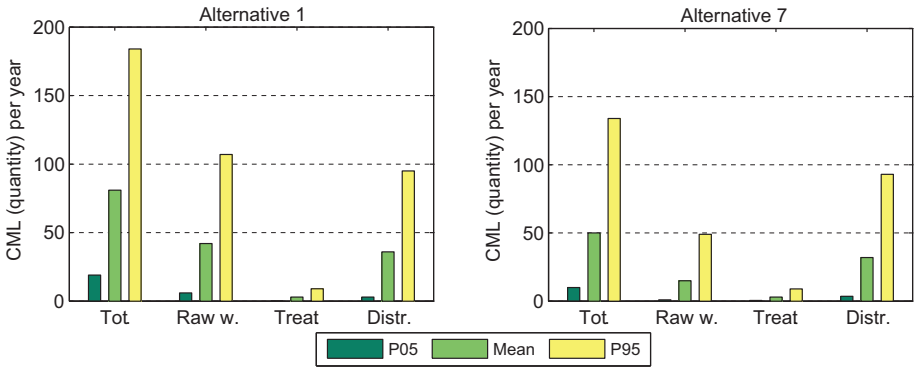


Figure 5.16 *Quantity-related risk levels after the treatment capacity has been increased (alternative 1) and after the treatment capacity has been increased in combination with the two possible water sources (alternative 7). The mean, 5- and 95-percentiles are presented for the entire system (Tot.) and the three main subsystems.*

To analyse the cost-effectiveness of the alternatives the costs they are related to were identified and calculated based on a 100-year time horizon and with a discount rate of 3%. An uncertainty analysis was performed and it was concluded that although discount rates from 1 to 5% were used it did not affect the prioritisation of the alternatives. Using information on the cost and the effect in terms of reduced risk level, the *CER* was calculated for each alternative. The results for the analysed alternatives are summarised in Table 5.4 including the mean risk level, the probability of exceeding the safety target of 144 CML, the cost and the *CER* for each alternative. Two example criteria (0.10 and 0.05) for the probability of exceeding the safety target are included to show how it may affect the final prioritisation. These criteria represent a highest acceptable probability of not meeting the safety target. Note that the definition of such criteria must be made by the decision-maker.

From the results presented in Table 5.4 it can be seen that alternatives 2, 3 and 6 do not meet any of the criteria. Alternative 1 may be accepted if 0.10 is used as a criterion for the probability of not meeting the safety target. Alternatives 4, 5 and 7 meet all criteria. If the certainty criterion of 0.05 is used, alternative 4 is most cost-effective since it reduces the risk to an acceptable level at the lowest cost. Alternative 1 is associated with a slightly lower cost compared to alternative 4 and is most cost-effective if the certainty criterion of 0.10 is used.

The *CER* values show that the cost per reduced unit of risk is lowest for alternative 2. However, this alternative does not meet any of the criteria and can thus not be accepted. Hence, the *CER* values should be analysed in combination with the other results to avoid a too small risk reduction (alt. 2) as well as an unnecessarily large risk reduction. It may be argued that there is no reason for reducing the risk below the acceptable level. The resources can be used for other investments instead. This is further discussed in Paper IV.

Table 5.4 *Summary of risk levels (R_j), probabilities of not meeting the safety target $P(R_j > R_c)$, costs (C_j) and cost-effectiveness ratios (CER_j) for the alternatives. The safety target value is 144 CML. For the probability of not meeting the safety target two example criteria are used (0.10 and 0.05). Figures in bold indicate that the criterion is not met.*

CRITERION	144	0.10	0.05		
ALTERNATIVE	R_j [CML]	$P(R_j>R_c)$	$P(R_j>R_c)$	C_j [MSEK]	CER_j [MSEK/CML]
1. Increased capacity	81	0.08	**0.08**	280	0.53
2. Supply from small lakes	**364**	**0.73**	**0.73**	9	0.04
3. Supply from a large lake	**188**	**0.42**	**0.42**	372	0.87
4. Combination of alt. 1 and 2	59	0.05	0.05	289	0.52
5. Combination of alt. 1 and 3	52	0.04	0.04	652	1.16
6. Combination of alt. 2 and 3	**182**	**0.41**	**0.41**	381	0.88
7. Combination of alt. 1, 2 and 3	50	0.04	0.04	661	1.17

As concluded in, for example, Section 5.1 there are aspects of decision problems that often cannot be included in a risk assessment but which should be considered when using the results to support decisions. For the alternatives analysed here only the effect on the quantity-related risk were studied. If the large lake is included in the system it will most likely also provide raw water of better and more stable quality compared to the current main raw water source. Cost-benefit calculations were performed to illustrate how the economic value of risk

reduction and additional benefits may affect the prioritisation of alternatives. In Figure 5.17 the net benefit is presented for the seven alternatives as a function of the economic value of 1 minute of additional water supply per year and consumer (c), see Equations (5.4) and (5.5). The intersection points in Figure 5.17 clearly show that the value of c affects the relationship between the alternatives. Furthermore, if c is SEK 0.07 or higher all alternatives have a positive net benefit and if it is less than SEK 0.03 only alternative 2 is beneficial.

Increased treatment capacity in combination with supply from the large lake (alt. 5) is associated with a high cost. However, as mentioned above it is expected that the large lake will provide increased raw water quality, which may result in a reduced health risk. If the additional benefits are added to alternative 5 it will also result in a positive net benefit if the value of c is lower than 0.07. The results in Figure 5.17 provide a basis for discussing benefits that may have been overlooked and how they may affect the prioritisation.

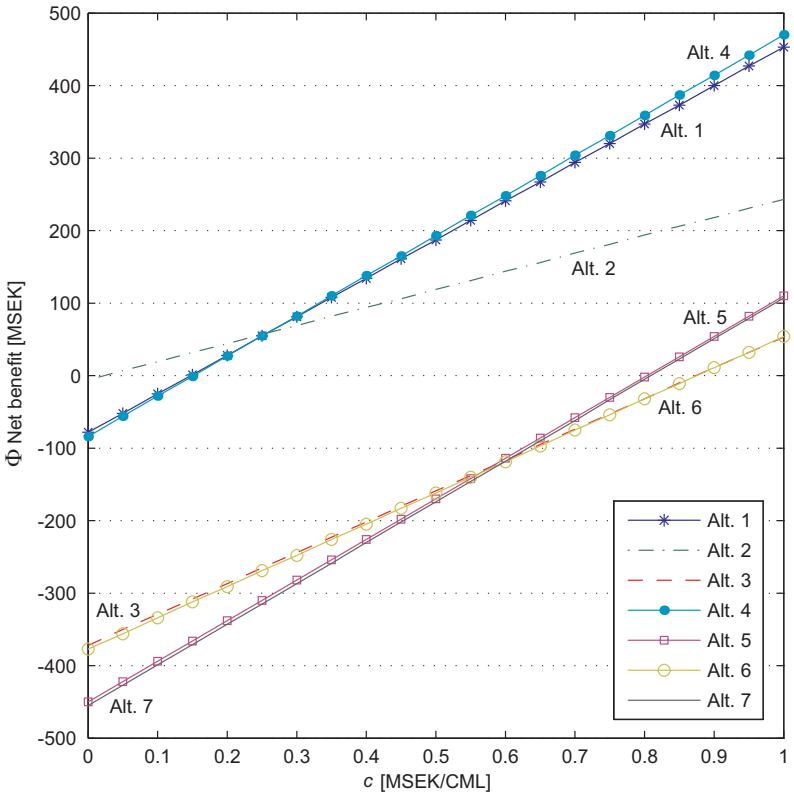


Figure 5.17 *Net benefit of the seven alternatives as a function of the economic value of 1 minute of additional water supply per year per consumer (c).*

The results presented above show how well the seven alternatives perform in relation to different criteria and advantages and limitations are illustrated. The final decision on which alternative to select must to be made done by the decision-makers.

Key aspects when modelling and evaluating risk reduction

In addition to the key aspects presented in Section 5.2 the following aspects must be identified as important to consider when modelling and evaluating risk-reduction measures using the dynamic fault tree model and CEA:

- Describe how the possible risk-reduction measures are expected to affect the system. Translate this information into changes in the fault tree model and the input data.
- When analysing the effect of risk-reduction measures, the uncertainty in risk levels should be considered by analysing the probability of not meeting predefined safety targets. Decide what is the highest acceptable probability of not meeting a predefined safety target.
- Analyse the residual risk after the measures have been implemented and see how the different subsystems are affected. Information on failure rates and downtimes can also be used to further analyse the effect on the system.
- Include costs for planning and construction as well as maintenance when estimating the cost of risk-reduction measures. Perform uncertainty analysis to see how the selection of the discount rate affects the final prioritisation of the alternatives.
- The alternative that meets the defined criteria at the lowest cost is the most cost-effective alternative.
- Use the *CER* values to show the cost of reducing the risk by one unit but do not use it as a single criterion for evaluating risk-reduction measures.
- If possible, perform cost-benefit calculations to further analyse the risk-reduction measures and to illustrate how the economic value of risk reduction may affect the prioritisation. Consider possible additional benefits as well as drawbacks that are not included in the risk assessment but which could affect the performance of the alternatives.

5.4 Multi-criteria decision models

The dynamic fault tree method provides a quantitative tool for assessing risks, modelling risk-reduction measures and providing decision support. However, integrated risk assessments of drinking water systems are commonly performed using risk ranking (Section 3.1). Risk ranking is used to prioritise risks and this type of assessment is also suggested as part of WSPs (Section 2.4). However, a structured way of using risk ranking in order to also prioritise risk-reduction measures is currently lacking. Therefore, two decision models based on multi-criteria decision analysis (MCDA) were developed to enable the use of risk ranking results to evaluate and compare risk-reduction measures. The MCDA models and the applications are presented in detail in Paper V and a summary of the main aspects of the models is presented here.

General approach

Risk-reduction measures implemented in drinking water systems may have different effects and be associated with several aspects that are important to consider. Therefore, an MCDA approach was used when developing two alternative decision models (Section 3.4). The models were devised to be applicable with risk ranking but they can also be combined with other risk assessment methods.

As a basis for the MCDA models a risk ranking is needed and risk priority numbers should be calculated so that the risk reduction of possible alternatives can also be calculated (Section 3.1). Risk priority numbers can be calculated in different ways although the description of the MCDA models here is based on the common description of risk as a combination of probability and consequence, see Equation (3.2). The risk caused by an event is thus defined using a probability of occurrence and one or several consequences. Since an event may cause a set of n different consequences it may also be associated with n different risk types (R_k, $k = 1, 2,..., n$). The risk types may be related, for example, to supply interruptions and health risks. It is assumed that the probability of occurrence is independent of the consequence.

As illustrated in the risk matrix in Figure 5.18 a risk-reduction measure may affect the probability and/or the consequence of an event, see also Section 2.5. The risk reduction (ΔR_{jik}) that an alternative (j) is estimated to have on risk k related to event i is calculated as

$$\Delta R_{jik} = R_{jk} - R_{jik} \tag{5.6}$$

where R_{ik} is the initial risk level prior to any risk-reduction measure and R_{jik} is the residual risk after the measure has been implemented. Using this approach it is possible to consider that a risk-reduction measure may affect several events and for each event also several risk types.

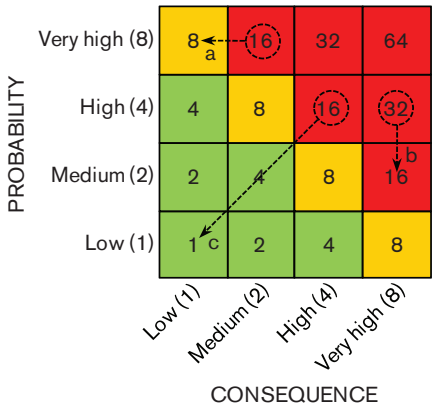


Figure 5.18 *Example of a risk matrix, including risk priority numbers calculated by multiplying the value of the probability class by the value of the consequence class. The green, orange and red represent acceptable risk (1-4), the ALARP region (8) and unacceptable risk (16-64) respectively.*

The calculated risk reductions are used slightly different in the two models to calculate the overall benefit of risk reduction and to also take uncertainties into consideration in the calculations. In one of the models discrete probability distributions are used and the model is thus named *the discrete model*. In the other model Beta distributions are used and therefore the model is named *the beta model*. The calculations are in both models performed using Monte Carlo simulations (Section 3.5).

It is suggested that an analysis of the cost of each risk-reduction measure is included when applying the MCDA models. The costs should be considered in order to enable CEA and CBA. The main steps in the two MCDA models are presented in Figure 5.19.

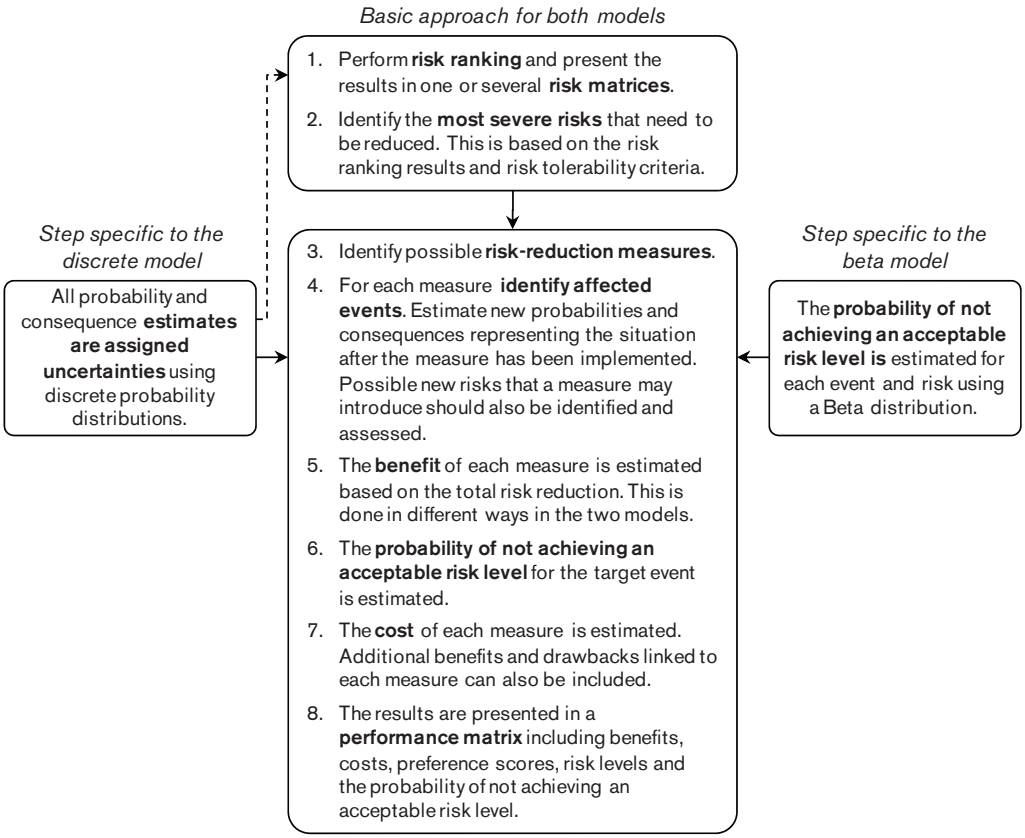


Figure 5.19 *The main steps in the MCDA models, starting with the risk ranking that provides input for the models. The steps common to the two models are presented in the middle and at each side the step specific to each model is shown.*

The discrete model

In the discrete model each probability and consequence value assigned to the events are estimated with consideration given to uncertainties. Discrete probability distributions are used and to facilitate model application a set of predefined distributions can be used (Figure 5.20). The example in Figure 5.20 illustrates discrete distributions for probability and consequence classes divided into four classes and assigned the values 1, 2, 4 and 8. The user can first estimate the most likely value (y-axis) and then consider how uncertain this estimate is (x-axis). To define distributions with the same degree of uncertainty, i.e. the columns in Figure 5.20, information about the distributions' entropy can be used. This is described and discussed further in Paper V.

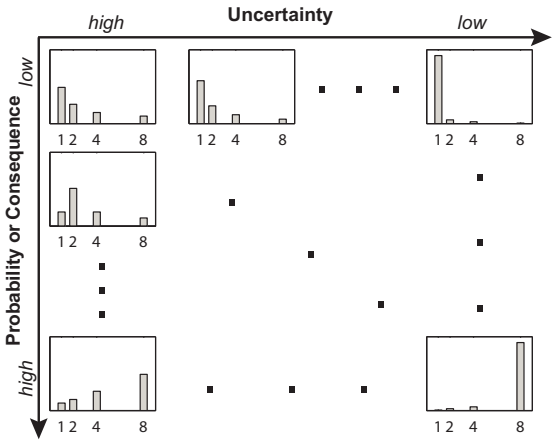


Figure 5.20 *Example of how a set of discrete distributions can be defined and used to help when identifying suitable distributions for the probability and consequence estimates.*

Based on the estimate probability and consequence values, including uncertainties, the total expected benefit ($\overline{u}_j$) of a measure (j) is calculated as a weighted sum of all reduced risks (k) for all affected events (i). Hence,

$$\overline{u}_j = \sum_i \sum_k \Delta R_{jik} w_k \tag{5.7}$$

where ΔR_{jik} is the estimated risk reduction of measure j related to event i and risk k, and $w_k \geq 0$ are weighting factors determining how much the reduction of each risk type contributes to the total benefit.

Since uncertainties are considered, the probability of *not* achieving an acceptable risk level can be calculated. A risk-reduction measure may affect several events but it is designed for one specific event and it is the probability of this target event not being acceptable that is most relevant.

The beta model

In the beta model the benefit of risk reduction is calculated based on the assumption that the highest benefit is achieved when the risk is reduced to an acceptable level. Compare, for example, risk reduction c and b in Figure 5.18. The same amount of reduction, in terms of a reduced risk priority number, is considered more beneficial if the risk is reduced from unacceptable to acceptable compared to if the final risk is still unacceptable. The probability of the final risk level being acceptable is therefore estimated for each risk-reduction measure using Beta distributions. The estimation is made based on the final risk level and

uncertainties about this level. As for the discrete model a set of distributions can be defined to facilitate model application, see Paper V (cf. Figure 5.20). For the discrete model the entropy was used to find distributions with the same level of uncertainty. For the Beta distributions the sum of the shape parameters α and β can be used (Paper V). Note that in comparison to the discrete model uncertainties are not assigned to each probability and consequence value in the beta model.

The total expected benefit of a risk-reduction measure ($\overline{u}_j$) that affects a set of events (i), and for each event a set of risks (k), is calculated as

$$\overline{u}_j = \sum_j \sum_k \Delta R_{jik} l_{jik} w_k \tag{5.8}$$

where ΔR_{jik} is the estimated risk reduction of measure j related to event i and risk k, l_{jik} represents the probability of achieving an acceptable risk level and $w_k \geq 0$ are weighting factors determining how much the reduction of each risk type contributes to the total benefit. For the target event the probability l_{jik} is also used in the final comparison of the risk-reduction measures.

Performance score and matrix

A performance score (s_j) is calculated for the alterative risk-reduction measures based on the benefit of risk reduction, the cost and possible other criteria included in the models. The score is calculated as a weighted sum based on how well the alternatives perform for each criterion, see Equation (3.8). The performance for each criterion is normalised so that, for example, the benefit of risk reduction may attain a value from 0 to 1, where 1 represents the highest benefit.

To summarise the MCDA results they are presented in a risk matrix including: (1) the benefit of risk reduction; (2) the cost; (3) the overall performance score; (4) initial and final risk levels for the target event; and (5) the probability of not reaching the acceptable risk level for the target event (one probability for each risk type). Initial and final risk levels are included so that alternatives not reducing the risk enough can be identified and so that the results can be analysed from an ALARP approach, see Section 2.5.

In addition to the results presented in the performance matrix, the uncertainties can be analysed further by calculating for the probability of each measure having

the highest performance score. This gives a quantification of the difference between the scores with consideration given to uncertainties. Furthermore, rank correlation coefficients can be calculated to analyse where additional information is most useful to reduce the uncertainties in the results.

Case study

The MCDA models were applied to analyse risk-reduction measures for the drinking water system in Bergen, Norway. A waterborne *Giardia* outbreak occurred in Bergen in 2004 and up to 6,000 persons were infected. As a result, it was concluded that a risk assessment covering the entire system was needed. A risk ranking was performed (Røstum *et al.*, 2009; Røstum and Eikebrokk, 2008) and the results of this work were used as input to the MCDA models.

The risk ranking identified 85 undesired events and the following four target events were used to exemplify how the MCDA models can be used:

1. Intrusion of contaminants in the distribution system during periods of low or no water pressure, causing unacceptable water quality.
2. Pipe break in the water mains due to wear or external forces, causing water quantity and quality problems.
3. Failure of UV disinfection due to power failure, causing water quality problems.
4. Raw water scarcity due a long drought, causing water quantity problems.

The events were analysed based on three risk types (R_k) that relate to: (1) *water quality*, i.e. health risks; (2) *water quantity*, i.e. supply interruptions; and (3) *loss of reputation/economy*. The probability and consequence scales were divided into four classes as in Figure 5.18. The same definition of acceptable risks, ALARP risks and unacceptable risks as shown in Figure 5.18 were used in the risk ranking in Bergen. No risk priority numbers were calculated in the risk ranking but for the purpose of the MCDA, the probability and consequence classes were assigned values as illustrated in Figure 5.18. The risk priority numbers were calculated using Equation (3.2) with $a = b = 1$, see results in Figure 5.18.

The risk-reduction measures presented in Table 5.5 were identified for the four target events. The alternative measures were analysed based on the benefit of reduced risk levels and the cost of implementing them. To simplify the example and provide transparent results that facilitate model evaluation a couple of

assumptions were made. In the discrete model a set of four distributions with the same degree of uncertainty was used to define the probability and consequence values. For the beta model a set of seven distributions, one for each risk level, was used to estimate the probability of the final risk level being acceptable. These distributions were also defined to be equally uncertain. Hence, no alternative sets of distributions as presented in Figure 5.20 were used. The distributions are presented in Paper V. Furthermore, the three risk types were assumed to be equally important when calculating the benefit in both models, i.e. $w_k = 1$. The benefit of risk reduction and the cost were also considered equally important and equal to 0.5 when calculating the performance score.

Table 5.5 *Risk-reduction measures identified for the four target events. For each measure the target event number and the number of additional events affected by each measure is specified.*

REF.	RISK-REDUCTION MEASURE	TARGET EVENT NO.	NO. OF ADDITIONAL EVENTS AFFECTED
1.1	Repair under pressure	1	0
1.2	Increase rehabilitation rate in the distribution network	1	2
1.3	Replace valves	1	0
1.4	New critical control point	1	0
1.5	More frequent recommendations for boiling	1	0
2.1	New pipeline	2	2
3.1	Monitor power supply	3	0
3.2	Increase UV capacity	3	0
3.3	Additional treatment barrier	3	1
3.4	Install system for uninterrupted power supply	3	1
3.5	Install emergency power supply	3	1
4.1	New reservoir	4	0
4.2	Repair leaks	4	1
4.3	Reduce water use	4	0
4.4	New raw water intake	4	0

The costs for implementing the measures were estimated qualitatively as low, low/medium, medium, medium/high or high. Discrete probability distributions were used to model uncertainties about the true cost categories in both models, see Paper V. The cost categories were translated into preference scores 0, 0.25,

0.50, 0.75 and 1, where 1 represents the most preferable outcome which is the low cost.

In Tables 5.6 and 5.7 the performance matrices are presented for the discrete and the beta model respectively. The matrices summarises the results of the MCDA models and provides a basis for evaluating and comparing the alternative measures. However, different approaches can be used when evaluating the results.

The risk-reduction measures can be compared based on the performance scores. However, what needs to be decided when analysing the performance scores is whether strong performance for one criterion is allowed to compensate for weak performance for other criteria. For example, for the discrete model (Table 5.6) measure 3.1 has the highest score for target event 3 although two of the risk types are unacceptable. To avoid this problem, critical performance levels can be defined such as that all risks must be reduced to an acceptable or ALARP level. By disqualifying alternatives not meeting the critical performance levels the remaining alternatives can be compared using the performance scores. Note, however, that the performance scores for the beta model (Table 5.7) look a bit different compared to the discrete model. This is because the probability of achieving an acceptable risk is included in the benefit calculation for the beta model. For each target event, none of the measures with the highest score are associated with unacceptable risks in the beta model.

One of the reasons why the initial and final risk levels are included in the performance matrices is to be able to consider the ALARP approach. As presented in Section 2.5 there is a risk level where some risks may be considered acceptable if it is economically and/or technically unreasonable to reduce them further. For example, in the beta model (Table 5.7) measure 1.2 has the highest score for target event 1 and it is able to reduce all risk levels to an acceptable level. Measures 1.1 and 1.4 have almost the same score but result in a quality risk in the ALARP region. Measure 1.2 is associated with the highest cost and from an ALARP perspective measure 1.1 or 1.4 could be selected instead if it is considered unreasonable to invest all the money required for measure 1.2.

Table 5.6 *Performance matrix for the discrete model including benefits ($\bar{u}_j$), costs and performance scores (s_j). For the target events (t) the initial (R_{tk}) and final (R_{jtk}) risk levels and the probability of the final risk being higher than the acceptable risk (R_{kc}) are presented. Red diamonds represent unacceptable risks, yellow triangles represent risks within the ALARP region and green circles represent acceptable risks.*

				$R_{tk} \rightarrow R_{jtk}$			$P(R_{jtk}>R_{kc})$		
Measure	$\bar{u}_j$	Cost	s_j	*qual.*	*quan.*	*rep.*	*qual.*	*quan.*	*rep.*
1.1	13.3	Low	0.50	◆→▲	●→●	▲→●	0.75	0.19	0.30
1.2	69.8	Medium/high	0.47	◆→●	●→●	▲→●	0.30	0.19	0.19
1.3	13.1	Medium	0.32	◆→▲	●→●	▲→●	0.76	0.19	0.30
1.4	13.0	Low	0.49	◆→▲	●→●	▲→●	0.77	0.19	0.30
1.5	8.9	Medium	0.29	◆→●	●→●	▲→◆	0.20	0.20	0.86
2.1	51.9	Medium	0.49	●→●	◆→●	▲→●	0.11	0.12	0.37
3.1	9.9	Low	0.48	◆→◆	▲→▲	◆→◆	0.86	0.75	0.87
3.2	10.8	Medium	0.30	◆→◆	▲→▲	◆→◆	0.87	0.75	0.86
3.3	17.2	High	0.15	◆→▲	▲→▲	◆→◆	0.76	0.76	0.88
3.4	41.3	Medium	0.45	◆→●	▲→●	◆→●	0.19	0.20	0.30
3.5	41.3	Medium	0.45	◆→●	▲→●	◆→●	0.20	0.19	0.29
4.1	31.2	Medium/high	0.31	●→●	◆→●	▲→●	0.13	0.20	0.20
4.2	42.9	Medium/high	0.36	●→●	◆→◆	▲→●	0.20	0.87	0.30
4.3	17.0	Medium	0.34	●→●	◆→◆	▲→●	0.19	0.87	0.30
4.4	33.0	High	0.24	●→●	◆→●	▲→●	0.12	0.13	0.19

Table 5.7 *Performance matrix for the beta model including benefits ($\bar{u}_j$), costs and performance scores (s_j). For the target events (t) the initial (R_{tk}) and final (R_{jtk}) risk levels and the probability of the final risk being higher than the acceptable risk (R_{kc}) are presented. Red diamonds represent unacceptable risks, yellow triangles represent risks within the ALARP region and green circles represent acceptable risks.*

				$R_{tk} \rightarrow R_{jtk}$			$P(R_{jtk}>R_{kc})$		
Measure	$\bar{u}_j$	Cost	s_j	*qual.*	*quan.*	*rep.*	*qual.*	*quan.*	*rep.*
1.1	8.5	Low	0.50	◆→▲	●→●	▲→●	0.50	0.12	0.31
1.2	57.7	Medium/high	0.65	◆→●	●→●	▲→●	0.31	0.12	0.12
1.3	8.5	Medium	0.32	◆→▲	●→●	▲→●	0.50	0.12	0.31
1.4	8.5	Low	0.50	◆→▲	●→●	▲→●	0.50	0.12	0.31
1.5	8.6	Medium	0.32	◆→●	●→●	▲→◆	0.12	0.12	0.69
2.1	53.6	Medium	0.72	●→●	◆→●	▲→●	0.02	0.02	0.31
3.1	5.0	Low	0.47	◆→◆	▲→▲	◆→◆	0.69	0.50	0.69
3.2	5.0	Medium	0.29	◆→◆	▲→▲	◆→◆	0.69	0.50	0.69
3.3	14.8	High	0.20	◆→▲	▲→▲	◆→◆	0.50	0.50	0.69
3.4	42.8	Medium	0.62	◆→●	▲→●	◆→●	0.12	0.12	0.31
3.5	42.7	Medium	0.62	◆→●	▲→●	◆→●	0.12	0.12	0.31
4.1	34.6	Medium/high	0.46	●→●	◆→●	▲→●	0.02	0.12	0.12
4.2	28.2	Medium/high	0.40	●→●	◆→◆	▲→●	0.12	0.69	0.31
4.3	9.5	Medium	0.33	●→●	◆→◆	▲→●	0.12	0.69	0.31
4.4	38.5	High	0.40	●→●	◆→●	▲→●	0.02	0.02	0.12

The alternative risk-reduction measures can also be analysed using a cost-effectiveness approach. For example, if it is required that all risks must be reduced to an acceptable level the measure that achieves this at the lowest cost is the most cost-effective. Although the costs are only estimated qualitatively, a cost-benefit approach can also be used when discussing the measures. For example, a high benefit at a low cost is of course more attractive compared to a low benefit at a high cost. However, when both the benefit and the costs are high or low it is less obvious which is most beneficial. This is basically the type of reasoning needed when evaluating ALARP risks.

The probability of not achieving an acceptable risk level can be used, for example, to compare measures resulting in the same risk levels. To further analyse the uncertainties in the results the probability of each measure having the highest score can be calculated. The histograms in Figure 5.21 show these probabilities for target events 1, 3 and 4. Note that the measures resulting in unacceptable risk levels are excluded from this analysis. The histograms show that the results from the two models are similar although it is much more likely that measure 1.2 has the highest score in the beta model compared to the discrete model. Measure 1.2 is the only measure for target event 1 that reduces all risk types to an acceptable level and this is also the reason for the differences that can be seen between the models.

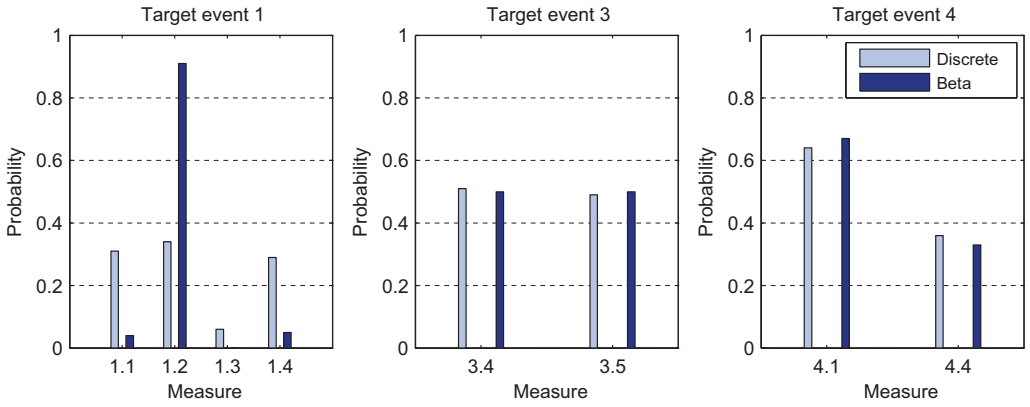


Figure 5.21 *Histograms showing the probability of each risk-reduction measure having the highest performance score. Measures resulting in unacceptable risk levels are excluded.*

The MCDA results should first of all be used to compare risk-reduction measures suggested for the same target events. However, due to limited economic resources or other reasons it may also be necessary to prioritise which measure,

out of a set of selected risk-reduction measures, should be implemented first. This type of prioritisation can be done by comparing the MCDA results.

Key aspects when applying the MCDA models

Based on the method development and the model applications, the following key aspects have been identified as important to consider when using the MCDA models:

- Select which MCDA model to use based on: (1) what is considered to be the best way to handle uncertainties; and (2) how the decision-maker perceives the benefit of risk reduction.
- Define values for the probability and consequence classes in a way that reflects the severity of the classes and define how risk priority numbers should be calculated.
- When selecting discrete and Beta distributions in the two models one should first decide what is the most likely value and then consider how uncertain this estimate is.
- As an aid when defining a set of discrete distributions the entropy can be used to identify distributions with the same degree of uncertainty. For the Beta distribution the sum of the shape parameters can be used instead.
- By considering more than one risk type (e.g. quantity and quality risks) in the MCDA the effect of risk-reduction measures can be evaluated thoroughly and a more comprehensive comparison of the measures is obtained compared to if only one risk type is considered.
- In addition to risk reduction and cost, possible additional criteria needed to evaluate risk-reduction measures should be identified for the specific decision problem. The weights for the different risk types and the criteria should be defined to reflect their relative importance.
- When evaluating and comparing the risk-reduction measures based on the performance scores it is important to consider the final risk levels. The results from the MCDA models can be used to identify the most cost-effective measure.
- Use the results to first identify which alternative is most suitable for each target event. The selected alternatives can then be compared to see what should be implemented first. This decision can also be based on the severity of the target event risks.

- Uncertainties can be analysed by, for example, calculating the probability of each measure having the highest score by using Monte Carlo simulations and analysing rank correlation coefficients. The latter analysis provides information on how to reduce the uncertainties in the results most effectively.
- It should be stressed that the MCDA models provide decision support based on the aspects and information included. As always, additional aspects may be necessary to consider when making the final decision.

6 DISCUSSION AND CONCLUSIONS

In this final chapter the contents of the thesis are discussed and the main conclusions are summarised. Possible further development and applications of the methods presented are also described.

6.1 Risk assessment from source to tap

Although risks have been managed by water utilities in the past, the more integrated and proactive approach emphasised today requires new methods. The risk-based water safety plans (WSPs) suggested by the WHO address the importance of considering the entire system in an integrated way, from source to tap (Section 2.4). By analysing the entire system and studying interactions between subsystems it is easier to see where risk-reduction measures are needed most and where they should be implemented to be most effective. The dynamic fault tree method presented in Section 5.2 and Papers I and II was developed because a lack of quantitative methods for integrated risk assessment had been identified.

The fault tree analysis of the drinking water system in Gothenburg showed that possible failures in the raw water system were the main contributors to the risk related to supply interruptions. It was also shown that the most effective alternative for reducing the risk included measures in the treatment part of the system. Single events, such as pump failure or quality deviation in the raw water source, do not need to affect the consumers. Instead, crucial situations arise when combinations, or chains, of events occur. If the water utility personnel are asked whether or not a specific event will cause harm to the consumers, the answer is often that it may do but it depends on other events and the functions of the system. Consideration of chains of events is therefore necessary to describe failure scenarios correctly. The dynamic fault tree method makes it possible to perform integrated risk assessments and to consider properly interactions between subsystems and events. Instead of focusing on one specific event, a fault tree model can include events that may differ in nature but all of which may contribute to the same type of system failure, such as supply interruptions or unacceptable water quality.

Integrated risk assessments and studies focused on a more limited number of events or focusing on a specific part of the system, should not be seen as competing activities. Both approaches are needed and the results from the different studies should be used as input for each other. An integrated risk assessment can identify problems that need to be analysed in more detail and a detailed analysis can provide input data when the entire system is analysed. It should be noted that the fault tree method can be applied when analysing smaller parts of a system. The method has been used, for example, to analyse parts of the water reclamation plant in Windhoek, Namibia. The analysis focused on how failures related to the coagulation, dissolved air flotation and filtration steps may affect the quality of the drinking water.

As described in Section 2.5, a model is a representation of the truth and is based on our interpretation and understanding of the truth. A good understanding of the analysed system is thus of paramount importance in obtaining useful risk assessment results. This emphasises the importance of including people with different areas of expertise when assessing risks to a drinking water system. The task of constructing a fault tree model is one example where a good understanding of the analysed system is crucial. Haimes (2009) points out the quality of the fault tree model as a possible major limitation in fault tree analysis. Significant failure events may be overlooked if the analyst does not fully understand the analysed system. This is of course relevant in all forms of analysis but may be considered especially important in quantitative methods. Those who are unfamiliar with a quantitative method may interpret the numerical results as true values not associated with any uncertainties. The importance of good-quality input data is also an argument for why uncertainties should be considered and analysed in risk assessments. By doing so it is possible to analyse the results in the light of uncertainties in input data, thus providing additional decision support.

6.2 Prioritising risk-reduction measures

The fact that we cannot eliminate every risk and that resources for risk reduction are limited makes correct prioritisation of risk-reduction measures important when balancing risks, costs and benefits. The applications presented here show how the quantitative fault tree method can be used to model the effect of risk-reduction measures (Paper III) and in combination with economic analysis provide decision support (Paper IV). It is also shown how a risk ranking approach can be used when estimating the effect of risk-reduction measures and how the results can be combined with other information in MCDA models

(Section 5.4 and Paper V). Different approaches are used when risk-reduction measures are evaluated based on the fault tree method and the MCDA models. Although different approaches are used, the case studies show that similar results can be obtained, including risk levels, costs and the probability of not meeting an acceptable risk level. Both approaches also make it possible to identify the most cost-effective alternative.

An integrated risk assessment approach may help to minimise sub-optimisation of risk-reduction efforts. The use of a fault tree model, for example, makes it possible to see how changes in one part of the system affect the function and risk level of the entire system. In addition to risk reduction other aspects are often important and the fault tree method was therefore combined with economic analysis. The fact that several aspects need to be considered when evaluating risk-reduction measures was also the reason why the decision models were based on an MCDA approach. The MCDA models were developed since qualitative/semi-quantitative risk ranking is recommended by the WHO as a useful tool when preparing WSPs, although a common structure for using the approach to evaluate risk-reduction measures is lacking. Although it may seem a simple task to estimate risks using a risk ranking approach and assigning scores in an MCDA, misleading results can be obtained if it is not based on a well-defined structure and approach.

A key question when evaluating risk levels and the effect of risk-reduction measures is what can be regarded as an acceptable risk. It should be stressed that it is the decision-makers who must define what is an acceptable risk and not the risk analysts. Both the fault tree method and the MCDA models showed that in addition to an acceptable risk the highest acceptable probability of not meeting this criterion should also be taken into account. Neither the calculated risk level nor the acceptable risk levels are free of uncertainty. Furthermore, what is considered to be an acceptable risk may vary. If, for example, the ALARP principle is applied then the benefit of further risk reduction is compared with the cost and technical requirements to achieve this reduction (Section 2.5). The decision whether or not the risk can be accepted depends on whether the benefit of risk reduction exceeds the costs and technical requirements.

The generic framework presented in Section 5.1 illustrates the basic steps involved in, and aspects affecting, risk management and decision-making in the context of drinking water supply. The close link between risk assessment and decision-making is shown and it is emphasised that risk assessments do not

provide answers but rather necessary decision support for making well-informed decisions.

6.3 Advantages and limitations of the methods developed

The dynamic fault tree method provides a new way of performing integrated risk assessments of drinking water systems and modelling risk-reduction measures that have not been available previously. The MCDA models provide a structure for using a risk ranking approach to not only prioritise risks but also to evaluate and compare risk-reduction measures. Common to the fault tree method and the MCDA models is that they are devised to consider uncertainties and thus enable uncertainty analysis. However, all methods are associated with both advantages and limitations. This is why one single method cannot be developed and used to analyse all the risk-related problems a water utility may face. Different methods are needed for different purposes. Available methods should be seen as part of a toolbox and the fault tree method and the MCDA models presented here are also part of this toolbox.

The dynamic fault tree method

The dynamic fault tree method provides information on the probability of failure as well as the failure rate and downtime at all levels in the fault tree. This is possible due to the approximate dynamic fault tree calculations, which also simplify model building and in particular reduce the computational demand compared to Markov simulations. The calculations can be performed using Monte Carlo simulations in traditional spreadsheet software. Information on failure rates and downtimes makes it possible to analyse the dynamic behaviour of the system. Since events are described using the concrete parameters of failure rate and downtime, elicitation of expert knowledge is also quite straightforward and unambiguous. Furthermore, since information on the proportion of consumers affected by different events is included in the fault tree it is possible to calculate risk levels. This is not common in fault tree analyses. However, risk levels should be analysed in combination with information on the dynamic behaviour of the system since subsystems with different failure rates and downtimes may cause the same level of risk.

The quantity- and quality-related risks are expressed as the number of minutes per year the average consumer is affected, i.e. Customer Minutes Lost (CML). For the case study application this was shown to be a useful way of expressing the

risk that could be compared to an existing performance criterion for the quantity-related risk. Note that the main failures included in a fault tree model can be defined in different ways. It may, for example, be of interest to analyse quality deviation due to a specific pathogen. For the quality-related risk the unit CML does not consider the actual health effects. However, results from a fault tree model could be combined with a quantitative microbial risk assessment to further analyse the health effects.

The comparison with results from Markov simulations shows that the approximate dynamic fault tree calculations in most cases only produce minor errors in the results. The errors can be accepted, especially when considering uncertainties in the results caused by uncertainty in input data. However, for the first AND-gate variant the errors increase with the number of compensating events included. Hence, if several compensating events are needed to model a system correctly, then uncertainty analysis must be performed to see how the errors affect the results.

The MCDA models

The two MCDA models are based on the traditional MCDA technique but have been devised to enable uncertainty analysis. This is not done in traditional risk ranking applications and can be seen as a major limitation. It may be difficult to evaluate the accuracy of MCDA results since there is no true and correct prioritisation of risk-reduction measures that can be used for comparison. However, if the model is based on theoretically well-founded techniques a reasonable way of evaluating it is to analyse whether or not the model includes the criteria that are considered important. The MCDA applications presented here include criteria for risk reduction and cost, although the models make it possible to include several other criteria that are deemed appropriate for evaluating risk-reduction measures.

The results from the MCDA models can be analysed based on different approaches and it is up to the decision-makers to select the approach to be used. As shown in the model applications, the performance matrices provide an overview of the results and make it possible to identify the strengths and limitations of the analysed risk-reduction measures.

A main advantage of MCDA is that results from different assessments, such as risk models and economic analysis, can be used as input when evaluating risk-reduction measures. Although the two MCDA models presented here are

combined with risk ranking they can be combined with other types of assessments. Results from a fault tree analysis can, for example, be used as input for an MCDA.

Conclusions

A fundamental difference between the fault tree method and risk ranking is that the first is quantitative whereas the latter is qualitative or semi-quantitative. To some extent the fault tree method requires more resources when building the model and collecting input data. However, the results are more detailed compared to the results from risk ranking (and the MCDA models). When a fault tree model exists, the task of updating it to model risk-reduction measures is not substantial. Risk ranking requires less detailed input data but to obtain accurate results the events need to be analysed carefully. Although there are differences between the methods, when used for assessing risks and evaluating risk-reduction measures they all help the users to identify and discuss important aspects that otherwise may be ignored.

Miller *et al.* (2005) list generic criteria important for risk assessment methods. The criteria include the logic soundness of the method, if relevant aspects of the problem can be considered, the accuracy and usefulness of the results and the applicability of the method. The dynamic fault tree method and the MCDA models all meet these criteria well although there are limitations. Specific recommendations on how to apply the methods are presented in Sections 5.2-5.4.

Efficient risk management, including proper risk assessments and decision analyses that enable well-informed decision-making, is necessary to achieve and maintain a reliable supply of safe drinking water. Research focused on developing theoretically well-founded methods that can be applied in practice contributes to the knowledge and the ability to assess risks. As not all risks can be eliminated, methods and tools for facilitating the task of balancing risks, cost and benefits are important. The methods for integrated risk assessment and decision analysis presented in this thesis provide useful decision support and facilitate efficient risk management of drinking water systems.

6.4 Communication and organisation

Although not the focus of this thesis, the task of communicating risk-related information is important and challenging. The risk assessment and decision

analysis results serve as a means of communicating what constitutes a risk and which risk-reduction measures are necessary to obtain and maintain an acceptable risk level. It is thus important to provide understandable results. Furthermore, for new methods to become useful they need to be communicated to potential users. The best way of doing this is by showing case studies as good examples.

In addition to good communication a basic requirement for efficient risk management is that the entire organisation understands and supports the proactive work being done. The process illustrated in the generic framework in Figure 5.1 neither should, nor can be, separated from the other work performed by a water utility. It should thus be an integral part of the work performed by the organisation. Based on two case studies, Summerill *et al.* (2010) discuss the role of organisational culture in the successful implementation of WSPs. Lack of time and resources, along with poor communication, were factors affecting the implementation of quality risk management projects at the case study sites. Dalgleish and Cooper (2005) point out that risk management procedures must be adjusted to fit the specific needs of the organisation as well as business culture and operating environment. Furthermore, MacGillivray and Pollard (2008) discuss the use of a capability maturity model for benchmarking risk management practice within the water utility sector. The Gothenburg case study showed that the use of risk assessment methods, such as the fault tree method, can be applied successfully and be used within organisations that are determined to work proactively using a risk-based approach.

6.5 Future research

The dynamic fault tree method and the MCDA models offer possibilities for further development and application. To further evaluate the applicability of the models and provide good examples, additional case studies could be performed. For the dynamic fault tree method, possible new approaches for combining information about several compensating events should be analysed to reduce the errors in the results from the first AND-gate variant. Structured updating of input data for a fault tree model could also be done in a case study to illustrate the possibilities. In the endeavour to provide a reliable drinking water supply and reduce costs, smaller systems are sometimes connected to a larger system and small water sources and treatment plants may in such cases be abandoned. However, actions of this nature need to be analysed thoroughly to avoid reducing

the overall reliability. The dynamic fault tree method could serve as a basis for analysing such scenarios.

The MCDA models here were applied using risk reduction and cost criteria. Strategies for how to include other important criteria when evaluating risk-reduction measures can be analysed. The suggested approaches to uncertainty assessment in MCDA can also be applied to problems not linked to drinking water supplies. By studying a wide range of possible applications further development may be possible.

The need for methods for risk assessment and decision analysis within the drinking water sector will not decrease in the future and it is thus important to further develop existing methods and devise new methods.

REFERENCES

Aller, L.T., Bennett, T., Lehr, J.H., Petty, R.J. and Hackett, G. (1987). *DRASTIC: A Standardized System for Evaluating Ground Water Pollution Potential Using Hydrogeologic Settings*, EPA-600/2-87-035, U.S. Environmental Protection Agency, Washington D.C.

Amari, S., Dill, G. and Howald, E. (2003). A new approach to solve dynamic fault trees, In *Annual Reliability and Maintainability Symposium 2003*, pp. 374-379, IEEE.

Ang, A.H.-S. and Tang, W.H. (2007). *Probability concepts in engineering: emphasis on applications in civil & environmental engineering*, 2nd ed., Wiley, New York.

Aven, T. (2003). *Foundations of risk analysis a knowledge and decision-oriented perspective*, Wiley, Chichester.

Aven, T. (2007). A unified framework for risk and vulnerability analysis covering both safety and security, *Reliability Engineering & System Safety*, 92 (6), 745-754.

Aven, T. (2010). On how to define, understand and describe risk, *Reliability Engineering & System Safety*, 95 (6), 623-631.

Aven, T. and Kørte, J. (2003). On the use of risk and decision analysis to support decision-making, *Reliability Engineering & System Safety*, 79 (3), 289-299.

Aven, T. and Renn, O. (2009). On risk defined as an event where the outcome is uncertain, *Journal of Risk Research*, 12 (1), 1-11.

AwwaRF (2006). *A Strategic Assessment of the Future of Water Utilities*, Awwa Research Foundation.

AZ/NZS (2004a). *Handbook: Risk Management Guidelines - Companion to AS/NZS 4360:2004*, Standards Australia/Standards New Zealand.

AZ/NZS (2004b). *Risk Management AS/NZS 4360:2004*, Standards Australia/Standards New Zealand.

Back, P.-E. (2006). *Value of Information Analysis for Site Investigations in Remediation Projects*, PhD Thesis No. 2551, Chalmers University of Technology, Göteborg.

Bartram, J., Corrales, L., Davison, A., Deere, D., Drury, D., Gordon, B., Howard, G., Rinehold, A. and Stevens, M. (2009). *Water safety plan manual: step-by-step risk management for drinking-water suppliers*, World Health Organization, Geneva.

Beauchamp, N., Lence, B.J. and Bouchard, C. (2010). Technical hazard identification in water treatment using fault tree analysis, *Canadian Journal of Civil Engineering*, 37 (6), 897-906.

Bedford, T. and Cooke, R.M. (2001). *Probabilistic risk analysis: foundations and methods*, Cambridge University Press, Cambridge.

Beuken, R., Sturm, S., Kiefer, J., Bondelind, M., Åström, J., Lindhe, A., Machenbach, I., Melin, E., Thorsen, T., Eikebrokk, B., Niewersch, C., Kirchner, D., Kozisek, F., Gari, D.W. and Swartz, C. (2008). *Identification and description of hazards for water supply systems - A catalogue of today's hazards and possible future hazards*, Deliverable no. D4.1.4, TECHEANU.

Blokker, M., Ruijg, K. and de Kater, H. (2005). Introduction of a substandard supply minutes performance indicator, *Water Asset Management International*, 1 (3), 19-22.

Boardman, A.E., Greenberg, D.H., Vining, A.R. and Weimar, D.L. (2006). *Cost-benefit analysis: Concepts and practice*, 3rd ed., Prentice Hall, Upper Saddle River, N.J.

Bouchard, C., Abi-Zeid, I., Beauchamp, N., Lamontagne, L., Desrosiers, J. and Rodriguez, M. (2010). Multicriteria decision analysis for the selection of a small drinking water treatment system, *Journal of Water Supply: Research and Technology—AQUA*, 59 (4), 230-242.

Boudali, H., Crouzen, P. and Stoelinga, M. (2007). A Compositional Semantics for Dynamic Fault Trees in Terms of Interactive Markov Chains, In *Automated Technology for Verification and Analysis*, Namjoshi, K.S., Yoneda, T., Higashino, T. and Okamura, Y. (Eds.), pp. 441-456, Springer, Heidelberg.

Breach, B. and Williams, T. (2006). The pivotal role of water safety plans, *Water 21*, August, 21-22.

Brouwer, W.B.F. and Koopmanschap, M.A. (2000). On the economic foundations of CEA. Ladies and gentlemen, take your positions!, *Journal of Health Economics*, 19 (4), 439-459.

Burgman, M.A. (2005). *Risks and decisions for conservation and environmental management*, Cambridge University Press, Cambridge.

CAN/CSA (1997). *Risk management: Guideline for decision-makers*, CAN/CSA Q850-97, Canadian Standards Association, Etobicoke, Ontario.

CDW/CCME (2004). *From source to tap: Guidance on the Multi-Barrier Approach to Safe Drinking Water*, Federal-Provincial-Territorial Committee on Drinking Water and Canadian Council of Ministers of the Environment Water Quality Task Group, Health Canada.

Cepin, M. and Mavko, B. (2002). A dynamic fault tree, *Reliability Engineering & System Safety*, 75 (1), 83-91.

Codex (2003). *Hazard and Critical Control Point (HACCP) System and Guidelines for its Application*, Annex to the Recommended International Code of Practice-General Principle of Food Hygiene, CAC/RCP 1-1969, Rev. 4-2003, Codex Alimentarius Commission.

Cohon, J.L. and Marks, D.H. (1975). A review and evaluation of multiobjective programming techniques, *Water Resources Research*, 11 (2), 208-220.

Communities and Local Government (2009). *Multi-criteria analysis: a manual*, Department for Communities and Local Government.

Cox, A.L. (2008). What's Wrong with Risk Matrices?, *Risk Analysis*, 28 (2), 497-512.

CSA (1997). *Risk Management: Guideline for Decision-Makers*, CAN/CSA-Q850-97, Canadian Standards Association.

Dalgleish, F. and Cooper, B.J. (2005). Risk management: developing a framework for a water authority, *Management of Environmental Quality*, 16 (3), 235-249.

Damikouka, I., Katsiri, A. and Tzia, C. (2007). Application of HACCP principles in drinking water treatment, *Desalination*, 210 (1-3), 138-145.

Davidsson, G., Haeffler, L., Ljundman, B. and Frantzich, H. (2003). *Handbook on risk analysis (In Swedish)*, The Swedish Rescue Services Agency, Karlstad.

Davison, A., Howard, G., Stevens, M., Callan, P., Fewtrell, L., Deere, D. and Bartram, J. (2005). *Water Safety Plans: Managing drinking-water quality from catchment to consumer*, WHO/SDE/WSH/05.06, World Health Organization, Geneva.

Dewettinck, T., Van Houtte, E., Geenens, D., Van Hege, K. and Verstraete, W. (2001). HACCP (Hazard Analysis and Critical Control Points) to guarantee safe water reuse and drinking water production – A case study, *Water Science and Technology*, 43 (12), 31-38.

Dugan, J.B., Bavuso, S.J. and Boyd, M.A. (1992). Dynamic fault-tree models for fault-tolerant computer systems, *IEEE Transactions on Reliability*, 41 (3), 363-377.

Durga Rao, K., Gopika, V., Sanyasi Rao, V.V.S., Kushwaha, H.S., Verma, A.K. and Srividya, A. (2009). Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment, *Reliability Engineering & System Safety*, 94 (4), 872-883.

Durga Rao, K., Sanyasi Rao, V.V.S., Verma, A.K. and Srividya, A. (2010). Dynamic Fault Tree Analysis: Simulation Approach, In *Simulation Methods for Reliability and Availability of*

Complex Systems, Faulin, J., Juan, A.A., Martorell Alsina, S.S. and Ramírez-Marquez, J.E. (Eds.), pp. 41-64, Springer, London.

DWWA (2006). *Guidelines for safe drinking water quality (In Danish)*, Danish Water and Wastewater Association, Skanderborg.

EC (1998). *Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption*, Official Journal of the European Communities, L 330, 5.12.98, 32-54.

EC (2000). *First report on the harmonisation of risk assessment procedures, Part 2: Appendices 26-27 October 2000*, European Commission, Health and Consumer Protection Directorate-General.

Egerton, A.-J. (1996). Achieving reliable and cost effective water treatment, *Water Science and Technology*, 33 (2), 143-149.

Fife-Schaw, C., Barnett, J., Chenoweth, J., Morrison, G.M. and Lundéhn, C. (2008). Consumer trust and confidence: some recent ideas in the literature, *Water Science and Technology: Water Supply*, 8 (1), 43-48.

Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S.L. and Keeney, R.L. (1981). *Acceptable risk*, Cambridge University Press, Cambridge.

French, S. (1995). Uncertainty and Imprecision: Modelling and Analysis, *The Journal of the Operational Research Society*, 46 (1), 70-79.

Garzon, F. (2006). Water safety plans in a developing country context, *Water 21*, February, 37-38.

Gray, N.F. (2005). *Water technology: An introduction for environmental scientists and engineers*, 2nd ed., Elsevier Butterworth-Heinemann, Oxford.

Gunnarsdóttir, M.J. and Gissurarson, L.R. (2008). HACCP and water safety plans in Icelandic water supply: Preliminary evaluation of experience, *Journal of Water and Health*, 6 (3), 377-382.

Göteborg Vatten (2006). *Action plan water: Long-term goals for the water supply in Gothenburg (In Swedish)*, City of Gothenburg.

Haas, C.N., Gerba, C.P. and Rose, J.B. (1999). *Quantitative microbial risk assessment*, Wiley, New York.

Haimes, Y.Y. (2006). On the Definition of Vulnerabilities in Measuring Risks to Infrastructures, *Risk Analysis*, 26 (2), 293-296.

Haimes, Y.Y. (2009). *Risk modeling, assessment, and management*, 3rd ed., John Wiley & Sons, Hoboken, N.J.

Hajkowicz, S. and Collins, K. (2007). A Review of Multiple Criteria Analysis for Water Resource Planning and Management, *Water Resources Management*, 21 (9), 1553-1566.

Hamilton, P.D., Gale, P. and Pollard, S.J.T. (2006). A commentary on recent water safety initiatives in the context of water utility risk management, *Environment International*, 32 (8), 958-966.

Havelaar, A.H. (1994). Application of HACCP to drinking water supply, *Food Control*, 5 (3), 145-152.

Havelaar, A.H. and Melse, J.M. (2003). *Quantifying public health risk in the WHO Guidelines for Drinking-water Quality: A burden of disease approach*, RIVM report 734301022.

HDR Engineering (2001). *Handbook of public water systems*, 2nd ed., Wiley, New York.

Hokstad, P., Røstum, J., Sklet, S., Rosén, L., Pettersson, T.J.R., Lindhe, A., Sturm, S., Beuken, R., Kirchner, D. and Niewersch, C. (2009). *Methods for risk analysis of drinking water systems from source to tap: Guidance report on risk analysis*, Deliverable no. D4.2.4, TECHNEAU.

Howard, G. (2003). Water safety plans for small systems: A model for applying HACCP concepts for cost-effective monitoring in developing countries, *Water Science and Technology*, 47 (3), 215-220.

Hrudey, S.E. (2004). Drinking-water Risk Management Principles for a Total Quality Management Framework, *Journal of Toxicology & Environmental Health: Part A*, 67 (20-22), 1555-1567.

Hrudey, S.E., Hrudey, E.J. and Pollard, S.J.T. (2006). Risk management for assuring safe drinking water, *Environment International*, 32 (8), 948-957.

Hunter, P.R. and Fewtrell, L. (2001). Acceptable risk, In *Water Quality: Guidelines, Standards and Health*, Fewtrell, L. and Bartram, J. (Eds.), pp. 207-227, IWA Publishing, London.

IEC (1995). *Dependability Management – Part 3: Application guide – Section 9: Risk analysis of technological systems*, International Standard IEC 300-3-9, International Electrotechnical Commission.

ISO (2009). *31000:2009 Risk management – Principles and guidelines*, International Organization for Standardization, Geneva.

ISO/IEC (2002). *Guide 73:2009 Risk management – Vocabulary – Guidelines for use in standards*, International Organization for Standardization and International Electrotechnical Commission.

IWA (2004). *The Bonn Charter for Safe Drinking Water*, International Water Association, London.

Jagals, C. and Jagals, P. (2004). Application of HACCP principles as a management tool for monitoring and controlling microbiological hazards in water treatment facilities, *Water Science and Technology*, 50 (1), 69-76.

Joerin, F., Cool, G., Rodriguez, M.J., Gignac, M. and Bouchard, C. (2009). Using multi-criteria decision analysis to assess the vulnerability of drinking water utilities, *Environmental Monitoring and Assessment*, 166 (1-4), 313-330.

Johansson, J. and Hassel, H. (2010). An approach for modelling interdependent infrastructures in the context of vulnerability analysis, *Reliability Engineering & System Safety*, 95 (12), 1335-1344.

Johansson, P.-O. (1993). *Cost-benefit analysis of environmental change*, Cambridge University Press, Cambridge; New York.

Kammen, D.M. and Hassenzahl, D.M. (2001). *Should we risk it? Exploring Environmental, Health, and Technological Problem Solving*, Princeton University Press, Princeton.

Kaplan, S. (1991). The general theory of quantitative risk assessment, In *Risk-Based Decision Making in Water Resources V*, Haimes, Y.Y., Moser, D.A. and Stakhiv, E.Z. (Eds.), pp. 11-39, American Society of Civil Engineers, New York.

Kaplan, S. (1993). Bayes' Theorem and Quantitative Risk Assessment, In *Risk-Based Decision Making in Water Resources VI*, Haimes, Y.Y., Moser, D.A. and Stakhiv, E.Z. (Eds.), pp. 186-193, American Society of Civil Engineers, New York.

Kaplan, S. (1997). The Words of Risk Analysis, *Risk Analysis*, 17 (4), 407-417.

Kaplan, S. and Garrick, B.J. (1981). On The Quantitative Definition of Risk, *Risk Analysis*, 1 (1), 11-27.

Keeney, R.L. (1982). Decision Analysis: An Overview, *Operations Research*, 30 (5), 803-838.

Keeney, R.L. and Raiffa, H. (1993). *Decision with Multiple Objectives: Preference and Value Tradeoffs*, Cambridge University Press, Cambridge.

Kletz, T. (2001). *Hazop and Hazan: identifying and assessing process industry hazards*, 4th ed., Institution of Chemical Engineers, Rugby.

Klinke, A. and Renn, O. (2002). A new approach to risk evaluation and management: Risk-based, precaution-based, and discourse-based strategies, *Risk Analysis*, 22 (6), 1071-1094.

Kristensen, V., Aven, T. and Ford, D. (2006). A new perspective on Renn and Klinke's approach to risk evaluation and management, *Reliability Engineering & System Safety*, 91 (4), 421-432.

Leitch, M. (2010). ISO 31000:2009—The New International Standard on Risk Management, *Risk Analysis*, 30 (6), 887-892.

Levin, H.M. and McEwan, P.J. (2001). *Cost-effectiveness analysis: Methods and applications*, 2nd ed., Sage Publications, Thousand Oaks, California.

Li, H. (2007). *Hierarchical Risk Assessment of Water Supply Systems*, PhD Thesis, Loughborough University, Loughborough.

Lindhe, A., Sturm, S., Røstum, J., Kožíšek, F., Gari, D.W., Beuken, R. and Swartz, C. (2010). *Risk assessment case studies: Summary report*, Deliverable no. D4.1.5g, TECHNEAU.

MacGillivray, B.H., Hamilton, P.D., Strutt, J.E. and Pollard, S.J.T. (2006). Risk analysis strategies in the water utility sector: an inventory of applications for better and more credible decision making, *Critical Reviews in Environmental Science and Technology*, 36 (2), 85-139.

MacGillivray, B.H. and Pollard, S.J.T. (2008). What can water utilities do to improve risk management within their business functions? An improved tool and application of process benchmarking, *Environment International*, 34 (8), 1120-1131.

MacGillivray, B.H., Sharp, J.V., Strutt, J.E., Hamilton, P.D. and Pollard, S.J.T. (2007a). Benchmarking risk management within the international water utility sector. Part I: Design of a capability maturity methodology, *Journal of Risk Research*, 10 (1), 85-104.

MacGillivray, B.H., Sharp, J.V., Strutt, J.E., Hamilton, P.D. and Pollard, S.J.T. (2007b). Benchmarking risk management within the international water utility sector. Part II: A survey of eight water utilities, *Journal of Risk Research*, 10 (1), 105-123.

Mannan, S. and Lees, F.P. (Eds.) (2005). *Lees' loss prevention in the process industries: hazard identification, assessment and control. Vol. 1*, 3rd ed., Elsevier Butterworth-Heinemann, Amsterdam/Boston.

McCann, B. (2005). Global support for safety plans, *Water 21*, August, 14-15.

Melchers, R.E. (2001). On the ALARP approach to risk management, *Reliability Engineering & System Safety*, 71 (2), 201-208.

Miller, R., Whitehill, B. and Deere, D. (2005). A national approach to risk assessment for drinking water catchments in Australia, *Water Science and Technology: Water Supply*, 5 (2), 123-134.

Ministry of Health (2005a). *Drinking-water Standards for New Zealand 2005*, New Zealand Ministry of Health, Wellington.

Ministry of Health (2005b). *A Framework on How to Prepare and Develop Public Health Risk Management Plans for Drinking-water Supplies*, New Zealand Ministry of Health, Wellington.

Morrison, G.M., Åström, J. and Hartung, J. (2009). Enhancing consumer relations: the role of trust and confidence, In *TECHNEAU: Safe Drinking Water from Source to Tap*, van den Hoven, T. and Kazner, C. (Eds.), pp. 419-428, IWA Publishing, London.

Mullenger, J., Ryan, G. and Hearn, J. (2002). A water authority's experience with HACCP, *Water Science and Technology: Water Supply*, 2 (5-6), 149-155.

Murphy, C. and Gardoni, P. (2008). The Acceptability and the Tolerability of Societal Risks: A Capabilities-based Approach, *Science and Engineering Ethics*, 14 (1), 77-92.

Nadebaum, P., Chapman, M., Morden, R. and Rizak, S. (2004). *A Guide To Hazard Identification & Risk Assessment For Drinking Water Supplies*, Research Report 11, Cooperative Research Center for Water Quality and Treatment.

NFSA (2006). *Improved safety and emergency preparedness in water supply: Guidance (In Norwegian)*, Norwegian Food Safety Authority Oslo.

NHMRC/NRMMC (2004). *National Water Quality Management Strategy: Australian Drinking Water Guidelines*, National Health and Medical Research Council and Natural Resource Management Ministerial Council, Australian Government.

Nolan, D.P. (1994). *Application of HAZOP and What-If Safety Reviews to the Petroleum, Petrochemical and Chemical Industries*, William Andrew Publishing/Noyes, Park Ridge, New Jersey.

Norberg, T., Rosén, L. and Lindhe, A. (2009). Added value in fault tree analyses, In *Safety, Reliability and Risk Analysis: Theory, Methods and Applications*, Martorell, S., Guedes Soares, C. and Barnett, J. (Eds.), pp. 1041-1048, Taylor & Francis Group, London.

Norrman, J. (2004). *On Bayesian Decision Analysis for Evaluating Alternative Actions at Contaminated Sites*, PhD Thesis No. 2202, Chalmers University of Technology, Göteborg.

Olofsson, B., Tideström, H. and Willert, J. (2001). *Identification of risks to urban water supplies (In Swedish)*, Report 2001:2, Urban Water, Chalmers University of Technology, Göteborg.

Owen, A.J., Colbourne, J.S., Clayton, C.R.I. and Fife-Schaw, C. (1999). Risk communication of hazardous processes associated with drinking water quality – a mental models approach to customer perception, Part 1 – a methodology, *Water Science and Technology*, 39 (10-11), 183-188.

Paté-Cornell, M.E. (1996). Uncertainties in risk analysis: Six levels of treatment, *Reliability Engineering & System Safety*, 54 (2-3), 95-111.

Pettersson, T.J.R., Åström, J., Bondelind, M., Lindhe, A., Rosén, L., Røstum, J., Niewersch, C., Kirchner, D., Beuken, R., Sturm, S., Kiefer, J., Kozisek, F., Gari, D.W., Pumann, P., Swartz, C. and Menaia, J. (2010). *Catalogue of Risk Reduction Option in Drinking Water Systems*, Deliverable no. D4.3.1/2, TECHNEAU.

Pollard, S.J.T. (2008). *Risk Management for Water and Wastewater Utilities*, IWA Publishing, London.

Pollard, S.J.T., Strutt, J.E., Macgillivray, B.H., Hamilton, P.D. and Hrudey, S.E. (2004). Risk analysis and management in the water utility sector - a review of drivers, tools and techniques, *Process Safety and Environmental Protection*, 82 (6 B), 453-462.

Purdy, G. (2010). ISO 31000:2009—Setting a New Standard for Risk Management, *Risk Analysis*, 30 (6), 881-886.

Ramsey, S., Willke, R., Briggs, A., Brown, R., Buxton, M., Chawla, A., Cook, J., Glick, H., Liljas, B., Petitti, D. and Reed, S. (2005). Good Research Practices for Cost-Effectiveness Analysis Alongside Clinical Trials: The ISPOR RCT-CEA Task Force Report, *Value in Health*, 8 (5), 521-533.

Rausand, M. and Høyland, A. (2004). *System reliability theory: models, statistical methods, and applications*, 2nd ed., Wiley-Interscience, N.J.

Reason, J. (1990). *Human error*, Cambridge University Press, Cambridge.

Renn, O. (1998). The role of risk perception for risk management, *Reliability Engineering & System Safety*, 59 (1), 49-62.

Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world*, Earthscan, London.

Risebro, H.L., Doria, M.F., Andersson, Y., Medema, G., Osborn, K., Schlosser, O. and Hunter, P.R. (2007). Fault tree analysis of the causes of waterborne outbreaks, *Journal of Water and Health*, 5 (1), 1-18.

Rizak, S., Cunliffe, D., Sinclair, M., Vulcano, R., Howard, J., Hrudey, S. and Callan, P. (2003). Drinking water quality management: A holistic approach, *Water Science and Technology*, 47 (9), 31-36.

Rosén, L. (1994). A Study of the DRASTIC Methodology with Emphasis on Swedish Conditions, *Ground Water*, 32 (2), 278-285.

Rosén, L. (1995). *Estimation of hydrogeological properties in vulnerability and risk assessments*, Ph.D. Thesis No. 1153, Chalmers University of Technology, Göteborg.

Rosén, L., Hokstad, P., Lindhe, A., Sklet, S. and Røstum, J. (2007). *Generic framework and methods for integrated risk management in water safety plans*, Deliverable no. D4.1.3, D4.2.1, D4.2.2, D4.2.3, TECHNEAU.

Rosén, L. and Lindhe, A. (2007). *Trend report: Report on trends regarding future risks*, Deliverable no. D 1.1.9, TECHEANU.

Rosén, L., Lindhe, A., Chenoweth, J., Fife-Schaw, C. and Beuken, R. (2010). *Decision support for risk management in drinking water supply - Overview and framework*, Deliverable no. D4.4.1, TECHNEAU.

Rosness, R. (1998). Risk Influence Analysis A methodology for identification and assessment of risk reduction strategies, *Reliability Engineering & System Safety*, 60 (2), 153-164.

Ross, S.M. (1996). *Stochastic processes*, 2nd ed., Wiley, New York.

Roy, B. (2005). Paradigms and Challenges, In *Multiple Criteria Decision Analysis: State of the Art Surveys*, Figueira, J., Greco, S. and Ehrogott, M. (Eds.), pp. 3-24, Springer, New York.

Rygaard, M., Binning, P.J. and Albrechtsen, H.-J. (2011). Increasing urban water self-sufficiency: New era, new challenges, *Journal of Environmental Management*, 92 (1), 185-194.

Røstum, J., Aasen, A. and Eikebrokk, B. (2009). Risk and Vulnerability Assessment ("Ros-Analysis") of the Bergen Water Supply System – A Source to Tap Approach, In *Risk Management of Water Supply and Sanitation Systems*, Hlavinek, P., Popovska, C., Marsalek, J., Mahrikova, I. and Kukharchyk, T. (Eds.), pp. 73-83, Springer.

Røstum, J. and Eikebrokk, B. (2008). *Risk and vulnerability analysis of the Bergen water supply system (In Norwegian)*, Report no. SBF IN F08304, SINTEF.

Savage, L.J. (1954). *The foundations of statistics*, Wiley, New York.

Schaub, S. (2004). A Risk Assessment Framework for Waterborne Pathogens and Requirements for Producing a Complete Protocol, *Human and Ecological Risk Assessment*, 10 (1), 151-159.

Sinclair, M. and Rizak, S. (2004). Drinking-water Quality Management: The Australian Framework, *Journal of Toxicology & Environmental Health: Part A*, 67 (20-22), 1567-1580.

Slovic, P. (1987). Perception of risk, *Science*, 236 (4799), 280-285.

Slovic, P. (2001). The risk game, *Journal of Hazardous Materials*, 86 (1-3), 17-24.

Slovic, P. (2002). Terrorism as hazard: A new species of trouble, *Risk Analysis*, 22 (3), 425-426.

SLVFS 2001:30 *National Food Administration Ordinance on Drinking Water (In Swedish)*, Swedish National Food Administration.

SNAO (2008). *Drinking water supply: preparedness for large crises (In Swedish)*, 2008:8, The Swedish National Audit Office.

SNFA (2007). *Risk and vulnerability analysis for drinking water supply (In Swedish)*, Swedish National Food Administration, Uppsala.

Stewart, T. (2005). Dealing with Uncertainties in MCDA, In *Multiple Criteria Decision Analysis: State of the Art Surveys*, Figueira, J., Greco, S. and Ehrogott, M. (Eds.), pp. 445-466, Springer, New York.

Summerill, C., Pollard, S.J.T. and Smith, J.A. (2010). The role of organizational culture and leadership in water safety plan implementation for improved risk management, *Science of the Total Environment*, 408 (20), 4319-4327.

SWWA (2007). *Drinking water: Production and Distribution - Handbook on surveillance including HACCP (In Swedish)*, 2007-06-26, Swedish Water and Wastewater Association, Stockholm, Available from http://www.svensktvatten.se/web/haccp.aspx.

Van der Bruggen, B. (2010). The Global Water Recycling Situation, In *Sustainable Water for the Future: Water Recycling versus Desalination*, Escobar, I.C. and Schäfer, A.I. (Eds.), pp. 41-62, Elsevier.

van Leeuwen, C.J. and Vermeire, T.G. (2007). *Risk assessment of chemicals: An introduction*, 2nd ed., Springer, Dordrecht.

Vesely, W.E., Goldberg, F.F., Roberts, N.H. and Haasl, D.F. (1981). *Fault Tree Handbook*, NUREG-0492, U.S. Nuclear Regulatory Commission.

Vesely, W.E., Stamatelatos, M., Dugan, J.B., Fragola, J., Minarick, J. and Railsback, J. (2002). *Fault Tree Handbook with Aerospace Applications*, NASA Office of Safety and Mission Assurance, Washington.

West, M. and Harrison, J. (1997). *Bayesian forecasting and dynamic models*, 2nd ed., Springer, New York.

WHO (2004). *Guidelines for drinking-water quality. Vol. 1, Recommendations*, 3rd ed., World Health Organization, Geneva.

WHO (2008). *Guidelines for drinking-water quality [electronic resource]: Incorporating first and second addenda, Vol. 1, Recommendations*, 3rd ed., World Health Organization, Geneva.

Vieira, J.M.P. (2007). Water safety plans: Methodologies for risk assessment and risk management in drinking water systems, *IAHS-AISH Publication*, 310, 57-67.

von Neumann, J. and Morgenstern, O. (1947). *Theory of games and economic behavior*, 2. ed., Princeton University Press, Princeton, N.J.

Yokoi, H., Embutsu, I., Yoda, M. and Waseda, K. (2006). Study on the introduction of hazard analysis and critical control point (HACCP) concept of the water quality management in water supply systems, *Water Science and Technology*, 53 (4-5), 483-492.

Åström, J., Pettersson, T.J.R. and Stenström, T.A. (2007). Identification and management of microbial contaminations in a surface drinking water source, *Journal of Water and Health*, 5 (Suppl. 1), 67-79.

PAPERS

The following papers are appended to the printed version of the thesis but are not included in this electronic version:

I. **Lindhe**, **A**., Rosén, L., Norberg, T. and Bergstedt, O. (2009). Fault tree analysis for integrated and probabilistic risk analysis of drinking water systems, *Water Research*, 43 (6), 1641-1653.

II. **Lindhe**, **A**., Norberg, T. and Rosén, L. (2010). Approximate dynamic fault tree calculations for modelling water supply risks, Submitted to *Risk Analysis*.

III. Rosén, L., **Lindhe**, **A**., Bergstedt, O., Norberg, T. and Pettersson, T.J.R. (2010). Comparing risk-reduction measures to reach water safety targets using an integrated fault tree model, *Water Science and Technology: Water Supply*, 10 (3), 428-436.

IV. **Lindhe**, **A**., Rosén, L., Norberg, T., Bergstedt, O. and Pettersson, T.J.R. (2010). Cost-effectiveness analysis of risk-reduction measures to reach water safety targets, Accepted for publication in *Water Research*, doi: 10.1016/j.watres.2010.07.048.

V. **Lindhe**, **A**., Rosén, L., Norberg, T., Røstum, J. and Pettersson, T.J.R. (2010). Risk-based multi-criteria decision models for prioritising water safety measures, Submitted to *Water Research*.