THESIS FOR THE DEGREE OF LICENTIATE OF ENGINEERING

Integrated and Probabilistic Risk Analysis of Drinking Water Systems

ANDREAS LINDHE

Department of Civil and Environmental Engineering
Division of GeoEngineering
CHALMERS UNIVERSITY OF TECHNOLOGY
Göteborg, Sweden 2008

Integrated and Probabilistic Risk Analysis of Drinking Water Systems
ANDREAS LINDHE

ISSN 1652-9146
Lic 2008:8

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

Chalmers reproservice
Göteborg, Sweden 2008

Integrated and Probabilistic Risk Analysis of Drinking Water Systems
ANDREAS LINDHE
Department of Civil and Environmental Engineering
Division of GeoEngineering
Chalmers University of Technology

ABSTRACT

Drinking water supply is an essential public function but is at the same time exposed to risks. Since a totally risk-free society is not attainable, risks need to be managed efficiently to achieve an acceptable level of risk. A reliable supply of safe drinking water is vital and the World Health Organization emphasises an integrated risk management approach, including the entire drinking water system from source to tap. An integrated approach is important as there are interactions between different parts of a system. Efficient risk management requires appropriate risk analyses to characterise risk and support decision-making. Risk analysis based on an integrated approach facilitates well-informed decision-making and efficient use of resources for risk reduction. However, guidance on methods for integrated risk analysis of drinking water systems is limited.

To support risk management of drinking water systems, a method for integrated and probabilistic risk analysis has been developed and evaluated based on a real-world application. The method is probabilistic in order to include uncertainties of estimates, which always exist due to lack of knowledge and natural variation. A framework for integrated risk management of drinking water systems is also suggested to show the context for risk analysis and to point out important steps in risk management of drinking water systems. The suggested method can be used to model entire systems from source to tap and to include interactions between events. It provides information on risk levels as well as the dynamic behaviour of the system in terms of the failure rate and duration of failures. Furthermore, it enables comparisons of the results with performance targets and acceptable levels of risk. One single method cannot be used to handle all risk-related issues. What is needed instead is a set of tools. The method developed has been shown to facilitate integrated risk analysis from source to tap and thus also informed decision-making, which may assist in minimising sub-optimisation of risk-reduction options. The method is thus one source of input into a set of tools to assist water utilities in risk analysis and risk management.

Keywords: drinking water system, risk, hazard, risk analysis, water safety plan, fault tree analysis, integrated, probabilistic, uncertainty, customer minutes lost.

LIST OF PAPERS

This thesis includes the following papers, referred to by Roman numerals:

I. Lindhe, A., L. Rosén, T. Norberg and O. Bergstedt (2008). Fault tree analysis for integrated and probabilistic risk analysis of drinking water systems, Submitted to *Water Research*.

II. Lindhe, A., L. Rosén, T. Norberg, T.J.R. Pettersson, O. Bergstedt, J. Åström and M. Bondelind (2008). Integrated risk analysis from source to tap: Case study Göteborg, Revised version of paper in proceedings of the *6th Nordic Drinking Water Conference*, Oslo, 9-11 June, 231-241.

Division of work between authors

In Paper I, all 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, performed the simulations and was the main author of the paper.

In Paper II, all authors defined the objectives of the study and described the system. Lindhe structured the fault tree model and analysed input data in collaboration with the other authors. Lindhe also performed the calculations and was the main author of the paper.

Publications not appended

The author has contributed significantly to the following publications, which are not appended to the thesis:

- Beuken, R., S. Sturm, J. Kiefer, M. Bondelind, J. Åström, A. Lindhe, I. Machenbach, E. Melin, T. Thorsen, B. Eikebrokk, C. Niewersch, D. Kirchner, F. Kozisek, D.W. Gari and C. Swartz (2007). *Identification and description of hazards for water supply systems – A catalogue of today's hazards and possible future hazards*, Deliverable no. D 4.1.1, D 4.1.2, TECHEANU.
- Hokstad, P., J. Røstum, S. Sklet, L. Rosén, T.J.R. Pettersson, A. Lindhe, S. Sturm, R. Beuken, D. Kirchner and C. Niewersch (2008*). Analysing the*

risks of drinking water systems from source to tap (In prep), Deliverable no. D 4.2.4, TECHNEAU.

- Lindhe, A., L. Rosén, T. Norberg, T.J.R. Pettersson, J. Åström and M. Bondelind (2007). Integrated risk analysis of a drinking water system – a fault tree analysis (*Abstract*), Presented at the Society for Risk Analysis Europe 2007 Conference, The Hague, 17-19 June.
- Norberg, T., L. Rosén and A. Lindhe (2008). Added value in fault tree analyses (*In press*), European Safety and Reliability Association 2008 and 16th Society for Risk Analysis Europe Conference, Valencia, 22-25 September.
- Rosén, L., O. Bergstedt, A. Lindhe, T.J.R. Pettersson, A. Johansson and T. Norberg (2008). Comparing Raw Water Options to Reach Water Safety Targets Using an Integrated Fault Tree Model, Paper presented at the International Water Association Conference, Water Safety Plans: Global Experiences and Future Trends, Lisbon, 12-14 May.
- Rosén, L., P. Hokstad, A. Lindhe, S. Sklet and J. Røstum (2007). *Generic framework and methods for integrated risk management in water safety plans*, Deliverable no. D 4.1.3, D 4.2.1, D 4.2.2, D 4.2.3, TECHNEAU.
- Rosén, L. and A. Lindhe (2007). *Trend report: Report on trends regarding future risks*, Deliverable no. D 1.1.9, TECHEANU.
- Rosén, L., A. Lindhe, P. Hokstad, S. Sklet, J. Røstum and T.J.R. Pettersson (2008). Generic Framework for Integrated Risk Management in Water Safety Plans, In proceedings of the *6th Nordic Drinking Water Conference,* Oslo, 9-11 June, 193-203.

ACKNOWLEDGMENTS

The work on this thesis has been carried out within DRICKS, the framework programme for drinking water research at Chalmers University of Technology. A great deal of the work has also been part of the Techneau project, funded by the European Commission (contract no. 018320). Financial support has been provided by the Swedish Water & Wastewater Association, the City of Gothenburg and the Techneau project. The author gratefully acknowledges all financiers for their support.

I would like to express my heartfelt appreciation to my supervisors Professor Lars Rosén, Assistant Professor Thomas Pettersson and Associate Professor Tommy Norberg. Thank you all for your inspiring discussions, constructive feedback and extensive support.

I would also like to express my gratitude to my colleagues within DRICKS; besides Lars, Thomas and Tommy, also Johan Åström, Mia Bondelind and Olof Bergstedt. I am also grateful to my colleagues at the Division of GeoEngineering for being good friends and providing an inspiring working climate.

The successful results of this work are to a large extent due to the valuable and fruitful collaboration with Göteborg Vatten. My sincere thanks to Olof Bergstedt, Helena Hallagård, Claes Wångsell and the rest of the personnel at Göteborg Vatten who have participated in discussions and provided me with data and comments on the work.

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

Finally, I would like to thank my friends and family for their support and encouragement. Very special thanks to Therese for her love, patience and encouragement.

Göteborg, September 2008

Andreas Lindhe

TABLE OF CONTENTS

LIST OF NOTATIONS

The following notations are used in the main text of the thesis:

CML	Customer Minutes Lost
HACCP	Hazard Analysis and Critical Control Point
MDT	Mean Downtime
MTBF	Mean Time Between Failures
MTTF	Mean Time To Failure
PHRMP	Public Health Risk Management Plan
QCRA	Quantitative Chemical Risk Assessment
QMRA	Quantitative Microbial Risk Assessment
WHO	World Health Organization
WSP	Water Safety Plan

R	Risk
P	Probability
P_F	Probability of failure
μ	Mean repair rate
$1/\mu$	Mean downtime
λ	Mean failure rate
$1/\lambda$	Mean time to failure
C	Proportion of consumers affected
q	Probability of failure on demand

1 INTRODUCTION

The first chapter provides the background to the thesis, defines the main objectives and presents the scope of the work. Some limitations of the thesis are also described.

1.1 Background

A reliable supply of safe drinking water is essential for society and its sustainable development. Factors such as human health and economic development rely on a safe water supply. However, drinking water systems are vulnerable and subject to a wide range of risks. Since we cannot eliminate every risk and create a totally risk-free society, we instead need to manage risks efficiently to achieve an acceptable level of risk. The World Health Organization (WHO) emphasises in the third edition of the *Guidelines for Drinking-water Quality* that a comprehensive risk assessment and risk management approach is the most effective way to ensure the safety of a drinking water supply (WHO, 2004).

The WHO (2004) concludes that end-product testing is not sufficient to guarantee safe drinking water to consumers. Instead, the WHO recommends preparation of risk-based Water Safety Plans (WSPs), including *system assessment*, *operational monitoring* and *management plans* (Davison *et al.*, 2005; WHO, 2004). The WSPs should in a comprehensive way consider conditions in source waters as well as treatment and distribution systems. This preventive and integrated approach, i.e. from source to tap, is emphasised also in the *Bonn Charter* (IWA, 2004) and national guidelines, e.g. in Australia (NHMRC/NRMMC, 2004) and Canada (CDW/CCME, 2004). The WSP approach provides an important focus on risk issues related to drinking water systems but also includes limited guidance on specific tools and examples to assist water utilities in their work.

Efficient risk management, aimed at achieving an acceptable level of risk, requires that several tasks are carried out and performed in an iterative way. Risk management is often described as a process composed of: (1) *risk analysis*, including scope definition, hazard identification and risk estimation; (2) *risk evaluation*, including tolerability decision and analysis of risk-reduction options; and (3) *risk reduction/control*, including decision-making, implementation and

monitoring. The initial risk analysis step provides information for the subsequent evaluation. It is thus important that the risk analysis reflects the analysed system adequately and provides relevant information.

As part of the WSP approach, the WHO (2004) and Davison *et al.* (2005) suggest a general method for risk ranking. The method is based on a risk matrix with discrete probability and consequence scales. This qualitative (or semi-quantitative) method is simple to use and the results are easy to communicate. However, the method cannot be used to consider chains of events, model interactions between events or quantify the risk. Furthermore, it is difficult to perform meaningful uncertainty analysis for this type of method. Although the method has several limitations it is useful in many cases. It may, for example, be used to analyse systems with simple structures and perform preliminary analyses to guide further studies. To enable analyses of systems, including complicated conditions, additional methods and tools are required. A set of tools for risk analysis that supports the WSP approach would thus provide valuable support to water utilities.

To reflect system properties properly a risk analysis should integrate the entire drinking water system from source to tap. It is possible to carry out separate analyses of the different parts of the system and merge the results. However, an integrated analysis has several advantages, provided that interactions between parts and events can be considered. The potential to quantify the level of risk is also important since it enables comparison with other risks and acceptable levels of risk in absolute terms. Furthermore, the efficiency of risk-reduction options can be estimated quantitatively.

Managing risks is nothing new in the drinking water sector. Efforts to prevent failures have always been made although the structured way of working offered by risk management frameworks and the methods currently available in different fields are to a large extent new. The concept of WSP is attracting more and more attention around the world and is currently being implemented in many countries. The fact that drinking water systems often have a complex structure with interactions between sub-systems, and the fact that they are subject to a wide range of risks, makes risk analysis an important as well as difficult task. Consequently, tools for risk analysis that can support risk management of drinking water systems in accordance with the WSP approach are needed.

Society's interest in achieving efficient risk management of drinking water systems is pointed out, for example, in projects such as MicroRisk (contract no.

EVK1-CT-2002-00123) and Techneau (contract no. 018320), both funded by the European Commission. The latter project is closely linked to this thesis and parts of the work presented have been carried out within the Techneau project.

1.2 Aim and objectives

The overall aim of this thesis is

> *to contribute to the knowledge regarding quantitative risk analysis of drinking water systems in accordance with the Water Safety Plan approach.*

It is not possible to develop one single method that can cover all relevant risks to a drinking water system. Instead, a set of tools that complement each other is needed. This thesis mainly focuses on how integrated risk analysis can be performed with regard to the ability to deliver safe drinking water. Since uncertainties are typically considerable in risk analyses of drinking water systems, a probabilistic approach is used. A method for integrated and probabilistic risk analysis of drinking water systems has been developed and is aimed at serving as an important input into a set of tools for supporting water utilities in managing risks. To put quantitative risk analysis of drinking water systems in the right context, risk management and its connection to drinking water systems is described.

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

- To describe a framework for integrated risk management of drinking water systems.
- To develop a method for integrated and probabilistic risk analysis of drinking water systems.
- To apply the method and evaluate its benefits and limitations.

1.3 Scope of the work

To achieve the aim and objectives of the thesis a theoretical desk study, method development and method application in a case study have been carried out. Based on a literature review a theoretical background to risk and drinking water

systems is presented in Chapters 2 and 3. The specific objectives of the thesis have been fulfilled by performing the following tasks:

- A framework for integrated risk management of drinking water systems is described in Chapter 4. It is based on a literature review and studies of existing international and national frameworks and guidelines. The framework provides information on important steps to be carried out when managing risks to drinking water systems and illustrates the purpose of risk analysis in risk management.
- A quantitative method has been developed to facilitate integrated and probabilistic risk analysis of drinking water systems. The method is based on fault tree analysis and is described in Chapter 5 and Paper I. As a background to the method an introduction to qualitative and quantitative risk analysis is provided in Section 4.3.
- The developed fault tree method has been applied to a drinking water system in Sweden in order to test and evaluate it based on a real-world application. The application of the method and its possibilities, strengths and limitations are presented in Chapter 5 and Paper II.

The contents of the thesis are discussed further in Chapter 6 and the main conclusions of the work are summarised in Chapter 7.

1.4 Limitations

Risk and drinking water are two wide research fields and since all aspects cannot be assigned the same attention, proper limitations need to be made. The most important limitations of this thesis are:

- Apart from the framework for integrated risk management the thesis focuses mainly on risk analysis and not on risk evaluation and risk reduction/control.
- Risk analysis is part of the preventive work. Issues related to management of an event after it has occurred (crisis management) are not considered here.
- Risk analysis of drinking water systems can be performed in many different ways. The purpose of this thesis is to study integrated analysis,

i.e. include the entire supply chain, and to consider a wide range of hazards rather than focus on specific hazards in specific parts of the system.

2 THE CONCEPT OF RISK AND RISK MANAGEMENT

The first part of this chapter introduces the concept of risk and describes some important aspects related to it. Furthermore, the chapter presents a generic outline of the risk management process, its elements and how they are linked. Finally, risk analysis within the risk management process is described in more detail.

2.1 Risk

The word *risk* is used in different ways depending on the context. Sometimes it is used as a synonym for the probability of an undesired event to occur. However, a common description of risk is that it is a combination of the probability and the consequence of a hazardous event, see e.g. European Commission (2000) and documents by the International Electrotechnical Commission and the International Organization for Standardization (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):

- 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 by 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 (S_i, L_i, X_i), $i = 1, 2, \ldots, n$. 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 $R = \{< S_i, L_i, X_i >\}_c$. 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 commonly 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 cases be suitable to express risk in this way. Risk may also be expressed in many other ways depending on the specific situation (see Section 3.5).

Quantitative definitions of risk 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 other costs and benefits in the decision process. However, even if 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). As stated by Kammen and Hassenzahl (2001), risk analysis is intended to inform, but not determine, decisions.

A wide range of terms are used when describing and discussing risk issues. Two words closely related to risk are *hazard* and *uncertainty*. The IEC (1995) defines hazard as *source of potential harm or a situation with a potential of harm*. Consequently, hazard does not include any information about probability, while risk includes the hazard as well as the probability of occurrence. Burgman (2005) emphasises that the conversion of hazard assessment to risk assessment involves a probabilistic element, i.e. the probability of the hazard having an effect is assessed. The distinction between risk and uncertainty is discussed by Kaplan and Garrick (1981). They conclude that risk involves both uncertainty and some kind of loss or damage, while uncertainty alone can be related to something positive, e.g. a lottery prize.

The word *risk* is used in different ways, with different meanings. It is therefore important to state clearly what one means when using the word *risk*. In this thesis

risk is used based on the definition presented by Kaplan and Garrick (1981). Consequently, both the probability and consequence are taken into consideration.

2.2 Uncertainty

It has already been stated that risk is a combination of probability and consequence. However, as pointed out by e.g. Kaplan and Garrick (1981), a single number is not a big enough concept to communicate the idea of risk. A probabilistic approach should thus be applied where uncertainties of estimates are taken into account instead of relying solely on point estimations. In some sense one may argue that the probability part of risk is an expression of uncertainty. However, what Kaplan and Garrick (1981) refer to is uncertainties about the probability and consequence values, or other variable used to express risk. Different sources of uncertainty exist and typically, uncertainties due to natural variation (aleatory uncertainty) and lack of knowledge (epistemic uncertainty) are discussed (Aven, 2003; Back, 2006; Norrman, 2004). Uncertainties may be included in risk analysis in different ways (Paté-Cornell, 1996). Point estimates, for example, can be replaced by probability distributions to describe uncertainties in variables.

A Bayesian approach is also commonly applied in risk analyses (Bedford and Cooke, 2001; Kaplan, 1994). 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 part of risk analyses (Section 5.2).

2.3 Reasons for managing risk

The obvious reason for managing risk is to protect us from some kind of harm. The IEC (1995) emphasises that the objective of risk management is to control, prevent or reduce loss of life, illness, injury, damage to property and consequential loss, and environmental impact. Kaplan and Garrick (1981) point out that we are not able in life to avoid risk but only to choose between risks. Since we cannot eliminate all risks and create a totally risk-free society, we need to make proper decisions in order to achieve an acceptable level of risk. Hence, efficient risk management is of primary importance to enable good decision-making aimed at achieving an acceptable level of risk.

In the Australian/New Zealand standard on risk management (AZ/NZS, 2004), it is stated that risk management is about achieving an appropriate balance between realising opportunities for gains while minimising losses. Hence, it should be emphasised that risk management not only protects us from harm but also creates opportunities. If a risk is unknown this might restrain us from performing a specific project. If the risk is instead analysed and understood, if necessary also reduced or controlled, it might be possible to perform the project.

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. This example shows that if risk is managed efficiently it is possible to choose proper risk-reduction options and reduce the cost arising from, for example, over-design. This facilitates an efficient use of available resources.

2.4 The risk management process

The overall process of identifying hazards, estimating risk, evaluating risk and, if necessary, reducing or controlling risk, is often referred to as risk management. Figure 2.1 shows an outline of the risk management process as presented by the IEC (1995). It should be noted that the description of risk management varies depending on the type of risk and context, e.g. pure technological risks or risks to human health. The use of different terms may also vary slightly. Although some differences can be found in the literature regarding the presentation and outline of the risk management process, there is a rather strong consensus regarding its major contents. The risk management process includes the entire process from the initial description of scope and purpose of risk management, the identification of hazards and the estimation of risks, through the evaluation of risk acceptance and identification of possible risk-reduction options, to the selection, implementation and monitoring of appropriate reduction measures.

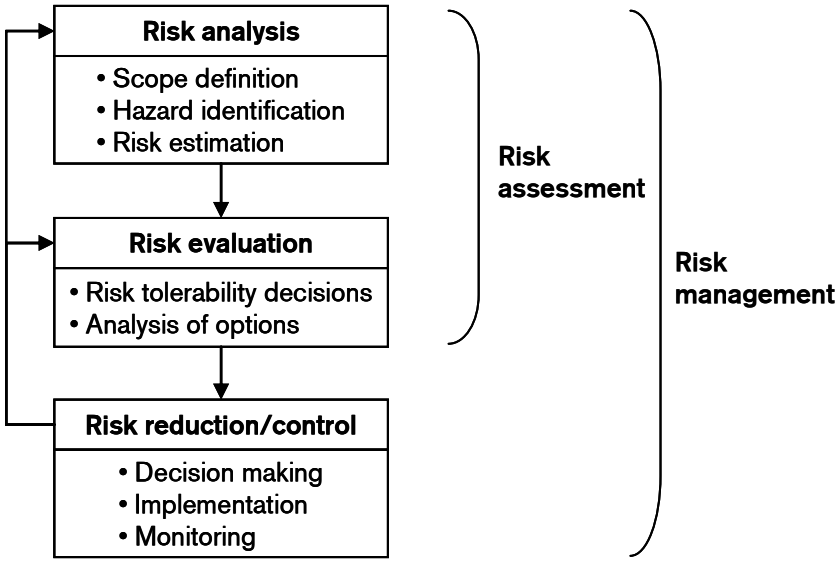

Figure 2.1. The risk management process according to the IEC (1995).

The main purpose of the risk analysis step is to provide information for the subsequent risk evaluation. When the risk has been evaluated, including possible risk-reduction options, decisions are made in the final step – risk reduction/control. The analysis and evaluation part is together often referred to as risk assessment. An important element of risk management is that it is an iterative process of continuous updating as new information becomes available and as conditions change. This is indicated in Figure 2.1 by the feedback arrows. To further explain risk management and its different parts, definitions of terms related to risk management are presented in Table 2.1.

An important aspect when managing risk is risk communication, i.e. the exchange or sharing of information regarding risk. Risk and related aspects need to be communicated between decision-makers, scientists, the general public and present or potential stakeholders. The importance of risk communication and taking into account the world around us as part of risk management is emphasised by, for example, the Swedish Rescue Services Agency (Davidsson *et al.*, 2003), see also Owen *et al.* (1999).

Table 2.1. Definitions of terms related to risk management (IEC, 1995).

Harm	Physical injury or damage to health, property or the environment.
Hazard	Source of potential harm or a situation with a potential of harm.
Hazardous event	Event which can cause harm.
Hazard identification	Process of recognising that a hazard exists and defining its characteristics.
Risk	Combination of the frequency, or probability, of occurrence and the consequence of a specified hazardous event.
Risk analysis	Systematic use of available information to identify hazards and to estimate the risk to individuals or populations, property or the environment.
Risk assessment	Overall process of risk analysis and risk evaluation.
Risk control	Process of decision-making for managing and/or reducing risk; its implementation, enforcement and re-evaluation from time to time, using the result of risk assessment as one input.
Risk estimation	Process used to produce a measure of the level of risk being analysed. Risk estimation consists of the following steps: frequency analysis, consequence analysis and their integration.
Risk evaluation	Process in which judgements are made on the tolerability of the risk on the basis of risk analysis and taking into account factors such as socio-economic and environmental aspects.
Risk management	Systematic application of management policies, procedures and practices to the task of analysing, evaluating and controlling risk.

2.5 Risk analysis

As stated in the above section, information and knowledge obtained from a risk analysis should enable evaluation of risk and possible options for risk reduction. Based on the definition of risk presented by Kaplan and Gerrick (1981), the aim of risk analysis can be described as providing information on scenarios, probabilities and consequences (e.g. Davidsson *et al.*, 2003).

The process of risk analysis is presented in Figure 2.2, including the main steps *scope definition*, *hazard identification* and *risk estimation*. Depending on what kind of system and risk is considered, the analysis process may vary. It should also be noted that a risk analysis can be either qualitative or quantitative, depending on its purpose (see Section 4.3). The analysis may also be a combination of quantitative and qualitative and may then be named semi-quantitative. The basis for qualitative and quantitative risk analysis is described further in Section 4.3.

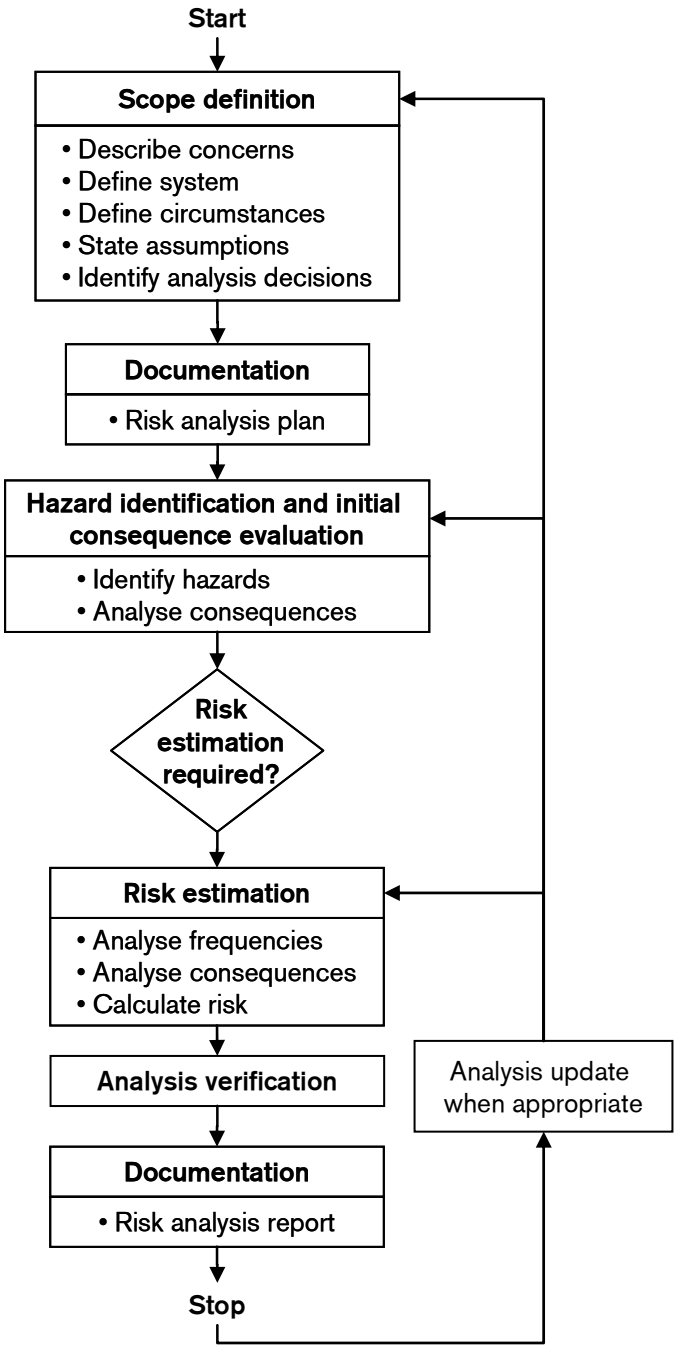

Figure 2.2. Risk analysis according to the IEC (1995).

The entire risk management should be an iterative process and consequently should a risk analysis also be continuously updated as new information becomes available. An important part of the risk analysis is to choose what type of consequences to include and to decide which measures to use. Slovic (2001) emphasises that the choice of risk measure can affect how risky a particular form of technology appears.

3 DRINKING WATER AND RISK

This chapter provides an introduction to drinking water systems and presents possible risks and existing approaches to managing risks to drinking water systems. There is also a presentation of the reasons for managing risks to drinking water systems and measures for expressing risk.

3.1 Drinking water systems

The structure and function of drinking water systems varies depending on, for example, natural conditions, water demand and available economic resources. Although differences exist, drinking water systems are commonly described as supply chains built up by three main sub-systems: raw water, treatment and distribution. Together these sub-systems cover the entire supply chain, from the raw water source through the treatment plant and distribution network to the consumers' taps.

Raw water sources can be groundwater, surface water or a combination of these (HDR Engineering, 2001). When natural groundwater resources are limited, artificial recharge is sometimes used in order to produce water similar to natural groundwater (see e.g. Fetter, 2001). In areas where water resources are scarce, treated wastewater may be reclaimed by groundwater recharge or used directly to produce drinking water. The European Commission is funding an ongoing research project named Reclaim Water (contract no. 018309), focused on reclamation technologies for safe artificial groundwater recharge.

The main difference between groundwater and surface water in drinking water production is in general the quality; groundwater often requires less treatment than surface water (Gray, 2005). Since clean raw water does not need the same degree of treatment as water of poor quality, it is often the case that fewer treatment steps are required when using groundwater compared to surface water.

According to Gray (2005) the objective of water treatment is to produce an adequate and continuous supply of water that is chemically, bacteriologically and aesthetically acceptable. However, the water should be completely safe microbiologically and not just bacteriologically. In addition to pathogenic

bacteria viruses, protozoa and other biological contaminants also pose a severe risk to human health related to drinking water. In order to supply consumers with drinking water that fulfils these requirements, a series of treatment steps needs to be designed and used based on the raw water quality and water demand.

To distribute water from the treatment plant to the consumers an extensive network of pipes is required. This network also includes pumps and service reservoirs needed to manage variations in water demand and to ensure adequate hydraulic pressure in the service areas.

Although the basic principles are similar for all drinking water systems, the detailed construction varies depending on local conditions. Figure 3.1 shows a flowchart including common components of a drinking water system and the connection between these components. Different water sources as well as different treatment and distribution alternatives are illustrated in the flowchart. Although the flowchart does not include all possible components it does illustrate a generic structure.

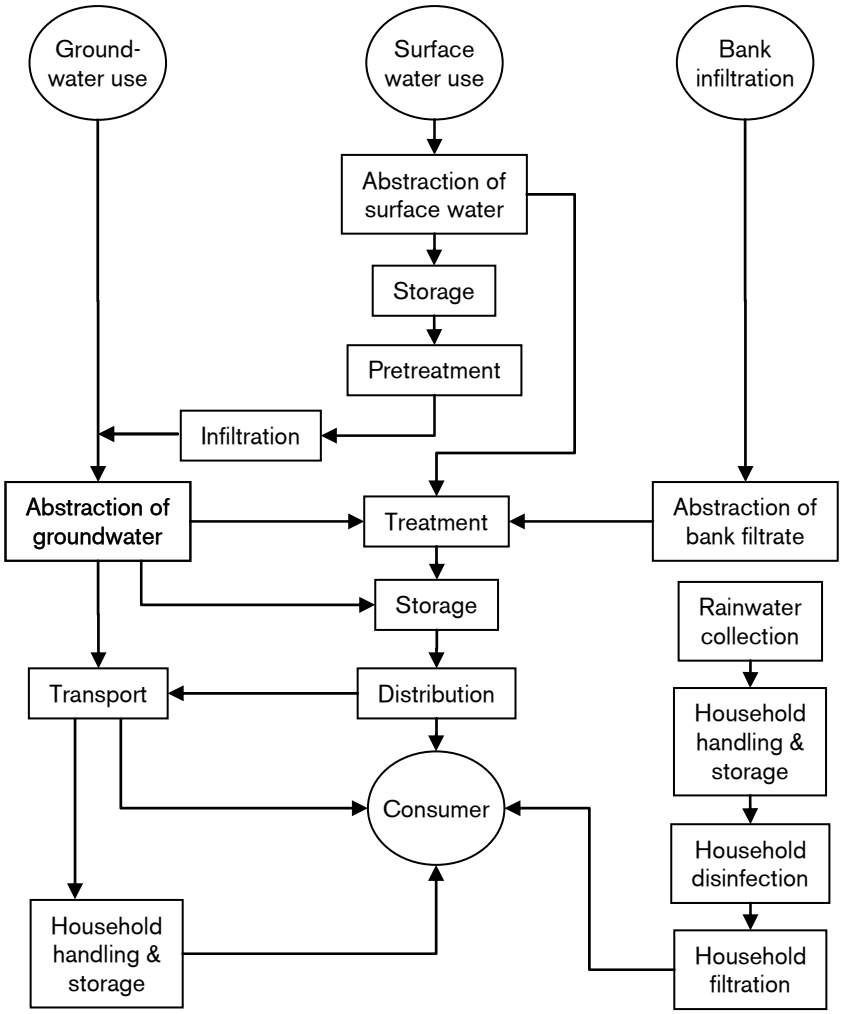

Figure 3.1. *Flowchart illustrating different main components of drinking water systems and their interconnections (Davison et al., 2005).*

3.2 Risks to drinking water systems

As described in Section 3.1 a drinking water system is composed of a large number of components. All components may be affected by different events and consequently a large number of events may occur with potential harm to the supply of drinking water (Beuken *et al.*, 2007; Nadebaum *et al.*, 2004; Olofsson *et al.*, 2001). Hence, these possible hazardous events pose a risk to the water utility and in the end to the public at large.

Hazards categories

The risk sources, i.e. hazards, can be categorised and structured in many ways. The objectives of water treatment presented by Gray (2005) can be categorised as quantity- or quality-related (Section 3.1). The quantity objective corresponds to a continuous, i.e. reliable, supply of water and the quality objective reflects the requirement that the water should be qualitatively acceptable. Based on these objectives hazards can also be categorised as quantity- or quality-related, depending on which objective a specific hazard may threaten. Quantity-related hazards may cause water shortage while quality-related hazards may cause unacceptable water quality. Interruption in the delivery of drinking water to the consumers may, for example, occur due to pipe breakage, pump failure, power failure or limited access to raw water. Events causing unacceptable water quality may, for example, be accidents with hazardous goods contaminating the source water, failing treatment processes or intrusion in the distribution system of contaminated water from the surrounding soil profile. The WHO (2004) emphasises that the most common and widespread health risk associated with drinking water is related to microbial contamination, primarily ingestion of water contaminated with human or animal faeces. Events may of course affect both the quantity and quality of water. Contamination of a water source, for example, obviously affects the water quality but in the end water shortage may arise due to the fact that no alternative water source exists.

The hazard categories described above are mainly focused on the effects the consumers may experience. If additional factors are included several other categories may be formulated. Pollard *et al.* (2004) describe the following six categories of risk important to the drinking water sector:

1. *Financial risk* – Associated with the financial operation and management of the business, both internal and external.
2. *Commercial risk* – Arising from competition and a demanding public.
3. *Public health risk* – Source contamination, human error and mechanical failure are some examples of how the water may be contaminated and pose a risk to public health.
4. *Environmental risk* – Environmental impact may arise as a consequence of equipment failure or human error, e.g. discharge of polluted water.
5. *Reputation risk* – Losing the confidence of the consumers.
6. *Compliance/legal risk* – Associated with failing to comply with legislation and uncertainties regarding future legislation.

Ezell *et al.* (2000) describe the communities' drinking water supplies as one key element of a nation's infrastructure and point out the following as factors posing a risk to such infrastructure: growing consumption by expanding populations; industrial and public pollution; tragedies caused by both natural and human accidents; and emergence of threats by domestic terrorists, disgruntled employees and computer hackers. To support water utilities when identifying hazards, checklists including hazardous events are provided by e.g. Beuken *et al.* (2007) and Nadebaum *et al.* (2004). The catalogue of hazards provided by Beuken *et al.* (2007) is based on existing national checklists and databases and lists events that may harm the supply of safe drinking water. The events that may affect the water quality negatively are associated with biological, chemical, radiological or physical agents. Events related to the availability of water, safety of personnel and external harm to third parties are also included.

Future hazards

An important part of risk management is to learn from earlier events, both accidents that have occurred and near-accidents. As has already been pointed out, risk management is based on a proactive approach and consequently non-occurred events also need to be identified. Some of these events may be seen as future hazards but, on the other hand, all events that have not occurred should accordingly not be considered as future hazards. Rosén and Lindhe (2007) state that future risks may arise as a consequence of different changes that have a direct or indirect effect on the drinking water system. Examples of such changes may be climate changes and a change in human activity in the catchment area.

As the rest of society is affected by different trends so also the drinking water sector. In recent years trends such as increased awareness of microbial pollutants, emergence of membrane filtration and privatisation of water works in some areas can be identified. Pollard *et al.* (2004) point out the following six factors endangering the drinking water sector and posing new risks as well as opportunities: privatisation, sector globalisation, increased competition, emerging technologies, increasingly stringent regulatory control and the trend towards financial self-sufficiency.

Based on a literature review, interviews and evaluation work carried out at Chalmers University of Technology, Rosén and Lindhe (2007) identified the following seven factors that pose potential risks to drinking water systems in the future:

- Sabotage and terrorist attacks
- Conflicts
- New chemicals
- Emerging pathogens
- Public concern
- Climate changes
- Technical failures in aging distribution systems

Trends affecting the drinking water sector, possible implications and coping strategies are also described by the Awwa (American Water Works Association) Research Foundation (AwwaRF, 2006), see also Segrave *et al.* (2007). As with all risks, future risks require a proactive approach. Rosén and Lindhe (2007) conclude that major challenges for the future risk management of drinking water systems include how to perform reliable and useful risk analysis, how to communicate the risks and how to evaluate risks in order to use available resources efficiently and sustainably.

3.3 Risk management in the drinking water sector

The WHO (2004) 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 International Water Association (IWA, 2004) emphasises that a reliable supply of safe drinking water is fundamental to public health and economic development. As presented in Section 3.2 many events may occur, harming the supply of safe drinking water. Risk management is therefore very important in the drinking water sector. The WHO (2004) concludes that a comprehensive risk assessment and risk management approach is the most effective way of ensuring the safety of a drinking water supply.

The drinking water sector faces risks as well as opportunities. At the same time, governments and regulators expect water utilities to adopt a management approach that focuses on avoiding losses and taking advantage of opportunities (Dalgleish and Cooper, 2005). Pollard *et al.* (2004) suggests that an enterprise-wide management approach should be used, which requires:

- integrated frameworks for the management of internal as well as external risks to the utility;
- support of board level, executive management and operational staff as well as that of external stakeholders; and
- effective communication of risk and engagement within decision-making processes both within companies and with external stakeholders.

Risks can be managed on different levels in an organisation depending on what kind of decision needs to be made. The different levels can be described as *strategic*, *programme* and *operational* (MacGillivray *et al.*, 2006; Pollard *et al.*, 2004). 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.

According to Pollard *et al.* (2004) the drinking water sector is formalising and making explicit approaches to risk management and decision-making that were formerly 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 focused on treatment plant design and operation (Hrudey *et al.*, 2006). One example is the increased use of the Hazard Analysis and Critical Control Point (HACCP) approach within the drinking water sector (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). Principles and concepts of the HACCP approach in particular have been used by the WHO to develop the Water Safety Plan (WSP) approach (WHO, 2004), which is currently being implemented in many countries. WSP and HACCP are described further in Section 3.4. 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 the 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.

End-product testing

Risk management is a proactive way of working. This means that efforts are made to prevent risks from arising or reduce them to an acceptable level. The opposite way of working is to only work reactively, which means that action will be taken after an event has happened and not before. An example of a reactive way of working is if end-product testing (compliance monitoring) alone is used to monitor and guarantee a safe water quality. Although end-product testing is a necessary part of water quality management, it cannot be used as the only means of guaranteeing safe drinking water (e.g. WHO, 2004). Note that the Drinking Water Directive (Council of the European Union, 1998) is based on end-product testing. The Federal-Provincial-Territorial Committee on Drinking Water and the Canadian Council of Ministers of the Environment (CDW/CCME, 2004) address the limited number of pathogens and contaminants that can be analysed and the time it takes to complete analyses, as weaknesses of end-product testing (see also 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 safety water quality. If unacceptable water quality is detected in the drinking water distributed to the taps, some consumers will at least use the water before the analysis is completed and corrective action has been taken. End-product testing should be used as one tool for verifying that the water is/was safe to drink but not as the only means of guaranteeing safe drinking water.

The multi-barrier approach

Instead of relying on end-product testing to guarantee safe drinking water, the use of a multi-barrier approach is advocated by e.g. the WHO (2004) and the CDW/CCME (2004). 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 form causing any unacceptable harm. Since multiple barriers are used, failure of one or more barriers can be compensated for by the others. The CDW/CCME illustrate the multi-barrier approach as shown in Figure 3.2. The figure shows different components of the multi-barrier approach and emphasises that it is not only the treatment plants that should include barriers. Protection of source waters and

distribution systems, as well as overall management, are important to achieve an efficient multi-barrier approach.

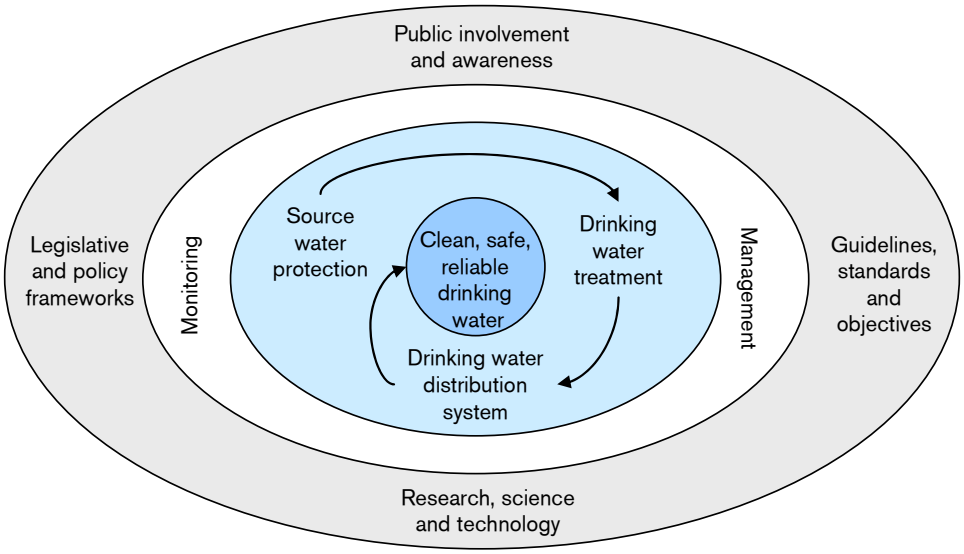

Figure 3.2. *Different components of the multi-barrier approach, according to the CDW/CMME (2004).*

3.4 Frameworks and guidelines

A number of different international and national frameworks and guidelines for managing risks to drinking water systems exist. In this section some of the most well-known frameworks and guidelines are briefly described and general trends are summarised.

Water Safety Plans

In the 3rd edition of the *Guidelines for Safe Drinking-water Quality*, the WHO presented a *framework for safe drinking water* (WHO, 2004). The framework consists of health-based targets, Water Safety Plan (WSPs) and independent surveillance (Figure 3.3). The health-based targets should be based on evaluation of health concerns by a high-level authority and reflect what is considered to be an acceptable level of risk. As noted in Section 3.3, the WHO (2004) 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*. The health-based targets are supposed to guide the WSPs and the independent surveillance aims to ensure the work is performed properly and also promotes improvement. The surveillance should be conducted by an independent agency

and include all aspects of safety. The WSPs are a key element in the framework and include *system assessment*, *operational monitoring* and *management plans* (Figure 3.3). The purpose of the system assessment is to determine whether the system is capable of delivering water that meets the health-based targets. The system assessment should include the entire system and consider interactions between elements. Operational monitoring should assess control measures in order to ensure that the system is operating properly. The management plans aim to document and communicate relevant information. To develop a WSP a number of different steps need to be performed. The main steps are presented in Figure 3.4.

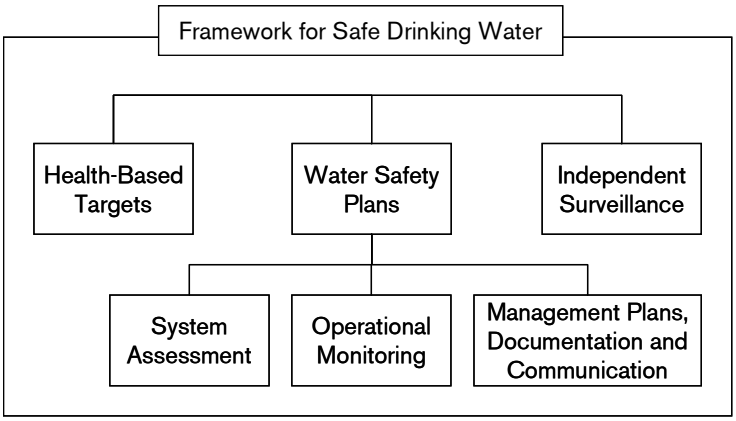

Figure 3.3. The framework for safe drinking water as presented by Davison et al. (2005).

The WSP approach is based on an integrated approach, i.e. the entire system from catchment to consumer should be considered, and includes principles and concepts from the multi-barrier approach and the Hazard Analysis and Critical Control Point (HACCP) system (described further below). WSPs are currently being implemented in countries around the world and are thus an important part of risk management of drinking water systems (Breach and Williams, 2006; Garzon, 2006; McCann, 2005; Vieira, 2007). In October 2008, the WHO will publish a manual aimed at providing practical guidance to facilitate WSP development.

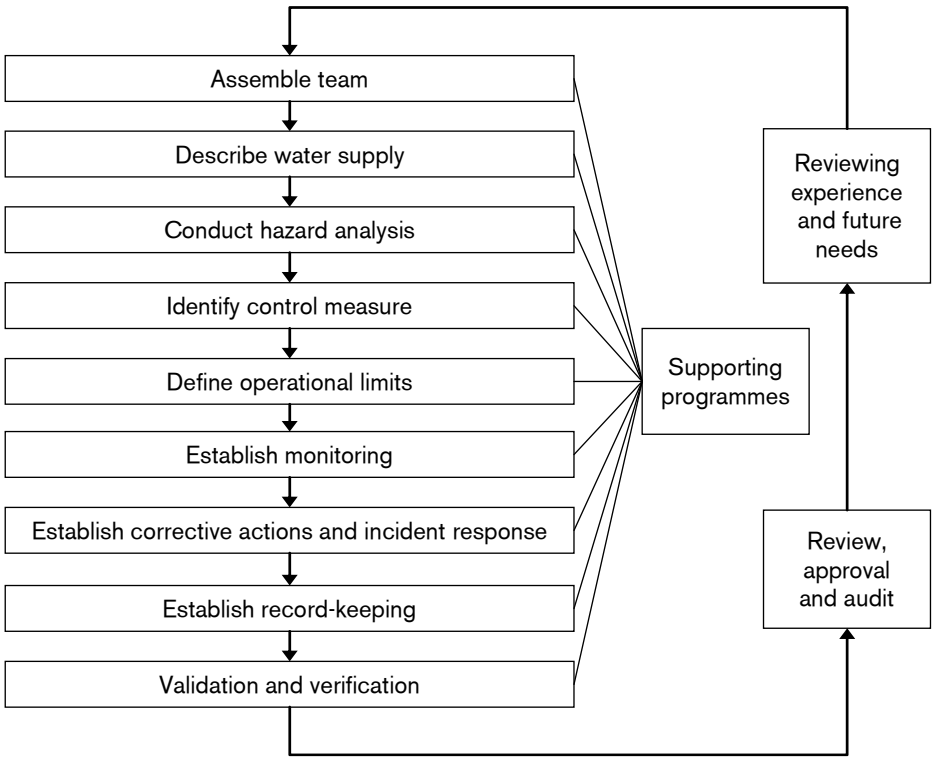

Figure 3.4. Key steps in developing a WSP (after Davison et al., 2005).

The Bonn Charter

The Bonn Charter for Safe Drinking Water (IWA, 2004) is a complementary document to the guidelines provided by the WHO (2004) 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. Institutional roles and responsibilities are also described and the goal of the Bonn Charter is stated to be *good safe drinking water that has the trust of consumers*. Furthermore, it is emphasised that drinking water should not only be safe to drink but also be of aesthetically good quality.

Hazard Analysis and Critical Control Point

The Hazard Analysis and Critical Control Point (HACCP) system can be described as a systematic way of identifying specific hazards and measures for their control (Codex, 2003). Since principles of HACCP have been included in the WSP approach, the two approaches have several similarities. Basically, the HACCP approach aims to identify hazards and for each hazard identify control measures, including points in the system where the hazard may be controlled, critical limits, monitoring and corrective actions. The Pillsbury Company

compiled the HACCP system in 1960 to assure food safety when delivering food to the NASA space programme. Although traditionally used in the food industry, Havelaar (1994) presented the first application of HACCP to drinking water supplies. Hrudey (2004) and the Australian National Health and Medical Research Council and Natural Resource Management Ministerial Council (NHMRC/NRMMC, 2004) point out that HACCP is most suitable to apply in the treatment part of a drinking water system, and not applied as easily to the important areas of source water and distribution system (see also Hamilton *et al.*, 2006).

Examples of national guidelines

In addition to international guidelines, such as those of the WHO (2004), some nations have compiled their own guidelines and frameworks. The Australian Drinking Water Guidelines (ADWG) for example, include a framework for management of drinking water quality (NHMRC/NRMMC, 2004). Rizak *et al.* (2003) describe the ADWG framework as a comprehensive and preventive strategy from catchment to consumer, see also Nadebaum *et al.* (2003). The framework constitutes four main areas: *commitment to drinking water quality management*, *system analysis and management*, *supporting requirements* and *review*. The framework provided by the NHMRC/NRMMC (2004) and the one provided by the WHO (2004) is to a large extent similar. The primary differences are mainly related to the outline and presentation of the frameworks.

In New Zealand the use of Public Health Risk Management Plans (PHRMPs) is suggested by the Ministry of Health (2005a; 2005b). The PHRMP is described as a tool that will aid water utilities identify, manage and minimise events that could cause water quality to deteriorate. Compared to the guidance on the WSP approach (Davison *et al.*, 2005; WHO, 2004) the documents provided by the Ministry of Health in New Zealand include more detailed guidance on how to prepare a PHRMP. There are also other national guidelines provided by, for example, the Swedish Water and Wastewater Association (SWWA, 2007), the Swedish National Food Administration (SNFA, 2007), the Danish Water and Wastewater Association (DWWA, 2006) and the Norwegian Food Safety Authority (NFSA, 2006). These guidelines are not described further here.

General trends

By comparing different international and national frameworks and guidelines the following general trends can be identified:

- The weaknesses of end-product testing is emphasised as a main reason why risk management of drinking water systems is important.
- The from source to tap approach, or even more comprehensively from catchment to consumer, is advocated in the guidelines as an important basis for managing drinking water systems.
- The multi-barrier approach is stressed as a key strategy to guarantee safe drinking water.
- Existing frameworks and guidelines are mainly focused on water quality issues. Limited guidance is provided on aspects related to water availability and reliability of water supplies.
- The importance of having good knowledge of the system (i.e. *to know the system*) is emphasised as being fundamental when analysing a drinking water system.
- Co-operation between stakeholders is pointed out as being important if drinking water systems are to be managed efficiently.

3.5 Risk measures

The concept of risk is viewed differently in different fields and depending on the purpose and context, risk may be expressed using different measures, i.e. units (see e.g. Aven, 2003). In Section 2.1 risk was described as a combination of the probability, or frequency, and consequence of a hazardous event. However, sometimes only the probability is considered and in other cases the main focus may be on the consequences. When carrying out a Quantitative Microbial Risk Assessment (QMRA, see Section 4.3) for example, risk is expressed as the probability of infection and when analysing distribution systems the probability of pipe breakage may be studied. However, it is also possible to combine the probability of infection and the probability of pipe breakage with the actual consequences. The results from a QMRA may, for example, be combined with information on health effects in order to estimate the risk as Disability Adjusted Life Years (DALY), see e.g. Havelaar and Melse (2003). DALY is a health gap measure that includes both years lost due to premature mortality and years lost due to some degree of disability during a period of time (Homedes, 1996). One DALY represents loss of one year of full health and the WHO (2004) states the use of a reference level of 10^{-6} DALYs per person per year for the drinking water guidelines (WHO, 2004).

Risk measures that can be used to combine different consequences are useful, since hazardous events may have multiple consequences. DALY is an example of a measure that combines different health effects. Another way to combine different consequences is to translate them into monetary units. This facilitates economic analyses such as cost-benefit and cost-effectiveness analysis. It should be noted that it may be controversial to translate health effects and other consequences to monetary units.

When analysing risks to drinking water systems the choice of risk measure is influenced by different factors. If, for example, a hazardous event causing the water source to become polluted is analysed, different measures will be implemented if the actual health effects are to be estimated or the results are to be compared with a threshold value for raw water quality. The point of compliance, i.e. the point in the system where criteria are defined, is thus one of the factors that influence the choice of risk measure. Since risk is expressed using different measures it is important in a risk analysis to clearly define how risk is expressed and to be aware that different measures are used.

4 INTEGRATED RISK ANALYSIS OF DRINKING WATER SYSTEMS

In this chapter the integrated approach to analysing and managing risks to drinking water systems is presented. Based on Chapters 1 and 3, a framework for integrated risk management of drinking water systems is suggested. Principles of qualitative and quantitative risk analysis are also presented.

4.1 The from source to tap approach

In Section 3.2 it was concluded that since drinking water systems are extensive and composed of many different components, a wide range of events may affect them and cause harm. Hence, as stated in the Australian guidelines on drinking water, efficient management of drinking water systems requires that consideration be taken to the entire supply chain (NHMRC/NRMMC, 2004). This means that all parts, from source to tap, or even more comprehensively from catchment to consumer, should be considered. This integrated approach is also emphasised by, for example, the WHO (2004) as part of the WSP approach, the IWA (2004) in the Bonn Charter and the CDW/CCME (2004) in their guidance on the multi-barrier approach.

There are several reasons why an integrated *from source to tap approach* should be applied, not only as an overall management approach but also when making risk analyses. Although a drinking water system may appear to have a simple structure it is often complex. A system can be described as a supply chain composed of a raw water source, treatment plant and distribution system, but there is an interaction between these sub-systems that needs to be considered. This means, for example, that events at the water source may affect the treatment and distribution. A drinking water system also has an inherent redundancy, which means it may compensate for failures. Failure of a pump in the distribution system, for example, may not affect the delivery to the consumers as there are reserve pumps. Unacceptable raw water quality may also 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. Hence, a drinking water system cannot be

described as a traditional series system where failure in one part automatically leads to failure of the whole system.

Based on the above description it can be concluded that overall risk management as well as risk analyses need to consider the entire system in order to be efficient. Integrated risk analysis facilitates minimisation of sub-optimisation of risk-reduction options and, consequently, 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 options. It might be more efficient to implement risk-reduction options to protect the water source or spend money on maintenance and upgrading the distribution network. Although integrated risk analyses are important, it should be noted that analyses of specific parts of the system as well as specific hazardous events are also important and cannot be replaced by one integrated analysis. The different types of analysis should complement each other to facilitate efficient risk management.

4.2 A suggested risk management framework

Background to the framework

Risk analysis is a key component in risk management. To show clearly the role of risk analysis in the management of drinking water systems, this section presents a suggested framework for integrated risk management in Water Safety Plans (WSPs). This framework is developed by the author and colleagues within Work Area 4 *Risk Assessment and Risk Management* of the Techneau project (Techneau, 2005). Techneau is a project funded by the European Commission under the Sixth Framework Programme (contract no. 018320). The framework is described further by Rosén *et al.* (2007) and includes a generic outline of the framework as well as supporting methods, tools and examples developed within Techneau. In this section only the generic outline is presented (see also Rosén *et al.*, 2008b).

Comparison of two approaches

The WSP approach (Section 3.4) is comprehensive and provides increased awareness and understanding of risk issues related to drinking water systems. The approach includes principles of HACCP and the multi-barrier approach, and emphasises the importance of considering the entire supply chain, from source to tap. When comparing the WSP approach (Figure 3.4 in Section 3.4) with the

more generic risk management process (Figure 2.1 in Section 2.4), similarities as well as differences can be identified. The WSP approach has been developed for a specific field of application (drinking water) while the risk management process is generic and should be suitable for a wide range of applications. By comparing the outlines of the WSP approach (Figure 3.4) and the risk management process (Figure 2.1) the following main observations were made:

- The importance of defining the scope is emphasised more clearly in the risk management process while the WSP approach place more emphasis on putting together a team of people to support the work.
- In contrast to the WSP approach the risk management process does not include a step that states explicitly that the system should be described. However, since the risk management process is more generic the system description step is part of the scope definition, which is shown in Figure 2.2 in Section 2.5. Figure 2.2 provides a more detailed description of how to carry out a risk analysis.
- In the WSP approach a step termed hazard analysis is included. The risk management framework distinguishes between hazard identification and the subsequent risk estimation.
- The risk management process includes a risk tolerability decision (acceptable risk), which is not a separate part in the WSP approach. Since WSPs are guided by health-based targets, these are intended to define what is an acceptable risk.
- Identification of control measures and definition of operational limits are steps included in the WSP approach. Within the risk management process these steps are not presented separately but are part of the step termed analysis of options.
- The risk management process illustrates decision-making as a separate step, while in the WSP approach this appears to be included in the other steps.
- The WSP approach includes monitoring, corrective action, record-keeping as well as validation and verification. In the risk management process the corresponding steps are termed implementation and monitoring.
- The WSP approach clearly points out the importance of supporting programmes linked to all steps, from assembling the team through to validation and verification. Furthermore, both the WSP approach and the

risk management process indicate that the work should be performed iteratively, i.e. be updated continuously.

The framework

The main reason for the differences between the WSP approach and the risk management process is the fact that the latter is generic while the former has a specific, intended use. The fact that WSPs are focused mainly on water quality issues also explains why some generic parts of risk management are not included in the WSP approach. However, risk management of drinking water systems needs to consider all risks on a strategic as well as operational level. To illustrate a generic approach to risk management of drinking water systems a framework based on the risk management process and the WSP approach has been developed and is presented in Figure 4.1.

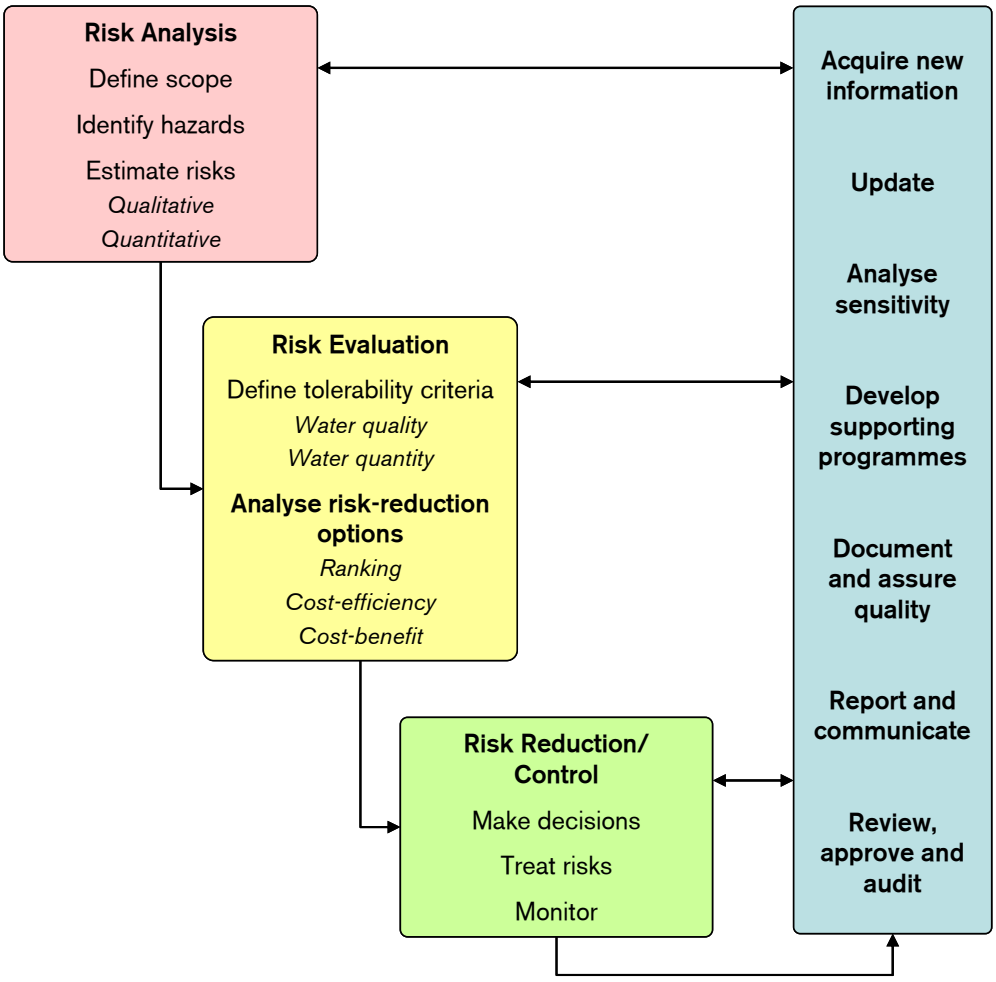

Figure 4.1. *Schematic illustration of a framework for integrated risk management in WSP (after Rosén et al., 2007).*

The overall structure of the framework (Figure 4.1) is based entirely on the risk management process but has been updated with important aspects of the WSP approach to link it more clearly to drinking water systems. The framework comprises three main parts: *risk analysis*, *risk evaluation* and *risk reduction/control*. However, important tasks such as review, communication, collection of new information and updating are also emphasised in the framework.

The first part of the framework is risk analysis, which starts with an initial scope definition. Defining the scope is important in order to set the basis for the risk analysis. It should include a definition and description of the system as well as descriptions of concerns, assumptions and required output to support decision-making. As clearly pointed out in the WSP approach, a team of people should be put together to support the risk analysis. The team should include people with knowledge of the system being analysed as well as people with knowledge of risk analysis. Together the team should have sufficient knowledge to perform the analysis. Once the scope has been defined, hazards should be identified and the risk estimated. The risk analysis can be qualitative or quantitative, depending on its purpose (see Section 4.3).

The output from the risk analysis should be used as input in the risk evaluation. To enable risk evaluation, tolerability criteria defining an acceptable level of risk are needed. The WSP approach includes health-based targets related to the water quality. However, targets related to water quantity and other stakeholder values are also needed in order to evaluate all the risks. Efficient risk management of drinking water systems must include risks related to both quantity and quality problems. If the risk is not acceptable, it needs to be reduced and/or controlled. Alternative options for risk reduction should be identified and evaluated by means of, for example, cost-effectiveness or cost-benefit analyses.

Based on the information from the risk analysis and risk evaluation (together termed risk assessment) decisions are made and implemented. This means that if considered necessary the risk is handled by, for example, lowering the probability of occurrence, reducing the consequence, or both. To evaluate the efficiency of the implemented safety measure monitoring may be used. The information from monitoring and reporting systems as well as other information sources should be used to update the risk analysis and the risk evaluation.

In addition to the analysis, evaluation and reduction/control steps, the framework in Figure 4.1 emphasises the importance of analysing and considering

uncertainties related to all steps. Furthermore, supporting programmes, documentation, communication and review are highlighted as important tasks.

Objectives of the framework

The purpose of the framework is to provide a structure and toolbox to assist water utilities in their risk management work. In this thesis the structure is presented above and one of the tools developed is presented in Section 5. The framework supports integrated risk management in WSPs and facilitates transparency and rational decision-making. The framework stresses the importance of an iterative process of continuous updating as new information becomes available and as conditions change. Communication between stakeholders is emphasised as important since it facilitates increased awareness and knowledge regarding risk issues among, for example, decision-makers, water utility personnel and the generic public. Furthermore, the framework includes methods and tools to assist hazard identification, risk estimation and evaluation in order to provide cost-effective and sustainable prioritisation of safety measures (Rosén *et al.*, 2007).

4.3 Principles of qualitative and quantitative risk analysis

In Section 2.5 the basis of risk analysis is presented and an overview of the tasks that are normally carried out is shown in Figure 2.2. Irrespective of whether a risk analysis is quantitative or qualitative, some tasks always need to be carried out. It is important, for example, to define the scope and clearly state the purpose of the analysis. This should also be linked to the type of decision situations the analysis is supposed to support. Furthermore, identification of hazards is always required regardless of whether the subsequent part of the analysis is qualitative or quantitative. In order to identify relevant hazards it is important to define and understand the system being analysed, e.g. a drinking water system. A system description is thus required and may be combined with a conceptual model describing how hazards may occur and cause harm to a receptor (Figure 4.2). The receptor may, for example, be the consumers supplied with drinking water or something else that should be protected. The term pathway is used to describe how the hazard may overcome possible barriers and affect the receptor. A hazard could be a microbial contaminant that enters a drinking water system through faecal contamination of the water source. For the contaminant to harm the consumer it needs to pass barriers in, for example, the treatment plant.

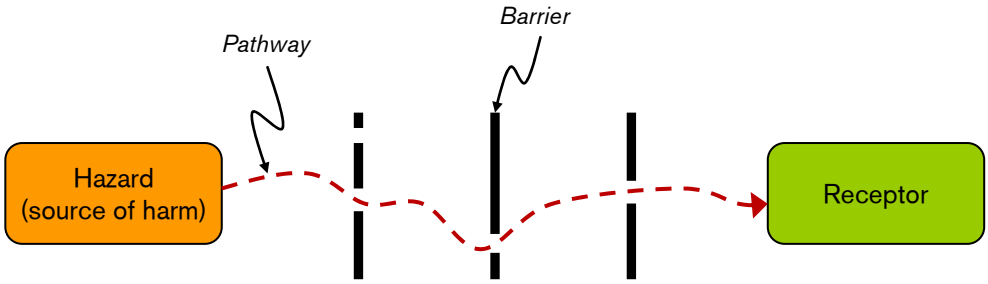

Figure 4.2. *Conceptual model illustrating how a hazard may cause harm to a receptor if existing barriers are unable to prevent a pathway between them.*

To support hazard identification, experience from the past, brainstorming, checklists and more structured methods such as *What if* analysis and Hazard and Operability Analysis (HAZOP) can be used (see e.g. Hokstad *et al.*, 2008; Kletz, 2001; Mannan and Lees, 2005; Nolan, 1994). To support water utilities in identifying hazards, checklists including hazardous events are provided by e.g. Beuken *et al.* (2007) and Nadebaum *et al.* (2004). The checklists should preferably be used in combination with brainstorming, experience from the past and other techniques to identify hazards relevant to the system being analysed.

Risk analysis may be performed in an almost infinite number of ways depending on the context. A simple way to distinguish between different methods is to categorise them as qualitative or quantitative. In a qualitative analysis the risk is described in words whereas a quantitative method aims to estimate the risk numerically. The term semi-quantitative is sometimes used to describe analyses that are mainly qualitative but to some extent may be seen as quantitative. In semi-quantitative analyses risk is often categorised using discrete probability and consequence scales that have been assigned numbers. In this thesis the semi-quantitative methods are also defined as qualitative.

Qualitative risk analysis

A qualitative (or semi-quantitative) method for risk analysis commonly used in different fields is risk ranking using risk matrices. The WHO (2004) suggests the use of a risk matrix to prioritise identified hazards. Table 4.1 shows an example of a risk matrix to be used in a WSP, presented by Davison *et al.* (2005). To rank risks the probability and consequence of identified hazards are estimated using discretised probability and consequence scales (Table 4.1). To determine whether the risk is acceptable or not tolerability criteria need to be defined. In Table 4.1 each combination of probability and consequence in the matrix is defined in terms of low, moderate, high or extreme risk. More than four categories can be

used. Furthermore, which of these categories of risk that can be accepted or not needs to be defined. A principle commonly used to evaluate risks which is applicable to this case is the As Low As Reasonable Practicable (ALARP) principle, see e.g. 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). Sometimes each probability and consequence scale is assigned a score (e.g. 1-5) and a risk index is calculated by multiplying the scores (semi-quantitative risk estimation).

It should be noted that the categories of probability and consequence need to be defined specifically for the system that is being analysed. Since all systems are unique and the purpose of different analyses may differ no generic definitions of scales can, or should, be defined. The combination of the probability and consequence scales in Table 4.1, for example, is not applicable to all systems. It is likely that the probability scale in most cases would have been defined to also include events that occur much more seldom than once every fifth year. Logarithmic-based probability scales are often used. The specification of which risk level the different combinations of probability and consequence refers to also needs to be made for each system being analysed. In Table 4.1 an event that causes catastrophic consequences (mortality expected from consuming water) and occurs rarely (once every five years) is considered a high risk. In other cases it is likely that this risk would have been regarded as an extreme risk, i.e. the highest risk level according to the scale in Table 4.1.

Table 4.1 *Example of a risk matrix and definitions of likelihood and severity categories to be used in risk scoring in a WSP (after Davison et al., 2005; WHO, 2004). Classes of relative risk tolerability are shown in shades of grey.*

	Severity of consequences				
Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
Almost certain	H	H	E	E	E
Likely	M	H	H	E	E
Moderate	L	M	H	E	E
Unlikely	L	L	M	H	E
Rare	L	L	M	H	H

Note: The number of categories should reflect the needs of the study.
E – Extreme risk, immediate action required; H – High risk, management attention needed;
M – Moderate risk, management responsibility must be specified; L – Low risk, management by routine procedures.

Examples of definitions of likelihood and severity categories that can be used in risk scoring

Item	**Definition**
Likelihood categories	
Almost certain	Once a day
Likely	Once a week
Moderate	Once a month
Unlikely	Once a year
Rare	Once every 5 years
Severity categories	
Catastrophic	Mortality expected from consuming water
Major	Morbidity expected from consuming water
Moderate	Major aesthetic impact possibly resulting in use of alternative but unsafe water sources
Minor	Minor aesthetic impact causing dissatisfaction but not likely to lead to use of alternative, less safe sources
Insignificant	No detectable impact

Risk ranking by means of risk matrices is easy to perform and the results are also easy to understand. Hence, this type of analysis is useful in many cases, especially as an initial risk analysis used to identify where further and more detailed studies are needed. However, the method also has limitations that requires more sophisticated methods such as quantitative methods. Burgman (2005) emphasises that risk ranking methods assume a discrete nature of hazards, although there is often a range of possible outcomes of an event. Furthermore, if events are considered separately, important chains of events are not analysed. Often combinations of two or more events may cause severe events that should be considered. Risk ranking is thus not suitable for modelling complex systems with interactions between components and events. Burgman (2005) also points out the lack of quantitative estimates of risk and the lack of procedures for uncertainty

analysis as limitations of risk ranking. Cox (2008) also discusses the limitations of risk matrices.

In addition to risk ranking using risk matrices, there are other qualitative methods applicable to drinking water systems exist. Groundwater vulnerability, for example, can be assessed using rating methods such as DRASTIC (Aller *et al.*, 1987; Rosén, 1994; 1995).

Quantitative risk analysis

The motive for performing a quantitative risk analysis, in addition to not considering interactions between events, is that a qualitative analysis is not considered to be detailed enough and cannot estimate the risk in quantitative terms. One main advantage of a quantitatively estimated risk is that it facilitates comparison with other risks and acceptable levels of risk in absolute terms. Furthermore, a quantitative method facilitates a quantitative estimate of the efficiency of risk-reduction options, which facilitates a proper evaluation of possible options. It should be noted that although an analysis is considered to be quantitative, parts of it may be qualitative. For example, initial steps such as identification and descriptions of hazards are often performed in a qualitative manner. Kaplan (1992) explains some basic ideas linked to quantitative risk analysis.

A wide range of methods and tools are available for quantitative risk analysis. Some are comprehensive with a wide field of application, describing how to identify hazards as well as how to estimate the risk, while others are used only to assist in specific parts of an analysis. The purpose here is not to present all possible methods and tools but rather to provide some examples and describe some basic concepts of quantitative risk analysis applicable to drinking water systems.

Quantitative (and qualitative) analyses differ with regard to the range of hazards included and which parts of the drinking water system are included. An analysis may focus on a specific microbial pathogen or include events affecting the water quality as well as water availability (quantity). Some analyses consider only a separate part of the system whereas others include the entire system, from source to tap.

Quantitative methods for analysing health effects of chemicals and microbial pathogens are Quantitative Chemical Risk Assessment (QCRA) and

Quantitative Microbial Risk Assessment (QMRA) respectively. The latter method is used to estimate the probability of waterborne infections through four main steps: hazard identification, dose-response assessment, exposure assessment and risk characterisation (Haas *et al.*, 1999). A QCRA is performed in a similar way to a QMRA (see e.g. Leeuwen and Vermeire, 2007). Both methods include a limited number of hazardous agents (chemicals or microbial pathogens) but may consider the entire drinking water system from source to tap. They can thus be integrated although that is not always the case.

Physical models of processes in source waters, treatment plants and distribution systems may also be used in risk analyses. In addition to the methods mentioned above, a number of other comprehensive tools are available that can assist in different ways in a risk analysis. Examples of such tools are (e.g. Hokstad *et al.*, 2008; Pollard, 2008; Rosén *et al.*, 2007):

- Fault tree analysis
- Event tree analysis
- Reliability block diagram
- Influence diagrams and Bayesian belief networks
- Markov models
- Monte Carlo simulations

As described by Kammen and Hassenzahl (2001) the ultimate goal of risk analysis is informed decision-making. Risk analysis must thus characterise risks in a fashion that incorporates identified receptors, known variability, sources and effects of uncertainty, and implications of assumptions.

5 A SUGGESTED METHOD FOR INTEGRATED AND PROBABILISTIC FAULT TREE ANALYSIS

This chapter presents a method for integrated and probabilistic risk analysis of drinking water systems. The background to the method, its application, benefits and limitations are presented.

5.1 Method development

To develop a method for integrated and probabilistic risk analysis of drinking water systems different techniques can be used as a basis. To select a proper technique for the method presented in this thesis, a set of requirements were defined. The requirements include aspects related to the outcomes of the method and its ability to model drinking water systems. The method is intended to be:

- quantitative, i.e. provide quantitative results (Section 4.2);
- integrated, i.e. include the entire system from source to tap (Section 4.1);
- probabilistic, i.e. include uncertainties of estimates (Section 2.2);
- able to estimate risk levels expressed as the expected value of Customer Minutes Lost (CML) (Section 5.2);
- able to calculate failure probabilities, failure rates or time to failure and downtimes, i.e. duration of failure (Section 5.2);
- able to model interactions between events (Section 5.2); and
- able to model a system's ability to compensate for failure (Section 5.2).

Based on the above requirements, fault tree analysis was selected as a suitable technique and is used here to develop the suggested method. As described in Section 4.2, an integrated approach is important when managing drinking water systems because of interactions between events, i.e. chains of events need to be considered, and systems may compensate for failure due to inherent redundancies. Since a fault tree provides quantitative results and aims to model interactions between events, it was natural to base the method on fault tree analysis. Furthermore, the fact that fault tree analysis is a technique that can be

easily combined with Monte Carlo simulations made it possible to apply a probabilistic approach where uncertainties of estimates (e.g. probabilities and consequences) are included.

Although the method is based on fault tree analysis, several changes needed to be made compared to how fault tree analysis is traditionally carried out. The changes were made in order to apply the method to drinking water systems and enable calculations to be made of risk levels, failure rates and downtimes. The purpose and scope of the method were discussed and decided within a group composed of researchers and personnel from the water utility in Gothenburg. These were part of a team that supported the development of the method as well as its application. The latter is described further in Section 5.3. The development and application of the method were to some extent carried out simultaneously. The drinking water system in Gothenburg was thus an important source of information when identifying conditions specific to drinking water systems and it was considered necessary that they be included in the method.

To identify how an entire drinking water system should be modelled using a fault tree, the system in Gothenburg was described and discussed thoroughly within the group of researchers and water utility personnel. The traditional fault tree technique was used as far as possible and when not applicable the need for further development was identified. New logic gates, described further in Section 5.2, were developed based on conditions that could not be modelled using the existing fault tree techniques. An example of such a condition is the inherent ability of a system to compensate for failure. It should be noted that conditions as well as main failure types to be included in the method were identified, not only based on the Gothenburg system but also in the light of aspects relevant to drinking water systems in general. While researchers as well as water utility personnel were included when discussing the function of the system and possible failures, more specific discussions on how to develop the fault tree technique and the actual development involved mainly researchers. However, during the development and when finalising the method supporting discussions were arranged involving all partners. To fulfil the requirements listed above, not only the technique on how to model a drinking water system but also how to calculate the risk and use available data have been developed further compared to the traditional fault tree technique.

To enable calculations of risk levels, consequences and probabilities needed to be included in the method. Traditionally, fault trees are used only to calculate the probability of failure. Based on analyses of available data, consideration of

suitable ways to elicit expert judgements and the fact that it would provide additional information about the system, it was decided to use the mean failure rate (or mean time to failure) and mean downtime to calculate the probability of failure. This is described further in Section 5.2.

The method developed fulfils the requirements defined above and thus provides information on how to model entire drinking water systems. A generic fault tree structure is provided together with an example of a specific application to the Gothenburg drinking water system. Equations needed to perform calculations and descriptions of how to model uncertainties are also provided.

5.2 The fault tree method

The fault tree method is presented in detail in Paper I although some of the most important parts are summarised and discussed further in this section. Fault tree analysis is a common tool in risk analyses and traditionally the aim is to calculate the probability of system failure. A fault tree is constructed to describe and model system failure based on occurrence or non-occurrence of other events (Bedford and Cooke, 2001). Interactions between events are modelled using logic gates. For example, two events may need to occur simultaneously to cause failure or it might be sufficient for one of a specific set of events to occur to cause failure. Figure 5.1 shows the structure of a fault tree, the different events and two common logic gates. System failure is represented by the *top event* in the fault tree and using logic gates this event is divided into other events until a suitable level of detail is obtained. Events at the lowest level of the fault tree are called *basic events*, i.e. events initiating failures, and events between the top and basic events are called *intermediate events*. Two basic logic gates used in fault tree analyses are the OR-gate and the AND-gate. The OR-gate models conditions where it is sufficient that *one* of several input events occurs to cause failure. The AND-gate models conditions where *all* input events need to occur to cause failure. The fault tree in Figure 5.1 illustrates that intermediate event A occurs if basic events 1 or 2 occur. However, intermediate event A will also occur if both basic events occur simultaneously. For intermediate event B to occur both basic events 3 and 4 need to occur simultaneously. Equally, the top event occurs if at least one of the intermediate events occurs.

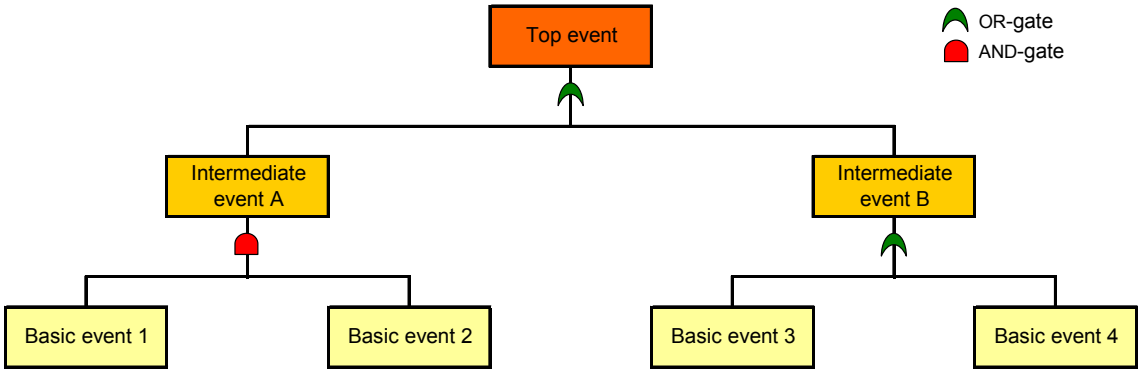

Figure 5.1. Example of a fault tree illustrating the OR- and AND-gate.

Commonly a fault tree is used to calculate the probability of the top event. The structure of the fault tree and the logic gates provide information on how to perform the calculation. As input variables the probabilities of the basic events (P_i) are needed. The probability of the output event (P_F) of an OR-gate with n input events are calculated as

$$P_F = 1 - \prod_{i=1}^{n} (1 - P_i). \qquad (1)$$

For an AND-gate with n input events the probability of the output event (P_F) is calculated as

$$P_F = \prod_{i=1}^{n} P_i . \qquad (2)$$

By combining Equations 1 and 2 according to the fault tree structure the probability of the top event can be calculated. A fault tree is considered detailed enough when it corresponds to the system analysed and when the variables needed are possible to estimate for the basic events.

The main differences between traditional fault tree analysis and the method presented in this thesis are: (1) the possibility to calculate not only the probability of failure but also the failure rate and downtime for each event in the fault tree; (2) the new logic gates that have been developed to include the ability of a system to compensate for failure; and (3) the fact that estimates of proportions of consumers affected by different failures are included in the fault tree, which enables calculations of risk levels, including both probabilities and consequences.

Failure types and conceptual model

As concluded in Section 3.2 the many events that may harm the supply of drinking water can be assigned to affect either the water quantity or water quality. The overall failure event included in the fault tree method is therefore termed *supply failure* and 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 comply with water quality standards. It should be noted that events affecting the water quality may cause quality as well as quantity failure. Contamination of the water source, for example, may cause the raw water to be considered unsafe for water production and if no alternative water source exists a water shortage may arise. However, if the contamination is not detected the contaminated raw water may be used and drinking water not meeting water quality standards may be delivered to the consumers. Hence, this example illustrates that quantity as well as quality failure may arise due to the same initial event, depending on the subsequent chain of events.

The fault tree method is integrated and the entire drinking water system is therefore included. The system is divided into its three main sub-systems (raw water, treatment and distribution) in order to consider interactions between these parts. Figure 5.2 shows how quantity and quality failure may arise in a drinking water system, including the ability to compensate for failure. However, although failure occurs somewhere in the system, it does not mean that the consumer is affected. Failure of a pump, for example, may be compensated for by a reserve pump. If no raw water can be supplied to the treatment plant, water stored at the treatment plant and reservoirs in the distribution system can supply the consumers during a limited period. The fault tree method thus focuses on possible consequences for the consumers. A pump that fails may result in economic consequences for the water utility but if this failure can be compensated for by a reserve pump and delivery to the consumers is not affected, the event is not considered to cause failure in the context of the fault tree method. However, as will be described later, events such as pump failure in the above example may also be analysed using the fault tree, although it does not specifically affect the consumers.

It should be noted that the boundaries between the three sub-systems shown in Figure 5.2 can be defined differently. Depending on, for example, local conditions and the aim of the analysis some components may in one case be considered to be part of the distribution system while in another case they may be considered to be part of the treatment system.

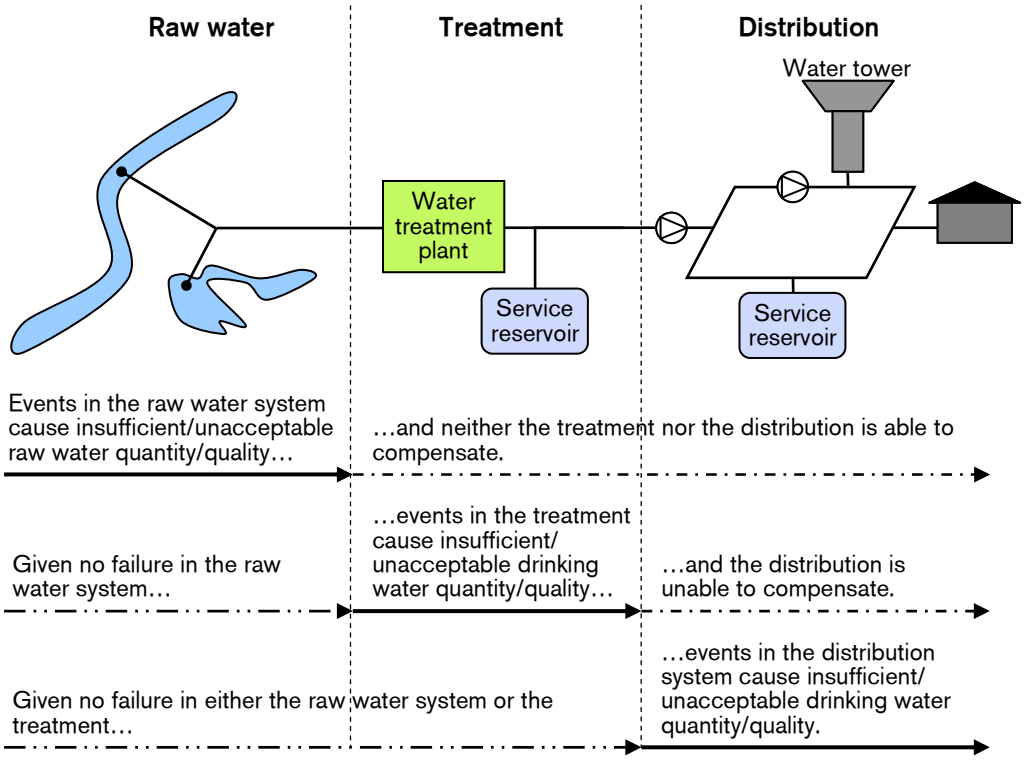

Figure 5.2. Conceptual model of how failure (quantity and quality) may arise in a drinking water system.

Fault tree and logic gates

In order to model entire drinking water systems and include their ability to compensate for failure, it was found that four different logic gates were needed. The logic gates must enable calculations of not only the probability of failure but also the mean failure rate (in this thesis expressed as the number of failures per year of operation) and mean downtime (duration of failure). The main reasons for calculating the failure rate and downtime are to facilitate expert judgements and analysis of the dynamic behaviour of the system, described further below. The mathematical foundation of the gates is presented by Norberg *et al.* (2008) and their use is presented further in Papers I and II. Two of the logic gates are the most common gates used in fault tree analysis, the OR- and AND-gate. As described above, the OR-gate is used to model situations where only one of several events needs to occur to cause failure. The AND-gate is used to model situations where all events included need to occur simultaneously to cause failure. To model the ability to compensate for failure, two variants of the AND-gate were developed. The first variant of the AND-gate models how failure may be compensated for by one or several components over a limited period of time. As long as at least one of the compensating components function the initial event

does not cause supply failure. When the ability to compensate is lost, supply failure arises and the duration is determined solely by the initial event. The compensating components are thus not assumed to be able to recover and start compensating again until the initial event has recovered. Table 5.1 provides examples of different conditions that can be modelled using the different types of logic gates. The second variant of the AND-gate also models the ability to compensate for failure but can include the ability of a compensating component to recover after failure. Thus, when the ability to compensate is lost a component is assumed to be able to recover and start compensating again. The duration of failure is thus determined by the initial event as well as the possibility of the compensating components to recover after failure. Both variants of the AND-gate include a separate variable describing what is termed probability of *failure on demand*. Failure on demand means that a compensating component is not capable at all of compensating, i.e. when required the ability to compensate does not exist. In contrast to failure on demand, failure that occurs after a certain period of compensation is termed *failure during operation*.

Table 5.1. Examples of conditions that may be modelled using the logic gates.

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 to, for example, 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 enable calculations of the failure rate and downtime on each level in the fault tree a Markovian approach is used (Rausand and Høyland, 2004). Each basic event in the fault tree is replaced by a Markov Process, which means that the event may either occur (1) or not occur (0). The transition between the two states (0 and 1) is described using the mean failure rate (λ) and the mean repair rate (μ). The mean time to failure thus corresponds to $1/\lambda$ and the mean downtime is equal to $1/\mu$. The probability of failure is thus equivalent to $P_F = \lambda/(\lambda + \mu)$. By replacing

the basic events in the four different logic gates with a Markov Process, equations for calculating the probability of failure, mean failure rate and mean downtime were developed (Norberg *et al.*, 2008), see Table 5.2.

Table 5.2. *Equations used for calculating the output of the logic gates (Norberg et al., 2008). For the variants of the AND-gate i = 1 corresponds to the failure that may be compensated for by events i = 2, …, n. For the second variant only one compensating event is considered, i = 2. Variable P_F is the probability of failure, λ_i the mean failure rates, μ_i the mean 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**
$\mu = \mu_1$	$P_F = \frac{\lambda_1}{\lambda_1 + \mu_1} \cdot \frac{\lambda_2 + q_2(\mu_1 + \mu_2)}{\lambda_2 + \mu_1 + \mu_2}$
$P_F = \frac{\lambda_1}{\lambda_1 + \mu_1} \cdot \prod_{i=2}^{n} \frac{\lambda_i + q_i \mu_1}{\lambda_i + \mu_1}$	$\lambda = \frac{\mu_1 \lambda_1 q_2 (\lambda_2 + \mu_1 + \mu_2) + \lambda_1 \lambda_2 (1 - q_2)(\mu_1 + \mu_2)}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_1 + \mu_2)(1 - P_F)}$
$\lambda = \frac{P_F}{1 - P_F} \cdot \mu$	$\mu = \frac{\mu_1 \lambda_1 q_2 (\lambda_2 + \mu_1 + \mu_2) + \lambda_1 \lambda_2 (1 - q_2)(\mu_1 + \mu_2)}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_1 + \mu_2) P_F}$

Since all drinking water systems are constructed in different ways it is not possible to provide one fault tree that is applicable to all systems. However, a generic structure can be composed to illustrate the main events and how they are interconnected. Figure 5.3 shows a generic fault tree, including the three main sub-systems (raw water, treatment and distribution). The fault tree illustrates that it is sufficient that failure (quantity or quality) occurs in one sub-system to cause supply failure. However, it is also shown that failure in one sub-system may be compensated for by other parts of the system (cf. Figure 5.2). The latter

circumstance is modelled by means of the first variant of the AND-gate. The generic fault tree structure is further presented in Paper I.

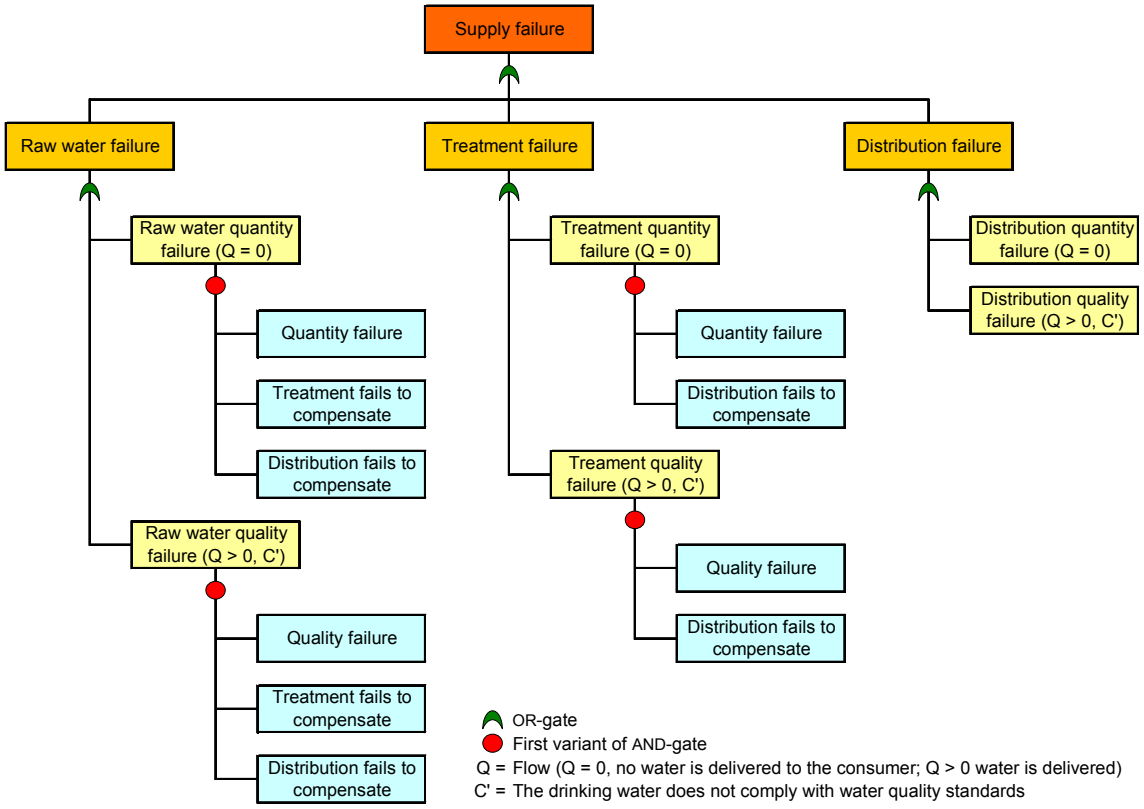

Figure 5.3. *Generic fault tree of a drinking water system, including quantity as well as quality failure in all three sub-systems.*

Risk and Customer Minutes Lost

Traditionally, fault tree analyses calculate only the probability of failure. However, to be able to quantify the risk, information on the consequence is also required. The consequences of quantity and quality failure may be described by the duration of failure and the number of people affected. The duration of failure corresponds to the mean downtime. An estimate of the number of people affected is thus required in order to calculate the risk. Using this information the risk may be expressed as

$$R = \lambda \cdot \frac{1}{\mu} \cdot C \,, \qquad (3)$$

where λ is the mean failure rate, $1/\mu$ the mean downtime and C the expected proportion of consumers affected by failure. By using these variables the risk is

calculated as the expected number of minutes the average consumer is affected by quantity or quality failure per year. Risk is thus expressed as the expected value of Customer Minutes Lost (CML), see e.g. Blocker *et al.*, (2005). For quantity failure, CML corresponds to the number of minutes per year the average consumer does not have access to drinking water. CML related to quantity failure represents the number of minutes per year the average consumer is supplied with water that does not meet the water quality standards. It should be noted that not all drinking water is used as plain drinking water or for cooking. Furthermore, it should be noted that the risk associated with quantity and quality failure must be presented separately to retain transparency. The reason why the risk is calculated for the average consumer is due to the fact that a proportion is used to define how many consumers are affected. To also consider that the system may not fail when in failure mode, it can be shown (Paper I) that Equation 3 can be reformulated and the expected value of CML calculated as

$$R = P_F C \,. \tag{4}$$

To be able to calculate the risk the consequence needs to be estimated. Since it is not possible or meaningful to estimate the consequence for the top event in the fault tree, a lower level in the fault tree must be identified. If this level only has OR-gates above it and does not combine events with totally different consequences, then the risk may be calculated as a sum of the risks caused by different events. The total risk is thus calculated as

$$R = \sum_{i=1}^{n} P_{Fi} C_i \,. \tag{5}$$

A possible strategy when identifying a suitable level for estimating the consequences is to divide quantity and quality failure into main failure events. This should be done under each of the three sub-systems.

To only calculate the risk (expressed as CML) it is not necessary to calculate the failure rate and downtime on each level in the fault tree. It is enough to calculate the probability of failure, since that in combination with the consequence (the proportion of consumers affected) can be used to calculate the risk using Equation 5. However, in order to evaluate the system properly information on the dynamic behaviour of the system is also needed. The failure rate and downtime must therfore be calculated on each level in the fault tree.

Uncertainties and uncertainty analysis

Since uncertainties are an important part of the risk concept, the fault tree method has been developed to include uncertainties of estimates using a probabilistic approach. In addition, a Bayesian approach has been used to facilitate integration of expert knowledge and hard data. The Bayesian approach enables updating of fault tree models as new hard data becomes available. All input variables in the fault tree model are replaced by probability distributions. Variables λ and μ are modelled as exponential rates using Gamma distributions. The proportion of consumers affected (C) as well as the probability of failure on demand (q) were modelled by Beta distributions (Paper I). The distribution classes used in the method facilitate the Bayesian approach.

The probabilistic approach used in the method facilitates: (1) analysis of uncertainties in each variable; (2) calculation of rank correlation coefficients, providing information on how much the uncertainty of each variable in the fault tree affects the uncertainty of the top event as well as the intermediate events; and (3) calculation of the probability of the risk exceeding specified criteria, i.e. acceptable levels of risk.

Using Monte Carlo simulations (described further below) the uncertainties in the input variables are used to calculate the results, including uncertainties. Instead of presenting the results as point values, they are thus expressed as probability distributions. This makes it possible to analyse how much each variable may vary, due to natural variation as well as lack of knowledge and other sources of uncertainty.

Uncertainties may be analysed in many different ways. Since Monte Carlo simulations are used in this method, it was possible to calculate rank correlation coefficients for each input variable in the fault tree model. A rank correlation coefficient illustrates the contribution of a variables to the uncertainties in the results. The coefficient can have values between -1 and 1, where negative values represent negative correlations and positive values represent positive correlations. A large correlation coefficient indicates a strong relationship. By analysing the rank correlation coefficients it is possible to identify which variables in the model should be analysed further in order to reduce the uncertainties in the results. It is also possible to identify which variables contribute least to the total uncertainty and hence should not be prioritised for further study.

Expert judgements

As described above, an important reason for using the failure rate and downtime is to facilitate expert judgements. Elicitation of expert judgements is an important part of many risk analyses since a sufficient amount of hard data is often missing (Paté-Cornell, 1996). However, estimating variables needed as input in a risk analysis may be difficult, especially when it comes to probabilities and uncertainties of estimates.

By using the mean time to failure (MTTF) and mean downtime (MDT) the probability of failure may be expressed as

$$P_F = \frac{\mathrm{MDT}}{\mathrm{MTTF} + \mathrm{MDT}}. \qquad (6)$$

The sum of MTTF and MDF corresponds to the mean time between failures (MTBF). The MTTF and MDT is equivalent to $1/\lambda$ and $1/\mu$ respectively. The probability of failure is thus equivalent to

$$P_F = \frac{1/\mu}{1/\lambda + 1/\mu}. \qquad (7)$$

Equation 7 can be reformulated and the probability of failure expressed based on the mean failure rate (λ) and mean repair rate (μ) as

$$P_F = \lambda/(\lambda + \mu). \qquad (8)$$

By allowing the experts to estimate, for example, the mean failure rate and mean downtime, the probability of failure can be calculated. In this way a direct estimation of the probability is avoided and the experts are required to consider the mean failure rate (or mean time to failure) as well as the mean downtime. When the method was applied in Gothenburg (Section 5.3) this was considered an advantage since questions about failure rates and downtimes are more easily understood and easier to answer, compared to questions about probabilities.

As described above all input variables in the fault tree model are replaced by probability distributions. To acquire information regarding these distributions the experts should be asked to estimate a probable highest and lowest value of each variable. This information should be used as percentiles when estimating the probability distributions. It is the task of the risk analyst to decide which percentiles the expert judgements correspond to. Based on the assessed accuracy

of the expert judgements the 5- and 95-percentiles may be used in one case, but in an another case the information may not be considered equally accurate and the 10- and 90-percentiles are used instead. To ensure suitable probability distributions are obtained mean or median values may also be considered.

Since elicitation of an expert judgement is based on communication between the expert and the risk analyst it is important to minimise linguistic uncertainties, i.e. uncertainties that arise due to words not being exact. A basic approach to do this is to describe clearly the variables being estimated and have an open dialogue.

Monte Carlo simulation

For the purpose of this thesis Monte Carlo simulation was used to calculate the uncertainties in the model results based on uncertainties in input variables (Figure 5.4). The simulations were performed using Crystal Ball©, an add-in software to Microsoft Excel. The Monte Carlo technique uses random numbers to sample values from probability distributions representing the input variables (see e.g. Ang and Tang, 2007). 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. Samples are more likely to be selected if they have higher probabilities of occurrence.

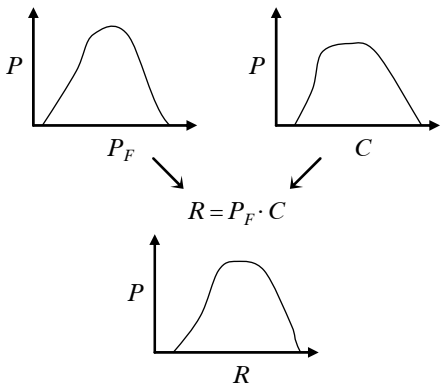

Figure 5.4. *Illustration of how Monte Carlo simulations can be used to include uncertainties in calculations.*

5.3 Case study Gothenburg

The application of the fault tree method to the drinking water system in Gothenburg presented in this section is based primarily on Paper II. The Gothenburg system includes several forms of interaction between events and parts of the system, which made it possible to evaluate the applicability of the fault tree method to a relatively complex drinking water system.

System description

The drinking water system in Gothenburg supplies approximately half a million people with drinking water. The system is based solely on surface water and the main water source is the Göta Älv river. Figure 5.5 shows an overview of the raw water supply in Gothenburg. The system includes two treatment plants and under normal conditions treatment plant no. 1 is supplied with raw water from the river. Water from the river is also pumped to the reservoir lakes, which in turn supply treatment plant no. 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 can also be used to supply the reservoir lakes, or treatment plant no. 2 directly, with water.

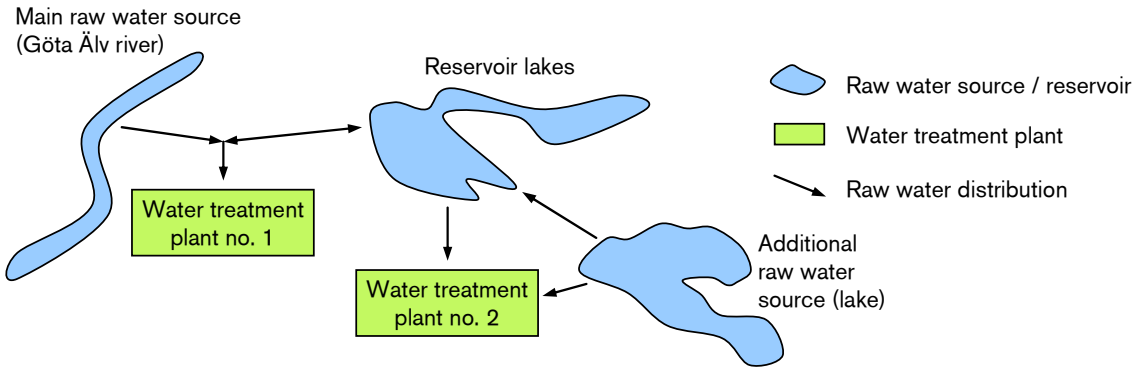

Figure 5.5. Schematic description of the raw water system in Gothenburg.

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 the 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, for example, on the online monitoring and reports from different operating bodies upstream.

Analysis procedure

As recommended by, for example, the WHO (2004) a team of people was put together to support the risk analysis in different ways. The team included water utility personnel with knowledge of the system and scientists with knowledge of risk analysis and drinking water systems. The analysis was based on the following main steps:

- Scope definition
- System description, hazard identification and fault tree construction
- Evaluation of available data
- Elicitation of expert judgements
- Risk estimation
- Uncertainty analysis
- Evaluation of results

The purpose of applying the fault tree method was to evaluate its applicability, including the possibility to model interactions between events and provide information on risks to the system that may help decision-makers to minimise sub-optimisations of risk-reduction options. To further support decision-making the analysis aimed to compare estimated risk levels with acceptable risk levels. The analysis included quantity as well as 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). After the scope had been defined the system was described at the same time that hazards were identified and the fault tree constructed. The fault tree thus illustrates the function of the system as well as how different events could cause failure.

The risk analysis team had several meetings to discuss possible hazards and the system function. The fault tree construction was performed iteratively where parts of the fault tree were discussed, evaluated and updated together with experts (water utility personnel) on the specific parts of the system.

When available, hard data such as statistics on events were used to estimate the variables needed in the fault tree model. However, in many cases sufficient hard data were not available and expert judgements were therefore used according to the description in Section 5.2. Based on preliminary results, an evaluation was made together with water utility personnel and the fault tree structure and input data were updated when necessary. Monte Carlo simulations were carried out using the software Crystal Ball© 7.3.1. Since the method is capable of handling estimate uncertainties, the probability of exceeding acceptable levels of risk could be calculated. Rank correlation coefficients were also calculated to analyse uncertainties. When compiled, the information provided by the analysis made it possible to evaluate risk levels as well as the dynamic behaviour of the system and the uncertainties in the results.

Fault tree

Based on the generic fault tree structure shown in Figure 5.3 and the different logic gates, a fault tree of the entire drinking water system in Gothenburg was constructed. In total, the fault tree included 116 basic events, 100 intermediate events and 101 logic gates.

The system was divided into its three main sub-system (raw water, treatment and distribution) and an OR-gate was used to model that failure (quantity or quality) only needs to occur in one sub-system to cause supply failure. However, to include the inherent ability of the system to compensate for failure, the first variant of the AND-gate was used in each sub-system to model that failure in one sub-system may be compensated for by other parts of the system. The raw water system was considered to include 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 system. 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 sub-system 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. If the calculated CML values had included situations where no water is delivered and situations where water unfit for human consumption is delivered, the results would not have been as informative and useful.

It is not only possible for one sub-system to compensate for failure in other parts of the system; interactions between parts in the same sub-system also provide opportunities for compensation. Both variants of the AND-gate were thus used to model different kinds of compensation within the three sub-systems. 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. The structure of the fault tree of the Gothenburg system is described further in Paper II.

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 sub-system 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 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. The main failure events only have OR-gates above them in the fault tree, which is required when Equation 5 (Section 5.2) is used to calculate the risk.

Results and discussion

The fault tree analysis provided quantitative results for, for example, risk levels. However, the actual fault tree and the process of constructing it are also important results. The fault tree structure provides information on how the system functions and how different events interact. In addition to information on risk levels expressed as CML, quantitative results on the probability of failure, failure rate and downtime were provided for all events in the fault tree. Furthermore, uncertainties in the results were calculated using Monte Carlo

simulations (10,000 iterations) and the rank correlation coefficients were calculated to support uncertainty analysis.

In Figure 5.6 and Figure 5.7 the expected CML per year (risk), probability of failure, mean 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 the raw water, treatment and distribution parts separately. Since uncertainties are considered in the analysis the 5-, 50- (median) and 95-percentiles are presented for all variables. Note that the scales differ between some of the variables in Figure 5.6 and Figure 5.7.

By studying the risk levels in Figure 5.6 and Figure 5.7 it can be concluded that for both quantity and quality failure the raw water system contributes most to the total risk level. 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 in Section 5.2). The probability of failure is calculated based on the mean failure rate and mean downtime (cf. Equation 8 in Section 5.2) 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 have a small 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 subjected to severe health effects.

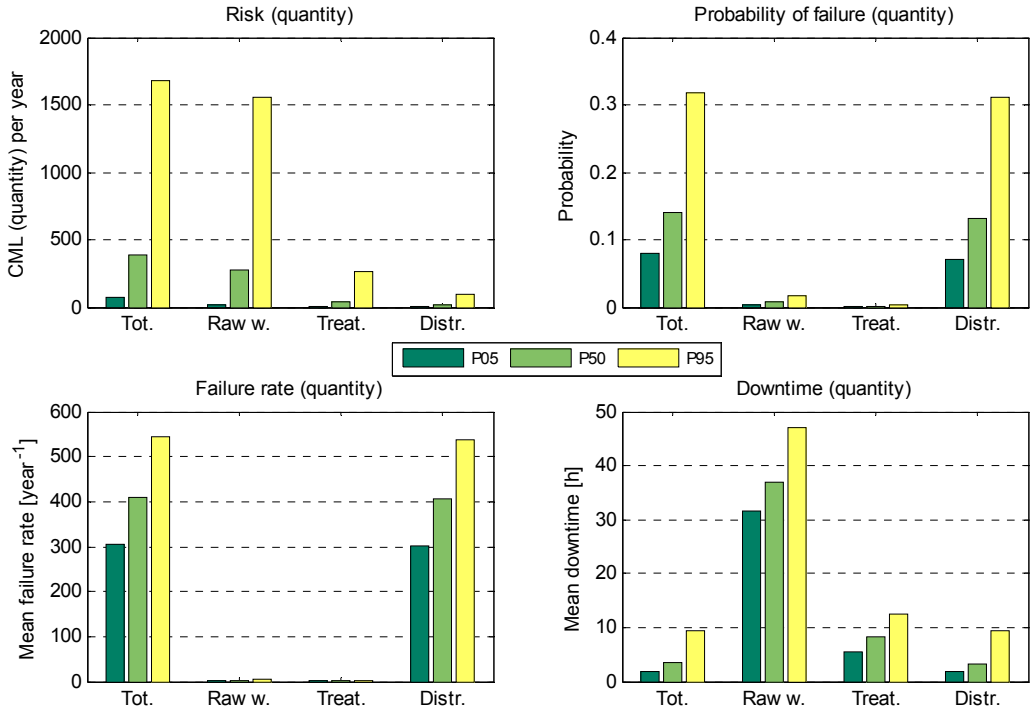

Figure 5.6. *Histograms showing the risk (expected value of CML), probability of failure, mean failure rate and mean downtime for quantity failure. The 5-, 50- and 95-percentiles are presented for the entire system (Tot.) as well as the three main sub-systems.*

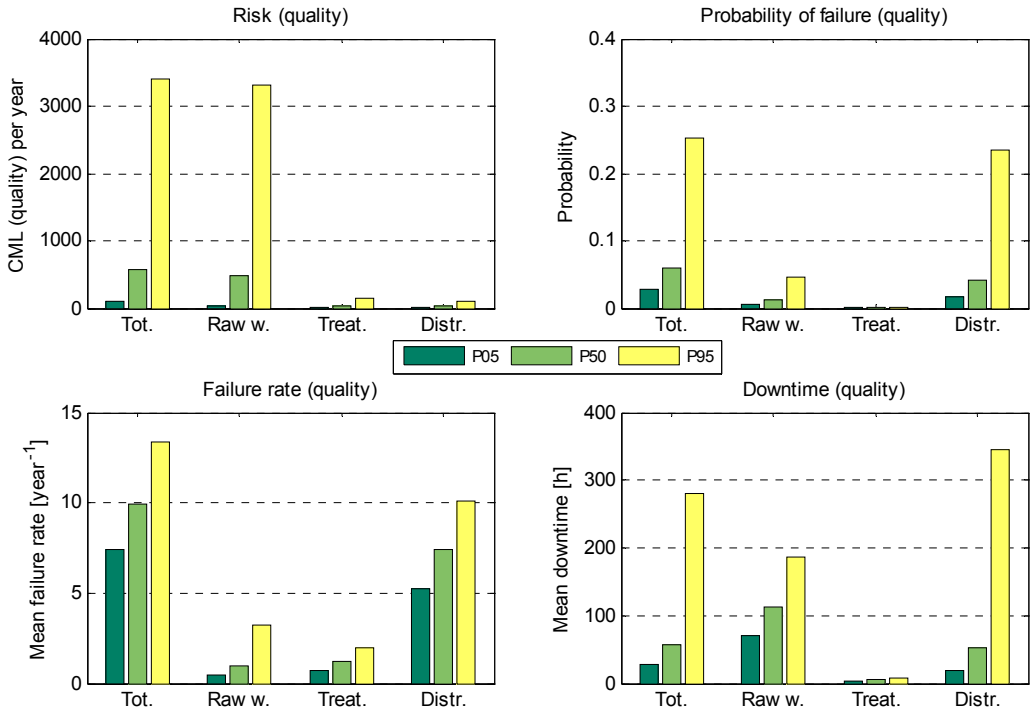

Figure 5.7. *Histograms showing the risk (expected value of CML), probability of failure, mean failure rate and mean downtime for quality failure. The 5-, 50- and 95-percentiles are presented for the entire system (Tot.) as well as the three main sub-systems.*

Figure 5.6 and Figure 5.7 show that the failure rate is higher for quantity failure compared to quality failure but the downtime is shorter for quantity failure. Quantity failures are therefore most common while quality failures have a longer duration. The percentiles in Figure 5.6 and Figure 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 performance target that can be regarded as being an acceptable level of risk. The performance 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). Figure 5.8 shows the comparison of the performance target, translated to 144 CML per year, with the risk level provided by the fault tree analysis (Figure 5.6). 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.

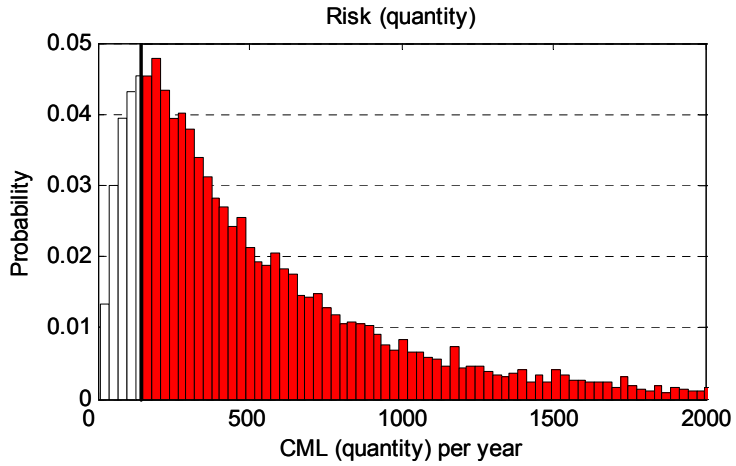

Figure 5.8. *Uncertainty distribution of quantity-related risk, including the entire system, compared with the performance target (144 CML per year) indicated by the solid vertical line. The probability of exceeding the performance target (red area) is 0.84.*

Figure 5.8 illustrates one way of using information on uncertainties in results to acquire additional information about the risk. To further analyse the uncertainties, 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 probability of distribution failure. 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 mean 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 8 in Section 5.2). 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.

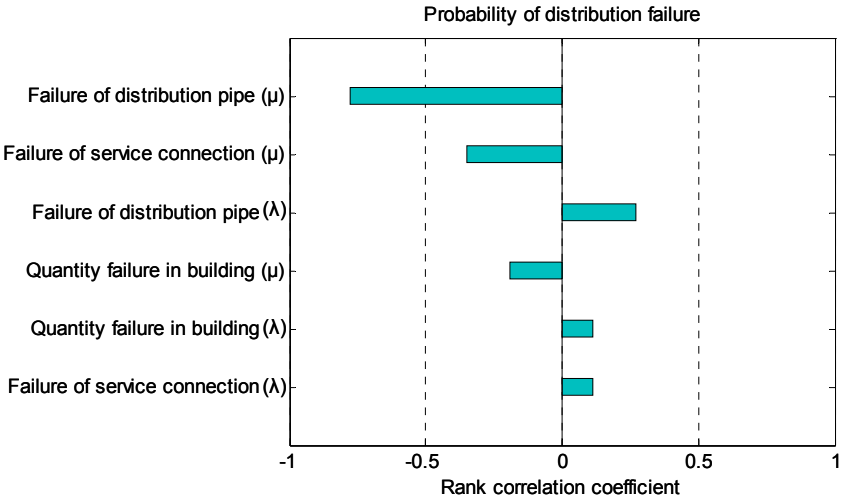

Figure 5.9. *Uncertainty analysis of the probability of distribution failure. The rank correlation coefficient of the six variables contributing most to the uncertainties in the probability of distribution failure are presented.*

5.4 Benefits and limitations

Like all methods the fault tree method has benefits as well as limitations. Miller *et al.* (2005) point out the following six generic criteria as important in methods used to assess risk:

- *The logical soundness of the method* – its justification based on theoretical arguments or scientific knowledge, and the validity of the model assumptions.
- *Completeness* – whether it can assess all aspects of the problem and the degree to which it excludes issues because they are too difficult to accommodate.
- *Accuracy* – the precision reflected in the confidence level associated with the results.
- *Acceptability* – compatibility with existing processes, that it is rational and fair and that it is clear and understandable.
- *Practicality* – the level of expertise, time and input data required.
- *Effectiveness* – the usefulness of results.

The fault tree method presented in this thesis is based on theoretically well established techniques, including fault tree analysis, Markovian processes and Bayesian statistics. Assumptions made when constructing a fault tree will differ between different applications. However, the analysis of the Gothenburg system provided results consistent with the understanding of the system by the water utility personnel.

Since the fault tree method enables analysis of entire drinking water systems and consideration to be given to quantity- as well as quality-related failures, it covers an extensive part of the relevant aspects. Although the method includes failures related to water quality issues, the actual health effect is not estimated. The possibility to combine the results of a fault tree analysis with a Quantitative Microbial Risk Assessment (QMRA) is discussed in Section 6.2.

The accuracy of the results originates from the fault tree construction, which varies between applications. However, the set of logic gates and the generic fault tree structure provide a helpful basis. Since the method includes uncertainties in all estimates, possible variations in the results are presented and decision-making does not need to be based on point estimations.

The developed logic gates make it possible to model drinking water systems accurately. Although a person without previous experience of fault tree analysis may not be able to construct a fault tree based on the method presented, it must be considered fairly simple to understand the basic concepts. Quite a high level of experience is therefore required to construct the fault tree and perform Monte

Carlo simulations. However, the required information for constructing the fault tree, i.e. system description and hazardous events, should be provided by people who know the system and does not require previous experience of fault tree analysis. Compared to risk ranking using risk matrices, a fault tree analysis is time-consuming and requires a substantial amount of data.

Since the method provides information on risk levels as well as the dynamic behaviour of the system, the results are useful when evaluating the system. The possibility to perform uncertainty analysis by calculating rank correlation coefficients makes it possible to identify where new information in the model is most valuable to reduce the uncertainties in the results and this information should be used to guide further studies. The possibility to model risk-reduction options also provides additional and valuable results.

6 DISCUSSION

This chapter provides a discussion of the contents of the thesis, including the fulfilment of the overall aim and the specific objectives presented in Section 1.2.

6.1 Managing risks to drinking water systems

Risk management in the drinking water sector should aim to secure a reliable supply of safe drinking water in order to protect public health, public functions and much more. The aim of risk management cannot be to eliminate all risks but rather to achieve an acceptable level of risk based on an efficient use of available resources for risk reduction. The concept of safe drinking water should include safe water quality as well as a reliable supply. Hence, both water quality and quantity are important. However, water utilities also need to consider financial, commercial, environmental, reputation and compliance/legal risks.

Frameworks describing risk management of drinking water systems exist although they do not apply an approach that includes all types of risk and they essentially lack guidance on methods and tools to assist water utilities in their risk management. For water utilities to be able to analyse and evaluate risks, as well as options for risk reduction, a set of tools is needed. The integrated and probabilistic fault tree method presented in this thesis provides a new means of making a risk analysis of drinking water systems. The presented framework for integrated risk management aims to provide a generic structure for managing risk. The framework aims to supplement and not in any way replace current frameworks in the drinking water sector.

Although risk analyses are performed, criteria defining acceptable levels of risk are needed in order to evaluate the results and decide whether or not risk-reduction options are required. Such criteria exist for water quality, for example the health-based targets defined by the WHO (2004). However, criteria defining acceptable levels of risk regarding water quantity aspects and other stakeholder values are also needed. These criteria should not be defined by international organisations but rather for each drinking water system, with consideration given to local conditions. In Gothenburg, for example, performance targets have been defined which can be express using CML as a measure. Although this thesis does

not focus on risk tolerability criteria it should be noted that aspects such as the willingness of the general public to pay for reducing or avoiding risk may also be used (see e.g. Smith, 2005).

Efficient risk management requires well performed and informative risk analyses as well as other factors, such as organisational structure and commitment. Based on international reports Pollard *et al.* (2004) describe critical aspects important to an organisation managing risk. These criteria include the importance of openness, transparency, involvement, proportionality, precaution, evidence and responsibility to good decision-making. Furthermore, the critical role of taking a long-term view in assessing the potential indirect consequences of management actions is stressed. As concluded by Lindberg and Lindqvist (2005), efficient communication of experiences and other relevant information between water utilities, governmental authorities and other stakeholders is also important to facilitate efficient risk management.

6.2 Integrated risk analysis

As described in Chapter 1, the purpose of a risk analysis is to support decision-making by providing the information required. It should be stressed that a risk analysis should only support decision-making and not determine decisions (Kammen and Hassenzahl, 2001). Results provided using, for example, the fault tree method are of a technical nature and do not take into account risk perception and other social aspects of risk. As described in Section 2.1, these aspects need to be included in the decision-making process. Pollard *et al.* (2004) point out that an organisation may lose public confidence if *hard* quantitative risk analysis tools are used without including transparent decision-making.

Approaches advocated as important when managing drinking water systems are the multi-barrier approach and the integrated, from source to tap, approach. In the context of fault tree analysis, the multi-barrier approach may be explained by one of the two variants of the AND-gate. Failure may thus be compensated for by means of one or several barriers and all barriers need to fail to cause system failure. This clearly illustrates the advantages of using multiple barriers when implementing risk-reduction options and the ability of the method developed to model such conditions. One of the main reasons why an integrated approach should be applied is the fact that there are interactions between events and parts of a drinking water system. The integrated approach is consistent with fault tree analysis since fault trees aim to model interactions between events.

Qualitative methods for risk analysis, such as risk ranking using risk matrices are useful in many cases but they also have a number of limitations. The complex structure and interactions between events and parts of a drinking water system makes is necessary to consider chains of events when making risk analyses. Integrated and quantitative methods facilitate: (1) proper representation of the system; (2) adequate estimation of the risk, including the entire system; and (3) proper modelling of risk-reduction options. The fault tree method can provide a proper representation of the system since the entire system can be included and the four logic gates make it possible to model different types of interaction. Furthermore, the method enables calculations of risk levels expressed as the expected value of CML. This is possible as the proportion of consumers affected by different failure events is estimated and included in the fault tree method. A traditional fault tree analysis is only capable of calculating the probability of failure and not the risk. The possibility to calculate the probability of failure as well as the failure rate and downtime for each event in the fault tree, makes it possible to analyse the dynamic behaviour of the system. Furthermore, the use of failure rates and downtimes is considered more suitable for expert judgements than direct estimations of failure probabilities. This is due to the fact that people are affected by many factors when they estimate and make judgements of probabilities (see e.g. Slovic *et al.*, 2004). The probabilistic approach used in the fault tree method makes it possible to calculate the probability of exceeding acceptable levels of risk. This information forces the decision-makers to define to what level of certainty acceptable levels of risk and other performance targets should be fulfilled.

Since the structure of the fault tree as well as the input variables may be changed, it is possible to model and in absolute terms evaluate the efficiency of different options for risk reduction. These circumstances, together with the fact that it is possible to compare different parts of the system to see how much they contribute to the total risk and in what way they contribute, make the fault tree method a valuable tool to support decision-making. Hence, sub-optimisation of risk-reduction options may be minimised and resources used efficiently. Using a fault tree model it is possible to analyse and evaluate the effects of, for example, an additional raw water source or installation of a reserve pump in a critical part of the distribution system. Decisions on the strategic as well as the programme and operational levels may thus be supported by results from a fault tree analysis.

The fault tree method enables calculations of rank correlation coefficients and consequently it is possible to identify which parts of the system should be analysed further in order to reduce the uncertainties in the results. Hence, this

information may guide further studies. It should be noted that the reason for uncertainty contribution from a variable may be natural variation as well as lack of knowledge. Consequently, it is not possible to reduce all types of uncertainty (see Section 2.2).

The results of the fault tree analysis carried out in the drinking water system in Gothenburg showed the importance of a reliable and safe supply of raw water. The results should not be interpreted in such a way that no resources should be spent on maintaining and improving the treatment and distribution system, but rather that the first part of a chain of sub-systems is critical and failure in this part may have severe consequences. The distribution system in Gothenburg was shown to include frequent failures. Although these failures have a short duration and affect a small number of consumers, maintenance of the distribution system is an important task to ensure the distribution system is reliable. The dynamic behaviour of the distribution system would not have been possible to identify if only the total risk levels had been analysed. The dynamic behaviour of the system should consequently be studied in combination with information on risk levels. The fact that the same risk level (expressed as the expected value of CML) may be obtained by different probability and consequence value combinations, emphasises the importance of studying different aspects of the results from a fault tree analysis.

Although the fault tree method is primarily a tool for quantitative risk analysis, it can be used to analyse a drinking water system qualitatively. Without performing any calculations the structure of the fault tree shows how the system functions. The interactions between events and parts of the system are shown by how the events are organised and combined with different logic gates.

When applying the fault tree method the criteria of quantity and quality failures may be defined in different ways. Instead of using unfit for human consumption as a criterion for unacceptable water quality, the focus could be on specific contaminants. Quantity failure does not need to correspond to the total interruption in the delivery of water. A specified pressure level, for example, may be used instead. It is thus possible to adjust the method to fit a specific analysis.

It should be stressed that a quantitative risk analysis can provide not only a quantified risk level but also valuable discussions. When making the risks analysis of the drinking water system in Gothenburg conditions in the system were identified which had earlier not been considered a problems. Hence, these discussions are also important since they may provide a better understanding and

awareness of how different events may harm the system and how the system functions. Since no single person can have all the knowledge required to perform a risk analysis of a drinking water system, it is crucial to work in a team that includes people with different areas of knowledge regarding the system and the risk analysis method.

If a risk analysis can be updated continuously it may become a helpful and central part of risk management. Using the Bayesian approach the fault tree method presented facilitates a mathematically formal updating as new hard data becomes available. Statistics on events and other sources of data can therefore be used to update the model. This would make it possible to study how the risk as well as other variables change over time.

As with all methods the fault tree method can also be improved in different ways. One possible further development would be to also include correlation between events. Furthermore, the fault tree method does not include the health effects of quality-related failures. However, information in provided on the expected number of minutes the average consumer is supplied with drinking water that does not meet the water quality standards. This information may be used as input, for example, in a Quantitative Microbial Risk Assessment (QMRA) (Haas *et al.*, 1999) and the system description provided by the fault tree model could be used to identify possible risk-reduction options. Fault tree analysis may also be used to analyse and structure occurred events of quality failure, in order to learn and improve fault tree models of similar systems (Risebro *et al.*, 2007).

6.3 Fulfilling the aim and objectives

The overall aim of this thesis is *to contribute to the knowledge regarding quantitative risk analysis of drinking water systems in accordance with the Water Safety Plan approach*. The following specific objectives are also stated in Section 1.2:

- To describe a framework for integrated risk management of drinking water systems.
- To develop a method for integrated and probabilistic risk analysis of drinking water systems.
- To apply the method and evaluate its benefits and limitations.

A framework for integrated risk management of drinking water systems is presented in Section 4.2. The framework illustrates the role of risk analysis in risk management and shows how the results of an analysis are intended to be used. This provides a better understanding of the importance of clearly defining the required output of the analysis and that the ultimate goal of risk analysis is informed decision-making. The framework also shows that both water quantity and quality risks need to be considered to achieve efficient risk management.

A method for integrated and probabilistic risk analysis has been developed and is presented in Chapter 5 and Paper I. The fault tree method developed is quantitative and makes it possible to include the entire system, from source to tap, to model interactions between events and to consider uncertainties of estimates. As noted above, risks related to water quantity as well as quality need to be considered and the method suggested can model both types. Although the method is based on fault tree analysis, a commonly used risk analysis tool, the theory has been further developed to suit analysis of drinking water systems. The fault tree method has been evaluated based on a real-world application, which is presented in Chapter 5 and Paper II. The method is shown to be applicable to drinking water systems and provides valuable results for informed decision-making aimed at minimising sub-optimisation of risk-reduction options.

The fault tree method developed, its application and evaluation as well as the framework for integrated risk management, come together to contribute new knowledge regarding quantitative risk analysis of drinking water systems in accordance with the Water Safety Plan approach.

7 CONCLUSIONS

The final chapter summarises the main conclusions of the thesis and presents possible further studies and new applications of the fault tree method.

The main conclusions of this thesis are:

- The fault tree method for integrated and probabilistic risk analysis of drinking water systems enables modelling of entire systems and provides information on the total risk level (expressed as the expected value of CML) as well as the contribution of each sub-system to the risk. In addition, the dynamic behaviour of the system is described using information on the probability of failure, mean failure rate and mean downtime for each event in the fault tree.
- Since uncertainties are included in the fault tree method it is possible to estimate the probability of exceeding acceptable levels of risk and other criteria. It is also possible to identify which events contribute most to the uncertainties in the results. The latter information makes it possible to assess where further information is most valuable in reducing the uncertainties in the results.
- The alternative logic gates that have been developed make it possible to model the function of drinking water systems adequately, since the ability to compensate for failure can be included. The Bayesian approach enables updating of input variables and consequently the entire analysis as new hard data becomes available. A fault tree model can also be used to analyse risk-reduction options and evaluate their efficiency.
- Risk measures such as CML are valuable since they provide understandable results and can be used to define performance targets, i.e. acceptable levels of risk. However, since the same risk can be obtained using different combinations of probability and consequence values, the risk level should be analysed in combination with information on the probability of failure and/or the consequence.
- The results of a quantitative risk analysis not only include figures on risk levels. Discussions during the performance of the analysis are also valuable, since important aspects of different risk issues are discussed.

Furthermore, the suggested method provides a structure that makes analysts identify and consider factors such as interactions between events and possibilities to compensate for failures. Factors such as these are often overlooked in risk analyses of drinking water systems, which affect the accuracy of the analysis results.

- The method presented for integrated and probabilistic risk analysis contributes to meeting the existing lack of guidance on methods and tools for risk analysis of drinking water systems. However, one single method cannot be used to analyse all kinds of risks. Water utilities must thus have access to a set of tools for risk analysis and other aspects of risk management to facilitate efficient risk management.
- The limitations of end-product testing are stressed as a main reason why a preventative risk management approach is important in the drinking water sector. An integrated from source to tap approach is advocated as essential since there are interactions between events and parts of a system. Furthermore, risks to drinking water systems should be managed using a multi-barrier approach.
- Tolerability criteria, i.e. acceptable levels of risk, need to be defined to enable evaluation of risk based on results from a risk analysis. In addition to water quality targets, quantity targets and targets representing other stakeholder values also need to be defined.
- The supply of drinking water is essential to society and since the systems are vulnerable, risk management is becoming increasingly important in the drinking water sector. Frameworks for risk management, such as the one presented in this thesis, helps water utilities to identify important tasks to be carried out and which aspects to include.

The fault tree method offers possibilities for further development and additional applications. In efficient risk management the use of risk analysis results in decision-making is also important. The following areas for further research have been identified:

- Apply the fault tree method to systems different to the Gothenburg system in order to further evaluate its applicability to, for example, less complex systems. Mathematically formal updating of an existing fault tree analysis should also be carried out and evaluated.

- To further compare the fault tree method with other methods in order to distinguish in which situations the different methods are most applicable and how they can support decision-making.
- Model and evaluate risk-reduction options using the fault tree method. This work should focus on how the method can be used as a decision support tool. This work has been initiated by using the method for studying the effects of various alternatives for increasing the reliability of the raw water supply in Gothenburg, see Rosén *et al.* (2008a). In the future, economic valuation of risk reduction against cost, as well as cost-benefit analyses, are likely to become increasingly important. Hence, the possibility to combine the fault tree method with economic valuation of risk-reduction options should be studied.
- To study steps in risk management subsequent to risk analysis in order to describe how cost-effective risk management in safe and sustainable drinking water systems may be achieved. This research should focus on decision support and include decision theory, value of information, cost-effectiveness and cost-benefit aspects.

To achieve a reliable supply of safe drinking water, risk analysis providing informed decision-making is of paramount importance. Integrated and probabilistic risk analysis carried out by means of, for example, the fault tree method presented is important since it includes the entire system and considers interactions between events. However, one single method cannot be used to handle all risk-related issues. Instead, a set of tools to assist water utilities in their risk management is of primary importance. Since information on available tools is limited the method for integrated and probabilistic risk analysis presented in this thesis contributes to the knowledge of quantitative risk analysis of drinking water systems in accordance with the WSP approach. As stated by LeChevallier *et al.* (1999), *knowledge is the first line of defence for those who provide safe drinking water*.

REFERENCES

Aller, L.T., T. Bennett, J.H. Lehr, R.J. Petty and G. Hackett (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.

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

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

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

AZ/NZS (2004). *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*, Ph.D. Thesis No. 2551, Chalmers University of Technology, Göteborg.

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

Beuken, R., S. Sturm, J. Kiefer, M. Bondelind, J. Åström, A. Lindhe, I. Machenbach, E. Melin, T. Thorsen, B. Eikebrokk, C. Niewersch, D. Kirchner, F. Kozisek, D.W. Gari and C. Swartz (2007). *Identification and description of hazards for water supply systems - A catalogue of today's hazards and possible future hazards*, Deliverable no. D 4.1.1, D 4.1.2, TECHEANU.

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

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

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

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.

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.

Council of the European Union (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.

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

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

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

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

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

Dewettinck, T., E. Van Houtte, D. Geenens, K. Van Hege and W. Verstraete (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.

DWWA (2006). *Guidelines for safe drinking water quality (In Danish)*, Danish Water and Wastewater Association, Skanderborg, http://worker.zmag.dk/showmag.php?mid=sqhq&preview=1.

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

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

Ezell, B.C., J.V. Farr and I. Wiese (2000). Infrastructure risk analysis model, *Journal of Infrastructure Systems*, *6* (3), 114-117.

Fetter, C.W. (2001). *Applied hydrogeology*, 4 ed., Prentice-Hall, Upper Saddle River.

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*, 2. ed., Elsevier Butterworth-Heinemann, Oxford.

Gunnarsdóttir, M.J. and L.R. Gissurarson (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., C.P. Gerba and J.B. Rose (1999). *Quantitative microbial risk assessment*, Wiley, New York.

Hamilton, P.D., P. Gale and S.J.T. Pollard (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 J.M. Melse (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*, 2 ed., Wiley, New York.

Hokstad, P., J. Røstum, S. Sklet, L. Rosén, T.J.R. Pettersson, A. Lindhe, S. Sturm, R. Beuken, D. Kirchner and C. Niewersch (2008). *Analysing the risks of drinking water systems from source to tap (In prep)*, Deliverable no. D 4.2.4, TECHNEAU.

Homedes, N. (1996). *The Disability-Adjusted Life Year (DALY) Definition, Measure and Potential Use*, Human Capital Development, Working Papers, HCDWP 68.

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

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/IEC (2002). *Guide 73 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 P. Jagals (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.

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

Kaplan, S. (1992). The general theory of quantitative risk assessment, In proceeding of the *5th Conference on Risk-Based Decision Making in Water Resources V*, ASCE, Santa Barbara, USA, 11-39.

Kaplan, S. (1994). Bayes' Theorem and Quantitative Risk Assessment, In proceeding of the *6th Conference on Risk-Based Decision Making in Water Resources*, ASCE, Santa Barbara, USA, 186-193.

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

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

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

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

LeChevallier, M.W., M. Abbaszadegan, A.K. Camper, C.J. Hurst, J. Rose, S. Schaub, T.R. Slifko, D.B. Smith, H.V. Smith, C.R. Sterling and M. Stewart (1999). Committee report: Emerging pathogens--bacteria, *Journal of the American Water Works Association*, *91* (9), 101-109.

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

Lindberg, T. and R. Lindqvist (2005). *Risk profile: Drinking water and microbial risks (In Swedish)*, Report 28 - 2005, Swedish National Food Administration, Uppsala, http://www.slv.se/upload/dokument/Rapporter/Dricksvatten/dricksvattenrapp_05/2005_28_Livsmedelsverket_Dricksvatten_och_mikrobiologiska_risker.pdf.

MacGillivray, B.H., P.D. Hamilton, J.E. Strutt and S.J.T. Pollard (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., J.V. Sharp, J.E. Strutt, P.D. Hamilton and S.J.T. Pollard (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., J.V. Sharp, J.E. Strutt, P.D. Hamilton and S.J.T. Pollard (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 F.P. Lees (2005). *Lees' loss prevention in the process industries: hazard identification, assessment and control. Vol. 1*, 3 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., B. Whitehill and D. Deere (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.

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

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

Nadebaum, P., M. Chapman, S. Ortisi and A. Baker (2003). Application of quality management systems for drinking water quality, *Water Science and Technology: Water Supply*, *3* (1-2), 359-364.

NFSA (2006). *Improved safety and emergency preparedness in water supply: Guidance (In Norwegian)*, Norwegian Food Safety Authority Oslo, http://www.mattilsynet.no/mattilsynet/multimedia/archive/00021/Sikkerhet_og_beredsk_21772a.pdf.

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., L. Rosén and A. Lindhe (2008). Added value in fault tree analyses (*In press*), European Safety and Reliability Association 2008 and 17th Society for Risk Analysis Europe Conference, Valencia, 22-25 September.

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

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

Owen, A.J., J.S. Colbourne, C.R.I. Clayton and C. Fife-Schaw (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.

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

Pollard, S.J.T., J.E. Strutt, B.H. Macgillivray, P.D. Hamilton and S.E. Hrudey (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.

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

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

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

Rizak, S., D. Cunliffe, M. Sinclair, R. Vulcano, J. Howard, S. Hrudey and P. Callan (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., O. Bergstedt, A. Lindhe, T.J.R. Pettersson, A. Johansson and T. Norberg (2008a). Comparing Raw Water Options to Reach Water Safety Targets Using an Integrated Fault Tree Model, Paper presented at the International Water Association Conference, Water Safety Plans: Global Experiences and Future Trends, Lisbon, 12-14 May.

Rosén, L., P. Hokstad, A. Lindhe, S. Sklet and J. Røstum (2007). *Generic framework and methods for integrated risk management in water safety plans*, Deliverable no. D 4.1.3, D 4.2.1, D 4.2.2, D 4.2.3, TECHNEAU.

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

Rosén, L., A. Lindhe, P. Hokstad, S. Sklet, J. Røstum and T.J.R. Petterson (2008b). Generic Framework for Integrated Risk Management in Water Safety Plans, In proceeding of the *6th Nordic Drinking Water Conference*, Olso, 9-11 June, 193-203.

Segrave, A., W. Pronk, T. Remarer and S. Zuleeg (2007). *Global treds affecting the water cycle: winds of change in the world of water*, Deliverable no. D1.1.7, TECHNEAU.

Sinclair, M. and S. Rizak (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.

Slovic, P., M.L. Finucane, E. Peters and D.G. MacGregor (2004). Risk as Analysis and Risk as Feelings: Some Thoughts about Affect, Reason, Risk, and Rationality, *Risk Analysis*, *24* (2), 311-322.

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

Smith, A. (2005). Capital maintenance: a good practice guide, Leading Edge Asset Decisions Assessment (LEADA), *Water Asset Management International*, *1* (1), 15-21.

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, http://www.slv.se/upload/dokument/livsmedelskontroll/dricksvatten/HANDBOK%20RSA%20DRICKSVATTENF%C3%96RS%C3%96RJNING%202007.pdf.

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

Techneau (2005). *Technology enabled universal access to safe water: Annex I - "Description of Work"*, Proposal/Contract no. 018320-02.

WHO (2004). *Guidelines for drinking-water quality. Vol. 1, Recommendations*, 3 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.

Yokoi, H., I. Embutsu, M. Yoda and K. Waseda (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., T.J.R. Pettersson and T.A. Stenström (2007). Identification and management of microbial contaminations in a surface drinking water source, *Journal of Water and Health*, *5* (1), 67-80.

Fault tree analysis for integrated and probabilistic risk analysis of drinking water systems

Lindhe, A., L. Rosén, T. Norberg and O. Bergstedt (2008).

Submitted to *Water Research*.

I

Fault tree analysis for integrated and probabilistic risk analysis of drinking water systems

Andreas Lindhe [a, *], Lars Rosén [a], Tommy Norberg [b], Olof Bergstedt [a, c]

[a] Department of Civil and Environmental Engineering, Chalmers University of Technology, SE-412 96 Göteborg, Sweden

[b] Department of Mathematical Sciences, Göteborg University and Chalmers University of Technology, SE-412 96 Göteborg, Sweden

[c] Göteborg Vatten, Box 123, SE-424 23 Angered, Sweden

* *Corresponding author*. Tel.: +46 (0)31 772 2060; fax: +46 (0)31 772 2107.
E-mail addresses: andreas.lindhe@chalmers.se (A. Lindhe), lars.rosen@chalmers.se (L. Rosén), tommy@chalmers.se (T. Norberg), olof.bergstedt@vatten.goteborg.se (O. Bergstedt).

ABSTRACT

Drinking water systems are vulnerable and subject to a wide range of risks. To avoid sub-optimisation of risk-reduction options, risk analyses need to include the entire drinking water system, from source to tap. Such an integrated approach demands tools that are able to model interactions between different events. Although fault tree analysis is a commonly used tool in risk analysis it is seldom applied to entire drinking water systems. Using fault tree analysis on an integrated level, a probabilistic risk analysis of a large drinking water system in Sweden was carried out. The primary aims of the study were: (1) to develop a method for integrated and probabilistic risk analysis of entire drinking water systems; and (2) to evaluate the applicability of Customer Minutes Lost (CML) as a measure of risk. The analysis included situations where no water is delivered to the consumer (quantity failure) and situations where water is delivered but does not comply with water quality standards (quality failure). Hard data as well as expert judgements were used to estimate probabilities of events and uncertainties in the estimates. The calculations were performed using Monte Carlo simulations. CML is shown to be a useful measure of risks associated with drinking water systems. The method presented provides information on risk levels, probabilities of failure, failure rates and downtimes of the system. This information is available for the entire system as well as its different sub-systems. Furthermore, the method enables comparison of the results with performance targets and acceptable levels of risk. The method thus facilitates integrated risk analysis and consequently helps decision-makers to minimise sub-optimisation of risk-reduction options.

Keywords: Drinking water system; risk analysis; fault tree; integrated; probabilistic; Customer Minutes Lost; uncertainties

1. INTRODUCTION

Efficient risk management is of primary importance to water utilities. Access to a reliable supply of drinking water and safe water quality are basic requirements for human health and economic development (IWA, 2004). In the third edition of the *Guidelines for Drinking-water Quality,* published by the World Health Organization (WHO), it is pointed out that a comprehensive risk assessment and risk management approach is the most effective way to ensure the safety of drinking water supply (WHO, 2004). To achieve an acceptable level of risk, it is crucial to analyse the risk and based on tolerability criteria evaluate the risk and alternative options for risk reduction.

As part of risk management, WHO recommends preparation of Water Safety Plans (WSPs), including *system assessment*, *operational monitoring* and *management plans* (Davison et al., 2005; WHO, 2004). To prioritise hazards, WHO suggests these be ranked using a risk matrix with discretised probability and consequence scales. This qualitative (or semi-quantitative) method is common in many disciplines and the main advantages are that it is simple to use and the result is easy to communicate. However, the method is not suitable for modelling complex systems with interactions between components and events. Burgman (2005) emphasises that risk-ranking methods assume a discrete nature of hazards, do not provide quantitative estimates and lack a procedure for uncertainty analysis, see also Cox (2008). To further support the WSP approach and risk management of drinking water systems in general, quantitative tools for risk analysis are also needed. A quantification of the risk facilitates, for example, comparison with other risks and acceptable levels of risk in absolute terms as well as quantitative estimations of the efficiency of risk-reduction options.

An important aspect when conducting risk analyses of drinking water systems is to consider the entire system, from source to tap (e.g. WHO, 2004). This means that the water source as well as the treatment system and the distribution network all the way to the consumers' taps should be taken into consideration. The main reasons for adopting an integrated approach are: (1) the existence of interactions between events, i.e. chains of events, needs to be considered; and (2) failure in one part of the system may be compensated for by other parts, i.e. the system has an inherent redundancy. If these circumstances are not considered, important information can be overlooked. In an integrated analysis it should be possible to compare the contribution made by different sub-systems to the risk in order to avoid sub-optimisation of risk-reduction options. It may not be worthwhile, for example, to increase the safety at an already efficient and safe treatment plant if no resources are spent on maintenance of the distribution system. Since resources for risk reduction are limited, it is necessary to prioritise and choose the most suitable option. The importance of an integrated approach is advocated by many, e.g. WHO (2004), IWA (2004), CDW/CCME (2004) and NHMRC/NRMMC (2004).

Fault tree analysis is a risk estimation tool with the ability to model interactions between events. A fault tree models the occurrence of an event based on the occurrence or non-occurrence of other events (Bedford and Cooke, 2001). This paper presents a method for integrated risk analysis of drinking water systems based on a probabilistic fault tree analysis. The fault tree method has been devised to estimate not only the probability of failure but also the mean failure rate and mean downtime of the system. Furthermore, the consequences of failures are included in the method and risk

levels are quantified using a measure called Customer Minutes Lost (CML). The method considers the entire supply system, from source to tap, and takes water quantity as well as water quality aspects into consideration. The primary aims of the study were: (1) to develop a method for integrated and probabilistic risk analysis of entire drinking water systems; and (2) to evaluate the applicability of CML as a measure of risk.

2. CONCEPTUAL MODEL

A drinking water system is commonly described as a supply chain composed of three main sub-systems: raw water, treatment and distribution. Together, these sub-systems cover the entire supply chain, from the water source to the consumers' taps. Along the supply chain there are hazards that may harm the system in different ways. The hazardous events may be different but their consequences are usually categorised as *quantity*- or *quality*-related. This means that either the ability to deliver water to the consumers or the water quality itself is affected. According to Gray (2005) the objective of water treatment is to produce an adequate and continuous supply of water that is chemically, bacteriologically and aesthetically acceptable. In addition to being bacteriologically safe, the water should also be microbiologically safe. It is not only pathogenic bacteria that may cause harm to public health; there are also viruses, protozoa and other biological contaminates. The objectives of water treatment can be divided into quantity and quality objectives and consequently they are in line with the two categories of consequences.

The overall failure event included in the method is *supply failure*, 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 comply with water quality standards. Figure 1 illustrates the two categories of failure as well as the main type of event that may cause these failures. Quantity failure may be caused either by component failure, e.g. pipe damage, or unacceptable water quality (raw water or drinking water) causing the water utility to stop the delivery. Quality failure may occur due to non-detection of unacceptable water quality and no action is thus possible, or due to unacceptable quality that is detected but no action is taken or it is not possible to stop delivery. The latter case may arise, for example, when the water utility decides to use raw water of unacceptable quality in order to avoid a water shortage.

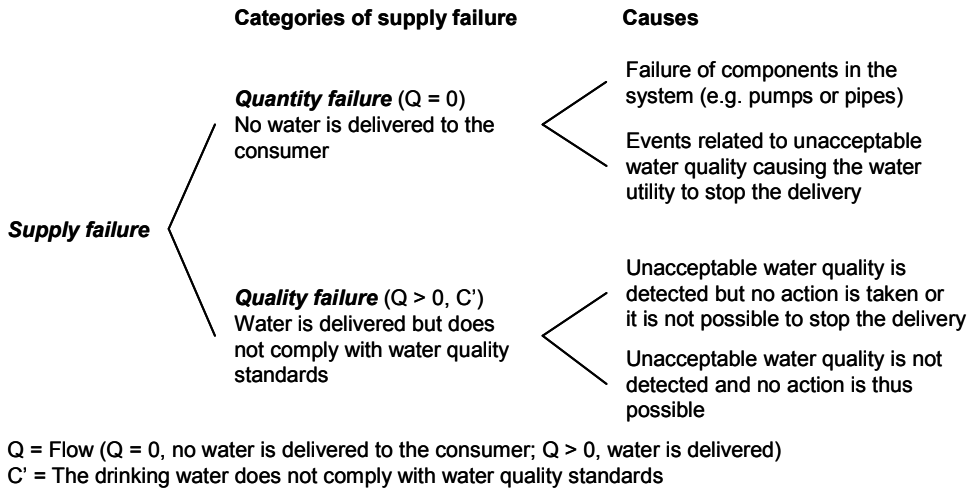

Figure 1. Categories of supply failure and their main causes.

Supply failure occurs because of events in one or more of the three main sub-systems (raw water, treatment and distribution). However, if failure occurs in one sub-system another may compensate and thereby prevent supply failure. Hence, to model a drinking water system its inherent ability to compensate for failure must be considered. For this reason the occurrence of failures could be as described in Figure 2. The figure includes the entire system, from source to tap, showing that failure may occur in any part of it. It also illustrates that the different sub-systems can compensate for failure. To determine the contribution made by each sub-system to the risk, failure in one part of the system is based on the assumption that the previous parts operate correctly (i.e. no failures in previous parts). It is assumed, for example, that no raw water failures have occurred when failures in the treatment are identified. Table 1 presents criteria for quantity as well as quality failures in the three sub-systems.

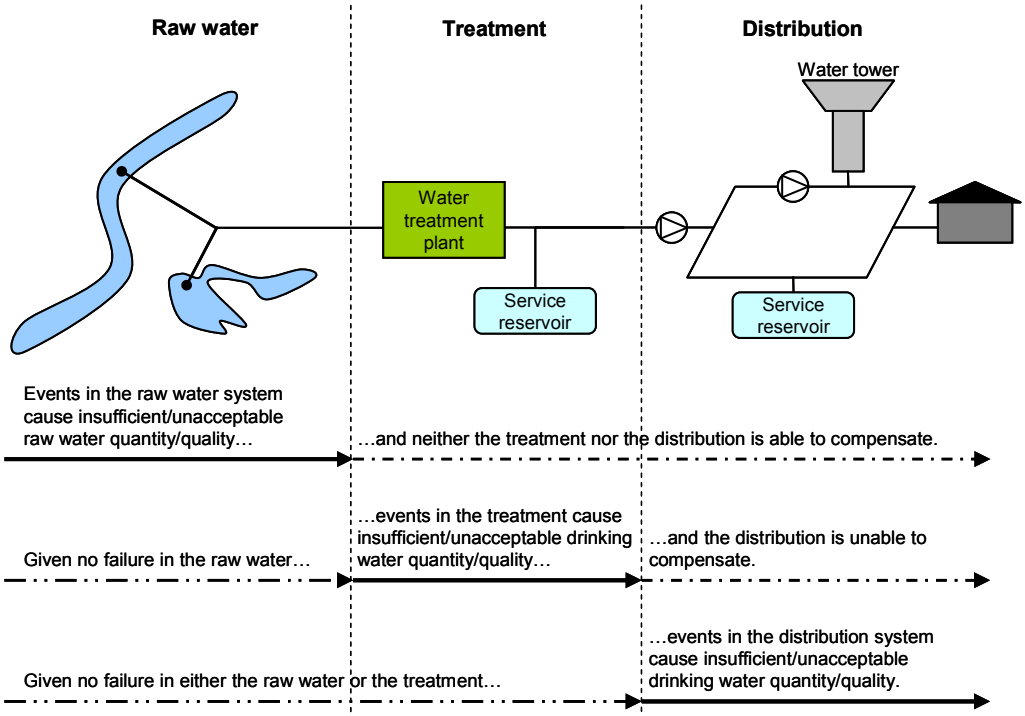

Figure 2. Illustration of how failures (quantity or quality) in different parts of the system may cause supply failure.

Table 1. Criteria for quantity and quality failures in raw water, treatment and distribution.

Sub-system	Category of failure	Failure criteria
Raw water	Quantity failure	○ Not enough raw water is transferred to the treatment plant(s), making it impossible to produce enough drinking water (the supply is less than the demand). ○ Treatment and distribution are unable to compensate.
	Quality failure	○ The raw water quality does not comply with health-based water quality standards. ○ Treatment and distribution are unable to compensate.
Treatment	Quantity failure	○ No raw water quantity failure. ○ The water transferred from the treatment plant(s) is less than the demand. ○ Distribution is unable to compensate.
	Quality failure	○ No raw water quality failure. ○ The drinking water produced does not comply with health-based water quality standards. ○ Distribution is unable to compensate.
Distribution	Quantity failure	○ No raw water or treatment quantity failure. ○ Water cannot be delivered to the consumer.
	Quality failure	○ No raw water or treatment quality failure. ○ The water quality does not comply with health-based water quality standards.

3. FAULT TREE ANALYSIS

A fault tree analysis is a structured process that identifies potential causes of system failure. A fault tree illustrates the interactions between different events using logic gates, and shows how the events may lead to system failure, i.e. the top event. The *top event* is a critical situation that causes system failure and the occurrence of the top event is described in terms of occurrence or non-occurrence of other events (Bedford and Cooke, 2001). Starting with the top event, the tree is developed until the required level of detail is reached. Events whose causes have been further developed are *intermediate events*, and events that terminate branches are *basic events*. While the top event can be seen as a system failure, the basic events are component failures. For a further description of fault tree analysis and its application in risk analysis see e.g. Rausand and Høyland (2004) and Bedford and Cook (2001).

In order to structure the fault tree of a drinking water system, four types of logic gates were identified. A Markovian approach was used with mean failure rate λ and mean downtime $1/\mu$ (see e.g. Rausand and Høyland, 2004). The mean time to failure is $1/\lambda$, and μ can be regarded as the repair rate, hence the probability of failure can be written as $P_F = \lambda/(\lambda + \mu)$. By replacing each base event in the logic gates with a Markov Process, equations for calculating the mean failure rate and mean downtime for the output events were developed. One of the main reasons for using the failure rate and downtime, and not just the probability of failure, is to facilitate elicitation of expert judgements. Since both the failure rate and downtime need to be considered when estimating the probability, these are estimated separately to maintain transparency. Norberg et al. (2008) present a comprehensive description of the theoretical foundations of the logic gates presented here.

3.1. OR-gate

The output of an OR-gate (Figure 3) occurs if at least one of the input events occurs. The OR-gate corresponds to a series system with *n* independent events where the probability of failure can be calculated using Equation 1. Supply failure, for example, may occur if there is failure in the raw water, treatment or distribution systems. Only one of the sub-systems needs to fail to cause supply failure. Using the mean failure rates and mean downtimes of the input events, Equations 2-4 are used to calculate the output event of an OR-gate.

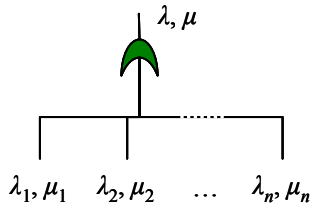

Figure 3. Fault tree with an OR-gate.

$$P_F = 1 - \prod_{i=1}^{n} (1 - P_i) \tag{1}$$

$$\lambda = \sum_{i=1}^{n} \lambda_i \tag{2}$$

$$\mu = \sum_{i=1}^{n} \lambda_i \cdot \frac{\prod_{i=1}^{n} \mu_i}{\prod_{i=1}^{n} (\lambda_i + \mu_i) - \prod_{i=1}^{n} \mu_i} \tag{3}$$

$$P_F = \frac{\lambda}{\lambda + \mu} = 1 - \prod_{i=1}^{n} \frac{\mu_i}{\lambda_i + \mu_i} \tag{4}$$

3.2. AND-gate

An AND-gate (Figure 4) is used to model events that must occur simultaneously in order for the output event to occur. The AND-gate corresponds to a parallel system where the probability of failure is calculated as the product of the *n* independent events' probabilities, see Equation 5. For example, if a water utility can use raw water from two different water sources, both must be unavailable to cause raw water shortage (provided that one source is sufficient to meet the water demand). The output event of an AND-gate is calculated using Equations 6-8.

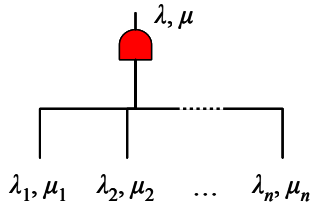

Figure 4. Fault tree with an AND-gate.

$$P_F = \prod_{i=1}^{n} P_i \tag{5}$$

$$\mu = \sum_{i=1}^{n} \mu_i \tag{6}$$

$$\lambda = \sum_{i=1}^{n} \mu_i \cdot \frac{\prod_{i=1}^{n} \lambda_i}{\prod_{i=1}^{n} (\lambda_i + \mu_i) - \prod_{i=1}^{n} \lambda_i} \tag{7}$$

$$P_F = \frac{\lambda}{\lambda + \mu} = \prod_{i=1}^{n} \frac{\lambda_i}{\lambda_i + \mu_i} \tag{8}$$

3.3. Variants of the AND-gate

To adequately model a system's inherent ability to compensate for failure, the AND-gate needs to be extended. It must include what in reliability applications is called *cold standby* and *imperfect switching*. If, for example, a pump station supplying a high altitude area with drinking water breaks down, water stored in the water tower can supply the consumers for a limited time. If the water tower is not in use due, for example, to failure or maintenance work, the water tower cannot compensate at all for failure (failure on demand). When the water tower operates normally and does not fail on demand, it is able to compensate until a failure occurs or it is emptied (failure during operation). The first variant of the AND-gate (Figure 5) is designed primarily for situations when the ability to compensate is limited in time. The output event of the first variant of the AND-gate is calculated using Equations 9-11, where q is the probability of failure on demand, and the mean failure rate (λ) is used to model failure during operation.

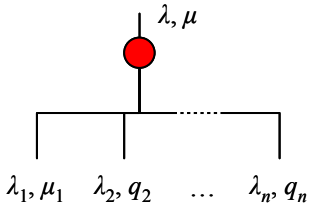

Figure 5. The first variant of the AND-gate, including the ability of the system to compensate for failure.

$$\mu = \mu_1 \tag{9}$$

$$P_F = \frac{\lambda_1}{\lambda_1 + \mu_1} \cdot \prod_{i=2}^{n} \frac{\lambda_i + q_i \mu_1}{\lambda_i + \mu_1} \tag{10}$$

$$\lambda = \frac{P_F}{1 - P_F} \cdot \mu \tag{11}$$

A second variant of the AND-gate is needed to model situations where the ability to compensate may recover after it has failed. This may arise, for example, when raw water of unacceptable quality is used but may be compensated for by treatment. If the unacceptable water quality cannot be compensated for at all, failure on demand arises.

However, if the unacceptable quality can be compensated for, failure does not arise until the treatment efficiency is affected due to failure in the treatment. When the failure has been taken care of, the treatment recovers and is able to compensate again until a new failure occurs. The output event of this second variant of the AND-gate (Figure 6) is calculated using Equations 12-14. The equations apply only when one component compensates for failure. If multiple components could compensate, a regular AND-gate can be used to combine the events. The output of the regular AND-gate is used as the compensating input event in the second variant of the AND-gate.

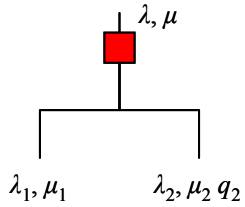

Figure 6. The second variant of the AND-gate, including a component's ability to recover after failure.

$$P_F = \frac{\lambda_1}{\lambda_1 + \mu_1} \cdot \frac{\lambda_2 + q_2(\mu_1 + \mu_2)}{\lambda_2 + \mu_1 + \mu_2} \quad (12)$$

$$\lambda = \frac{\mu_1 \lambda_1 q_2(\lambda_2 + \mu_1 + \mu_2) + \lambda_1 \lambda_2 (1 - q_2)(\mu_1 + \mu_2)}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_1 + \mu_2)(1 - P_F)} \quad (13)$$

$$\mu = \frac{\mu_1 \lambda_1 q_2(\lambda_2 + \mu_1 + \mu_2) + \lambda_1 \lambda_2 (1 - q_2)(\mu_1 + \mu_2)}{(\lambda_1 + \mu_1)(\lambda_2 + \mu_1 + \mu_2) P_F} \quad (14)$$

4. GENERIC FAULT TREE STRUCTURE OF A DRINKING WATER SYSTEM

The conceptual model and the logic gates form the basis for a generic fault tree structure of a drinking water system. Figure 7 illustrates possible failure paths. When the system operates normally, failure may occur in any of the three sub-systems and given failure in one sub-system another can either compensate or fail to compensate. It is also possible for more than one sub-system to fail at the same time. To simplify the figure, *no compensation* or *failure* is treated as the same event when the previous sub-system has failed. These two events could have been illustrated separately but since both cause failure they are merged here.

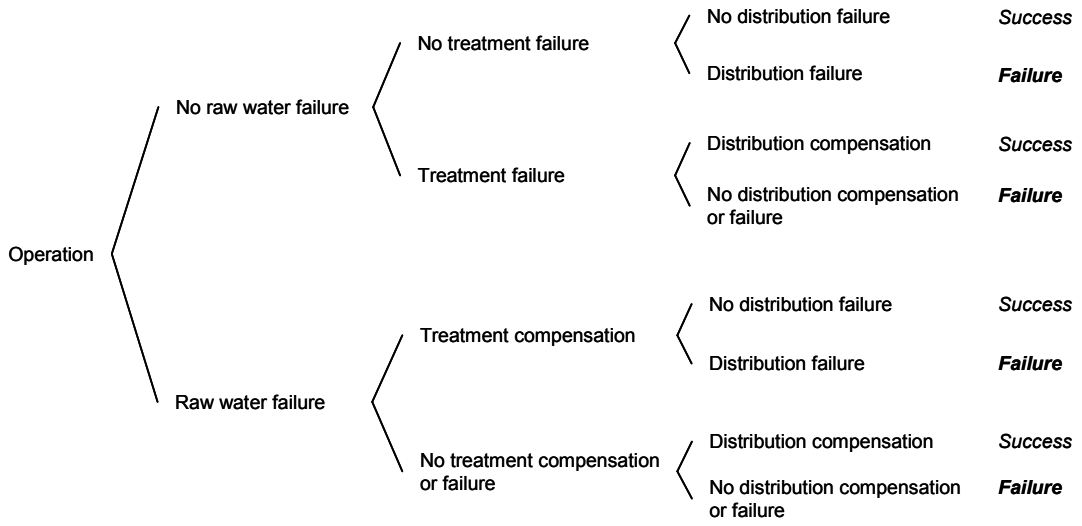

Figure 7. Possible paths leading to failure (quantity or quality). Each branch illustrates a situation where failure occurs or does not occur and compensation is possible or not possible.

Based on the alternatives in Figure 7, a generic fault tree structure applicable to drinking water systems is suggested (Figure 8). The system is broken down into its three main sub-systems, and the top event, *supply failure*, may occur due to failure in any one of them. In each sub-system, quantity or quality failures may occur. The first variant of the AND-gate is used to illustrate that failure (quantity or quality) in one sub-system may be compensated for by other sub-systems. A drinking water system can thus not be considered a traditional series system, where failure in one sub-system automatically causes system failure. The transfer gates in Figure 8 indicate that the fault tree is further developed elsewhere (Figure 9). Although the same transfer gates can be found in all three sub-systems, they do not refer to exactly the same events. For example, component failure in the treatment is not exactly the same event as component failure in the distribution. The generic fault tree structure (Figure 8 and Figure 9) includes the major events and the relationships between them. However, in a practical application the events need to be developed further for the structure to correspond properly to system properties and enable estimations to be made of the required variables for the basic events.

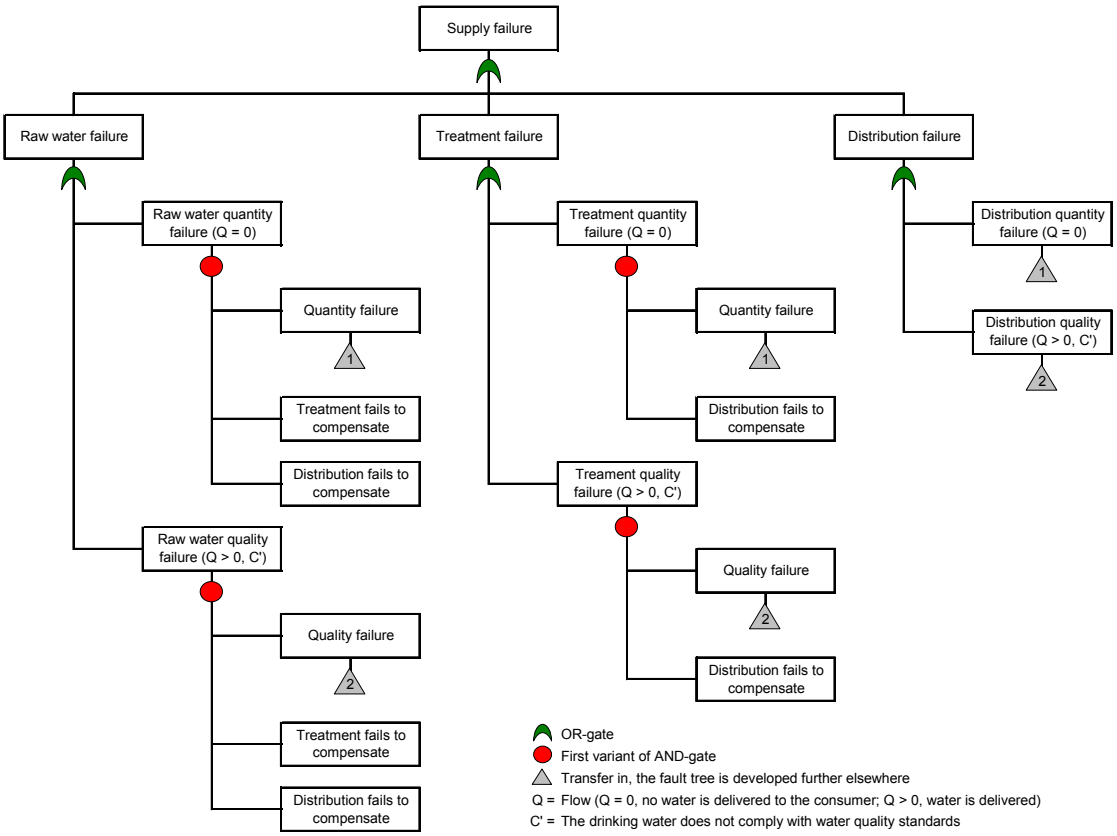

Figure 8. Generic fault tree illustrating the two categories of failure in the three sub-systems. The transfer in gates (1 and 2) refer to the transfer out gates in Figure 9.

Figure 9 shows that quantity failure occurs due to component failure or unacceptable water quality. For the unacceptable quality to cause quantity failure, three events need to occur simultaneously: the water quality needs to be unacceptable, the unacceptable quality needs to be detected and the water utility needs to decide to stop the delivery. If the water utility decides not to stop the delivery, a quality failure occurs instead (Figure 9). Quality failure may also occur when the water quality is unacceptable although the quality deviation is not detected and hence no action is possible.

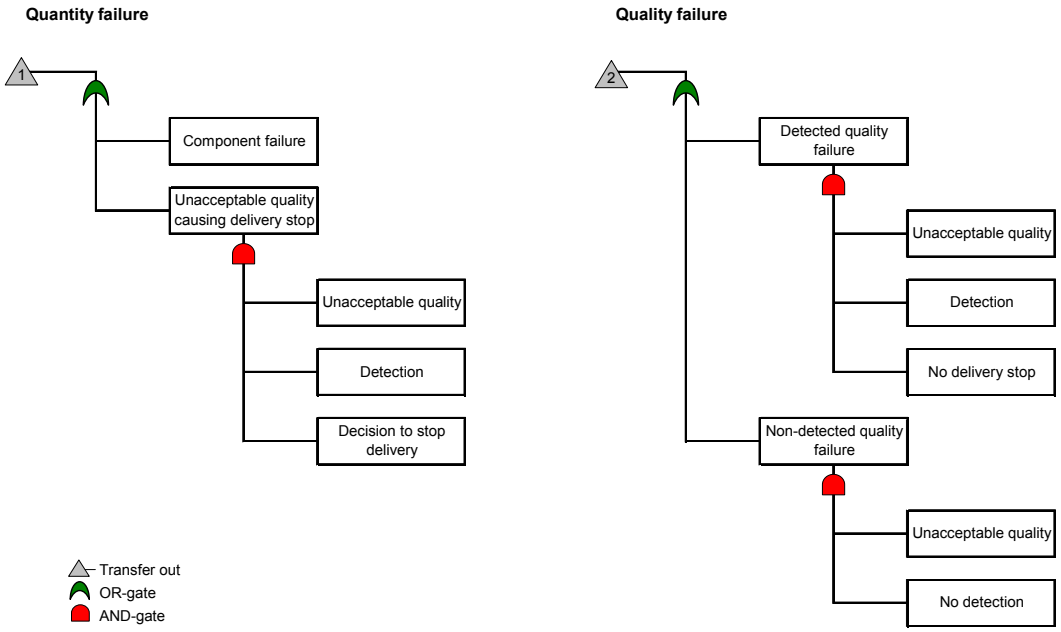

Figure 9. Schematic illustration of how quantity (1) and quality (2) failures may occur. The transfer out gates refer to corresponding transfer in gates in Figure 8.

5. ESTIMATION OF RISK

5.1. Risk

According to Kaplan and Garrick (1981), see also Kaplan (1997), the question "What is the risk?" actually comprises three questions: "What can happen?"; "How likely is it?"; and "What are the consequences?". Hence, the answers to these three questions together describe the risk. According to this widely accepted description, risk is expressed as a combination of the frequency, or probability, of occurrence and the consequences of a hazardous event, see e.g. IEC (1995), ISO/IEC (2002) and the European Commission (2000).

5.2. Risk as Customer Minutes Lost

For the purpose of this study, the consequences of failures (quantity and quality) are defined by *the duration of failure* and *number of people affected.* Since two attributes are used to describe the consequences, the evaluation of the results can be described as a multi-attribute problem. By multiplying the two attributes, the consequences are expressed in terms of *Customer Minutes Lost* (CML). In order to maintain transparency the estimated number of CML, as well as other results of the analysis, are presented separately for quantity and quality failure. The risk, expressed as the expected CML, is calculated as

$$R = \lambda \cdot \frac{1}{\mu} \cdot C, \qquad (15)$$

where λ is the mean failure rate, $1/\mu$ the mean downtime and C the expected proportion of consumers affected by failure. Since C is expressed as a proportion, the risk is estimated for the average consumer. When estimating the risk in terms of CML, the utility of the two attributes used to define the consequence (affected proportion of consumers and mean downtime) is assumed to be independent. Note that Equation 15 is an approximation, valid when $1/\mu << 1/\lambda$. To consider that a

system cannot fail when it is in its failure mode, the true failure rate should be calculated as

$$\omega = \frac{1}{\frac{1}{\lambda} + \frac{1}{\mu}} = \frac{\lambda\mu}{\lambda + \mu}. \qquad (16)$$

When based on the true failure rate (ω), the risk is expressed as

$$R = \frac{\lambda\mu}{\lambda + \mu} \cdot \frac{1}{\mu} \cdot C = \frac{\lambda}{\lambda + \mu} \cdot C. \qquad (17)$$

The probability of failure is defined as $P_F = \lambda/(\lambda + \mu)$, and Equation 17 is therefore equivalent to

$$R = P_F C. \qquad (18)$$

The risk is consequently calculated as the probability of failure multiplied by the proportion of consumers affected. However, it is not meaningful to define the affected proportion of consumers only at the top event (supply failure). Instead, a lower and suitable level for defining consequences must be identified. This level should be as close as possible to the top event and only have events that are combined by means of OR-gates above it. It is also important that an intermediate event, of which the consequences are defined, does not include events with totally different consequences. If these criteria are fulfilled the total risk may be calculated as a sum of the risks caused by different events. In the generic fault tree (Figure 8), it is suitable to define consequences for each type of failure (quantity and quality) in the three sub-systems. The fault tree in Figure 8 is generalised and in a real-world application the quantity and quality failures for each sub-system are preferably divided into different main types of event. These main types of event would constitute a suitable level for defining consequences. Since the consequences are defined for several (n) events, the total risk is

$$R = \sum_{i=1}^{n} P_{Fi} C_i. \qquad (19)$$

If the affected proportions of consumers are defined at a level in the fault tree where it is plausible that some of the events may occur simultaneously, the risks posed by the events may not be additive and Equation 19 may not be valid. It should be noted that two events with different probabilities, durations and number of people affected, may cause the same level of risk (expressed as CML). CML has previously been used as a performance indicator in the drinking water sector in the Netherlands (Blokker et al., 2005).

6. UNCERTAINTIES AND INPUT DATA

The method presented is probabilistic and therefore all input variables are replaced by probability distributions. A Bayesian approach is applied and the risk is calculated by means of Monte Carlo simulations, taking uncertainties of estimations into consideration (Figure 10).

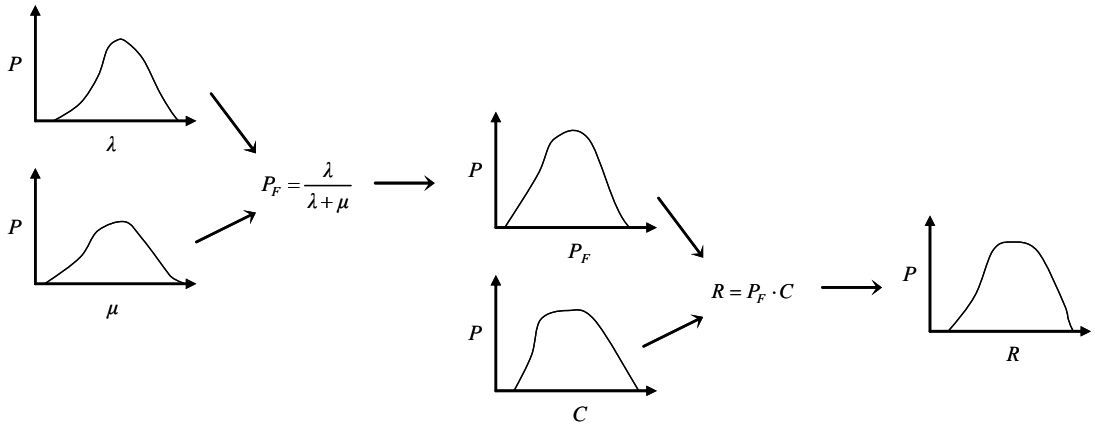

Figure 10. Illustration of how the uncertainties are taken into consideration when calculating the risk using Monte Carlo simulations.

Variables λ and μ are modelled as exponential rates using Gamma distributions. The use of constant failure rates is justified by the continuous maintenance being done by the water utility. The proportion of consumers affected (C) and the probability of failure on demand (q) are modelled by Beta distributions. The main reason for using Gamma and Beta distributions is the fact that they are conjugate to the exponential and binomial models respectively. This means, for example, that a prior Gamma distribution updated with hard data results in a posterior Gamma distribution. Hence, the distributional classes of the prior and posterior distributions are the same. The use of conjugate distributions thus facilitates a Bayesian approach, in which hard data can be used for a mathematically formal updating of previous knowledge. Furthermore, the Beta and Gamma distributions are flexible and capable of attaining a vide variety of shapes.

Hard data, such as measurements and statistics on events, expert judgements and combinations of these, are used as input data in the fault tree analysis. Expert judgements are used when hard data is not available or too limited. The experts, mainly water utility experts, are asked to estimate a plausible maximum and minimum value of the variable of interest. These estimates are used as percentiles when estimating the distribution. However, mean or median values should also be considered to ensure that a suitable distribution is obtained. The use of variables λ and μ to calculate the probability of failure facilitates expert judgements. Instead of estimating the probability of failure, which can be difficult, the experts estimate the mean failure rate (λ) and mean duration of failure ($1/\mu$), and based on this the probability of failure is calculated as $P_F = \lambda/(\lambda+\mu)$.

7. METHOD APPLICATION

An integrated and probabilistic fault tree analysis was conducted for the drinking water system in Gothenburg, Sweden. By applying the method in a system as extensive and complex system as in Gothenburg, it was tested and conditions specific to drinking water systems were incorporated. The method application is presented here with a focus on methodological aspects. Lindhe et al. (2008) presented the application in Gothenburg with a focus on aspects of the specific drinking water system.

7.1. Gothenburg water supply

Gothenburg is the second largest city in Sweden and approximately 500,000 people are supplied with drinking water. The raw water supply is solely based on surface water. The main water source is a river, although a number of lakes are also used as reservoirs and reserve water sources. The system includes two treatment plants with roughly the same production capacity and similar treatment processes, including chemical flocculation, sedimentation, filtration and disinfection. The distribution network is approximately 1,700 km in length and, to assure sufficient pressure in network areas at high altitudes, the water head is raised through booster stations. To meet peaks in the water demand, service reservoirs are used. The water quality in the river and the treatment plants is monitored online. Additional analyses, e.g. microbial, are also made in the water sources and at the treatment plants and different locations in the distribution system.

7.2. Fault tree structure

The fault tree of the Gothenburg system was based on the generic fault tree structure presented in Section 4. Supply failure may thus occur in the raw water, treatment or distribution (Figure 8). Within each sub-system, quantity and quality failures may occur. The first variant of the AND-gate was used to model failure in one sub-system being compensated for by other sub-systems. The failure events as well as the structure of the fault tree were identified and compiled in close collaboration with water utility personnel. Both previous and possible future events were included. The drinking water quality was considered unacceptable when unfit for human consumption, a criterion based on the Swedish quality standards for drinking water (SLVFS 2001:30). In total, the fault tree was composed of 116 basic events, 100 intermediate events and 101 logic gates.

The raw water part of the fault tree was structured to illustrate which of the two treatment plants is affected by failure. For quantity failure to occur all raw water sources must be unavailable for at least one treatment plant and the treatment and distribution systems must fail to compensate. The traditional AND-gate was used to model that all water sources must be simultaneously unavailable. In addition, the first variant of the AND-gate was used to model the ability to compensate for failure by means of increased production capacity at the non-affected treatment plant as well as stored water in service reservoirs at the treatment plants and in the distribution system.

To model quality failures in the raw water the second variant of the AND-gate was used. Hence, unacceptable raw water quality may be compensated for by the treatment. The probability that unacceptable water quality cannot be compensated for at all was represented by the probability of failure on demand. Estimates of the failure rate and downtime, i.e. how often the treatment efficiency is affected and for how long, was provided by the treatment part of the fault tree.

Quantity failure in the treatment may also be compensated for by means of increased production capacity at the non-affected treatment plant and service reservoirs at the treatment plants and in the distribution system. There is no subsequent sub-system that could compensate for failure in the distribution. However, the distribution system itself may compensate for quantity failures. If, for example, water cannot be

transferred to a delivery zone due to pump failure, water stored in water towers in that zone may be used.

7.3. Tolerability criteria

When risks have been analysed they need to be evaluated to determine whether the level of risk is acceptable or not. Sometimes tolerability criteria already exist whereas in other cases an acceptable level of risk needs to be defined for the specific analysis at hand. A combination of the two alternatives may also be required.

The City of Gothenburg has worked out an action plan which, among other things, includes performance targets for the supply of drinking water (Göteborg Vatten, 2006). These targets are politically established and can be considered as acceptable levels of risk. One target related to the reliability of the supply, i.e. water quantity, is defined 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.

This target corresponds to an acceptable risk level of 144 CML per year for the average consumer. In the result section this target is compared with the results of the fault tree analysis.

8. RESULTS

The calculations were performed using Monte Carlo simulations (10,000 iterations) and the main results are summarised in Figure 11. The risk level (expected value of CML), probability of failure, mean failure rate and mean downtime are presented for the entire system as well as the three sub-systems. The results are presented separately for quantity and quality failure.

The results show that the total risk level (CML) is mainly due to raw water failures. This is valid for both quantity and quality failure. The reason for this is long downtimes and the fact that a large number of people are affected when the first part of the supply chain fails. It should be noted that the probability of failure is a function of the mean failure rate and mean downtime. However, by studying all three variables additional information is obtained.

The probability of failure differs between the sub-systems and the probability of distribution failure is highest. Hence, the total probability of failure is governed mainly by the probability of distribution failure. Similar to the probability of failure, the total failure rate is influenced mostly by the frequent distribution failures. For quantity as well as quality failure, the mean downtime is highest for the raw water sub-system. However, the frequent failures in the distribution system have a short mean downtime and consequently the total mean downtime is in approximately the same range as the distribution failures.

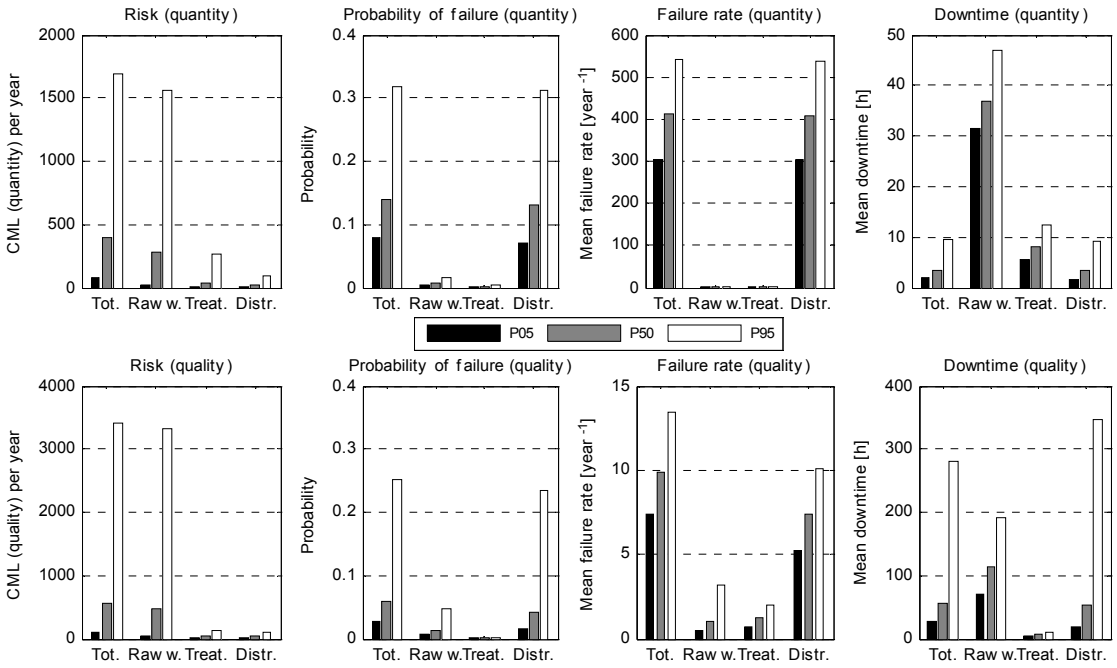

Figure 11. Histograms showing the 5-, 50- and 95-percentiles for quantity and quality failure. For each of the four variables the result is presented for the entire system (Tot.) as well as the three main sub-systems. Note that the scales are not the same for quantity and quality failure.

Figure 11 also shows the uncertainty of the results and for some variables there is a large difference between the percentiles, indicating a high degree of uncertainty in the results. The probabilistic approach also enabled a comparison of the quantity-related total risk level with the acceptable level of risk defined by the City of Gothenburg. Figure 12 shows the quantity-related CML, including uncertainties, and the tolerability criterion. The probability of exceeding the criterion is 0.84.

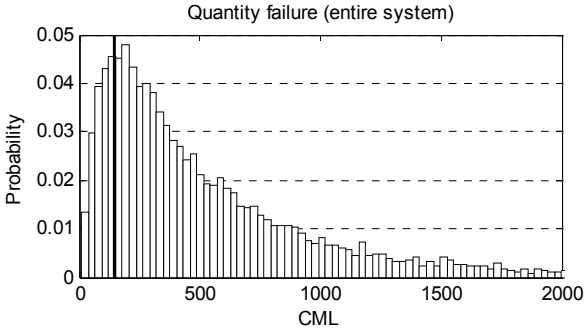

Figure 12. Uncertainty distribution of quantity-related CML for the entire system. The acceptable level of risk (144 CML per year for the average consumer) is indicated by a solid vertical line and the probability of exceeding the acceptable level is 0.84.

In addition to the quantified risk levels and other calculated variables, the fault tree can be analysed qualitatively. By studying the structure of the fault tree, information on what may cause failure and the interaction between different events and parts of the systems is provided. Hence, a person not involved in the fault tree construction can acquire valuable information by studying the fault tree.

9. DISCUSSION

For the Gothenburg system it was shown that the raw water system contributes most to the total risk level, expressed as CML, although it is the distribution system that contributes most to the probability of failure due to frequent failures. These finding are confirmed by existing knowledge of the system. By studying not only the level of risk but also the probability of failure, failure rate and downtime, information on the dynamic behaviour of the system is provided. A traditional fault tree analysis, not applying the Markovian approach and including the consequences, would only have provided information on the probability of failure and the dynamic behaviour of the system would not have been possible to calculate.

It is also important to study not only the results for the top event but also at lower levels in the fault tree. For example, the three sub-systems should be compared to see in what way they contribute to the risk. The results for the Gothenburg system show that the probability of raw water failure is low but when a failure occurs the mean downtime is long and many people are affected. The treatment has a low mean failure rate, short mean downtime and little impact on the total risk. The distribution system causes frequent failures but due to the short mean downtime and few people affected its contribution to the total risk is small.

Two sub-systems may cause the same number of CML but the probability of failure and the number of people affected may differ. Two sub-systems may also have the same probability of failure but different failure rates and downtimes. Properties like these can be identified using the fault tree and are important to know about when evaluating a system and suggesting ways of reducing the risk.

A fault tree should be constructed so that it represents circumstances of the actual system instead of being fitted to actual data. When hard data is missing or insufficient, expert judgements must be used. The fault tree construction is an iterative process where the structure and the results are evaluated continuously to ensure that a proper model is developed. A fault tree model makes it possible to evaluate each basic event as well as the intermediate events, depending on which is most suitable.

Uncertainty is an important part of the concept of risk and the probabilistic approach used in this method enables different types of uncertainty analysis. First of all, uncertainties regarding the results provide information on the variation in the calculated variables. The uncertainties may, for example, be due to modelling uncertainties, variable uncertainty or natural variability. The simulation approach also facilitates calculations of rank correlation coefficients. The rank correlation coefficients show how much each variable in the model contributes to the uncertainty of the result. The rank correlation coefficient can thus be used to identify where in the model new information is most, and least, valuable in reducing uncertainties in the results. Consequently, this information can be used to guide further studies. The probabilistic approach also enables, for example, calculation of the probability of exceeding acceptable levels of risk. The application to the Gothenburg system showed that the probability of exceeding the quantity-related criterion was 0.84. Results of this nature provide the decision-maker with additional information. It is not only important to define a tolerable level of risk but also a level of certainty by which the risk should not be exceeded.

The calculation of CML was possible since estimates of the affected proportions of consumers were included in the fault tree. The use of CML as a measure of risk is based on the assumption that the uncertainties of the probability of failure and the affected proportion of consumers are independent. Furthermore, the use of CML implies that two events that cause the same level of risk but have different failure rates, downtimes and affect different numbers of people, are regarded as being equally severe. In order to distinguish such events from each other, the calculated CML values should be evaluated together with information on the probabilities of failure and/or affected proportions of consumers. Since the probability of failure is defined by the failure rate and downtime of the system, these variables provide additional information that is important to consider when evaluating the results.

The model does not quantify the actual health risk and the CML related to quality does not include the health effect of drinking water that does not comply with quality standards. However, since the CML related to quality corresponds to the minutes per year that the average consumer is exposed to drinking water not complying with quality standards, it provides valuable information. The CML related to quality could, for example, be one important input in a Quantitative Microbial Risk Assessment (QMRA). In the Gothenburg case the criterion for quality failure was defined as *unfit for human consumption*. This criterion can be defined differently depending on the purpose of the study. Combining a QMRA with a detailed system description, represented by a fault tree model, enables a focused search for best options to reduce the health risk, which would otherwise have been very difficult. It is also possible to learn from actual quality failures by detailing them using a fault tree, see e.g. Risebro et al. (2007). The information gained can then be used to improve fault tree models for similar systems.

Due to the function of a drinking water system, it cannot be regarded as a simple series system where failure in one part of the system automatically affects the consumer. Consequently, integrated analyses, including the entire system and its ability to compensate for failure, are required. The fault tree method presented facilitates integrated risk analysis of drinking water systems and thus also minimises sub-optimisation of risk-reduction options. An advantage of the fault tree method is that, in addition to providing risk estimations, it can also be used to evaluate risk-reduction options. By changing the fault tree structure, e.g. adding events or changing the input data, risk-reduction options can be modelled (Rosén et al., 2008). The Bayesian approach, using Beta and Gamma distributions, enables a mathematically formal updating of previous knowledge as new hard data becomes available. Hence, expert judgements can be combined with hard data and the model can be updated continuously.

Compared to simpler methods for risk analysis, such as risk ranking by using risk matrices with discretised probability and consequence scales, the fault tree method enables modelling of chains of events and interconnections between events. The fault tree method also quantifies the level of risk and the dynamic behaviour of the system, which facilitates comparison with other risks and acceptable levels of risk. However, since risk ranking and the fault tree method provide different results and the latter method requires more time, data and need for training, the methods fulfil different demands.

10. CONCLUSIONS

The main conclusions of this study are:

- The fault tree method presented here can be used to perform integrated risk analysis of drinking water systems from source to tap. It includes the inherent ability of the system to compensate for failure. Hence, it supports decision-makers in the task of minimising sub-optimisation of risk-reduction options.
- Customer Minutes Lost (CML) is shown to be a valuable measure of risk since performance targets (acceptable levels of risk) can be defined using this measure. However, since different probability and consequence values can result in the same risk, calculated CML values should be analysed and compared in combination with information on the probabilities of failure and/or consequences.
- The possibility to not only estimate the probability of failure but also the mean failure rate and mean downtime at each intermediate level of the fault tree, provides valuable information about the dynamic behaviour of the system.
- The probabilistic approach enables uncertainty analysis and calculations of the probability of exceeding defined performance targets and acceptable levels of risk.
- Incorporation of expert judgements is facilitated by using the mean failure rate and mean downtime to model estimates of probabilities. The use of Gamma and Beta distributions enables a Bayesian approach with mathematically formal updating of the analysis as new hard data becomes available.

The construction of the fault tree, analysis of available data, expert judgements and the analysis of results facilitate discussions of risk as well as the function of the system. Hence, it should be stressed that not only the results of the calculations are valuable but also the actual process of performing the fault tree analysis. This, in combination with the ability to model risk-reduction options, makes the fault tree method an important source of support in decision-making.

ACKNOWLEDGEMENTS

This study has been carried out within the framework of the TECHNEAU project (Technology Enabled Universal Access to Safe Water), funded by the European Commission (contract number 018320), and with support from the Swedish Water & Wastewater Association and the City of Gothenburg. The authors would like to thank the City of Gothenburg for its valuable and fruitful collaboration.

REFERENCES

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

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

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

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.

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

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

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

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

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

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

ISO/IEC (2002). *Guide 73 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.

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

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

Lindhe, A., L. Rosén, T. Norberg, T.J.R. Pettersson, O. Bergstedt, J. Åström and M. Bondelind (2008). Integrated risk analysis from source to tap: Case study Göteborg, Paper presented at the *6th Nordic Drinking Water Conference*, Oslo, 9-11 June.

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.

Norberg, T., L. Rosén and A. Lindhe (2008). Added value in fault tree analyses (*In press*), European Safety and Reliability Association 2008 and 17th Society for Risk Analysis Europe Conference, Valencia, 22-25 September.

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

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

Rosén, L., O. Bergstedt, A. Lindhe, T.J.R. Pettersson, A. Johansson and T. Norberg (2008). Comparing Raw Water Options to Reach Water Safety Targets Using an Integrated Fault Tree Model, Paper presented at the International Water Association Conference, Water Safety Plans: Global Experiences and Future Trends, Lisbon, 12-14 May.

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

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

Integrated risk analysis from source to tap: Case study Göteborg

Lindhe, A., L. Rosén, T. Norberg, T.J.R. Pettersson, O. Bergstedt, J. Åström and M. Bondelind (2008).

Revised version of paper in proceedings of the *6th Nordic Drinking Water Conference*, Oslo, 9-11 June, 231-241.

II

Integrated risk analysis from source to tap: Case study Göteborg

Andreas Lindhe*, Lars Rosén*, Tommy Norberg, Thomas J. R. Pettersson*, Olof Bergstedt***, Johan Åström* and Mia Bondelind***

* Department of Civil and Environmental Engineering, Chalmers University of Technology, SE-412 96 Göteborg, Sweden; andreas.lindhe@chalmers.se.

** Department of Mathematical Sciences, Göteborg University and Chalmers University of Technology, SE-412 96 Göteborg, Sweden.

*** Göteborg Vatten, Box 123, SE-424 23 Angered, Sweden; Department of Civil and Environmental Engineering, Chalmers University of Technology, SE-412 96 Göteborg, Sweden.

Abstract.

To achieve an efficient risk management of a drinking water system the entire system has to be considered, from source to tap. An important part of risk management is to identify hazards and estimate risks, i.e. to conduct risk analyses. In order to provide a relevant basis for evaluating risks and efficiently prioritising risk-reduction options, a risk analysis needs to properly consider interaction between different parts and components of the system. This is especially important in complex systems. Logic tree models have the capability of properly reflect system functionality as well as facilitating quantification of risk levels. A fault tree model was therefore constructed for an integrated and probabilistic risk analysis of the drinking water system in Göteborg, Sweden. The main (top) event studied in the analysis was supply failure, which included quantity and quality failures. Quantity failure occurs when no water is delivered to the consumer and quality failure when water is delivered but unfit for human consumption according to existing water quality standards. Hard data and expert judgements were used for estimating probabilities of events, consequences and uncertainties of estimates. Monte Carlo simulations were used for the calculations in order to facilitate uncertainty analysis of risk levels. The risk analysis provided information on the probability of failure, mean failure rate and mean downtime of the system. The number of people affected was also included in the fault tree and risk levels were expressed as Costumer Minutes Lost. The primary aims of this paper were to apply a fault tree method, for integrated and probabilistic risk analysis of drinking water systems, to the system in Göteborg and show how the results can be used. The results showed, for example, that the raw water part contributes most to the total risk level and that the distribution part includes frequent failures that most often have a short duration and affect a small number of people. The method was found to facilitate a quantitative and integrated risk analysis of the drinking water system and the results provide information not only on risk levels, but also on the dynamic behaviour of the system. In addition, the method is capable of relevant handling interaction of system components. Furthermore, it provides transparency and facilitates for formal updating when new information becomes available. Hence, it is concluded that the method provides useful information for discussing and evaluating risks as well as possible risk-reduction options.

Introduction

Risk management is becoming increasingly important within the water utility sector. Access to reliable supply and safe quality of drinking water are basic requirements for human health and economic development (IWA, 2004). The World Health Organization (WHO) emphasises in the third edition of the *Guidelines for Drinking water Quality* the importance of using a risk-based approach, when managing drinking water systems, and to consider the entire supply system, from the water source to the consumers' taps (WHO, 2004). The integrated approach, i.e. from source to tap, is important since events in different parts of the system influence each other and failure in one part may be compensated for by other parts. Therefore, chains of events as well as the inherent ability of the system to compensate for failure have to be considered when analysing risks. If different parts of the system are studied separately and not

properly compared, this may cause a suboptimal prioritisation of risk-reduction options and consequently an inefficient use of available resources.

To facilitate integrated risk analyses of drinking water systems and the Water Safety Plan (WSP) approach as presented by WHO (2004) and Davison *et al*. (2005), a common strategy for modelling entire drinking water systems by means of fault trees was devised by Lindhe *et al*. (2008) and Norberg *et al.* (2008). The method provides information not only on the probability of failure but also on the mean failure rate and mean downtime of the system. By including consequences in the fault tree, in terms of number of people affected, the risk can be calculated as Customer Minutes Lost (CML).

To demonstrate and evaluate a practical application, the fault tree method was applied to the drinking water system in Göteborg, Sweden. The main event studied in the analysis was supply failure, which included failure to deliver water to the consumers (quantity failure) and failure to deliver water of acceptable quality (quality failure). The identification of hazards, construction of fault tree and analysis of data were conducted in close collaboration with the water utility personnel. To estimate probabilities of events, consequences and uncertainties of estimates, hard data and expert judgements were used. Monte Carlo simulations were used for the calculations and the estimated risk levels were compared to politically established performance targets regarding the supply of drinking water.

The primary aims of this paper were to apply a fault tree method for integrated and probabilistic risk analyses of drinking water systems and show how the results can be used. Although fault tree analysis is a commonly applied risk analysis tool, the integrated and probabilistic risk analysis for an entire drinking water system presented here is novel.

Method

The drinking water system in Göteborg was analysed using the fault tree method for integrated and probabilistic risk analyses of drinking water systems described by Lindhe *et al*. (2008) and Norberg *et al*. (2008). The mathematical foundation of the method is described by Norberg *et al*. (2008). Lindhe *et al*. (2008) present how the method can be applied to drinking water systems, including descriptions of a conceptual model, a generic fault tree structure, how to handle uncertainties of estimates and how to calculate CML. Here an overall presentation of the method is provided with reference to Lindhe *et al*. (2008) and Norberg *et al*. (2008) for further details. For information on the basics of fault trees and its application in risk analyses, see e.g. Rausand and Høyland (2004) and Bedford and Cook (2001).

Conceptual model

The main failure event studied in the analysis was supply failure, 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 unfit for human consumption according to existing water quality standards. Quantity failure may occur due to failure of components, e.g. pumps and pipes, or because the water utility detects an unacceptable water quality and decides to stop the delivery. The other type of failure, quality failure, may occur when an unacceptable water quality is not detected or when it is detected but no action is taken. The drinking water quality was considered unacceptable when unfit for human consumption. This criterion was based on the Swedish quality standards for drinking water, set by the by the National Food Administration (SLVFS 2001:30).

The drinking water system was modelled as a supply chain composed of three main sub-systems: raw water, treatment and distribution. Events in any of the sub-systems may cause supply failure, but they are also capable of compensating for failure. For example, in a system with two treatment plants failure of one plant to produce drinking water may be compensated for by reservoirs in the distribution system and increased production at the other treatment plant. However, the ability to compensate in this case is limited in time, due to limited reservoir volume. Another example is when raw water of unacceptable quality is used and the treatment plant still is able to produce drinking water that complies with the quality standards. To be able to determine each sub-system's contribution to the risk, failure in one part of the system was based on the assumption that the previous parts are functioning (i.e. no failure in previous parts).

Fault tree analysis

A fault tree is a logic tree diagram illustrating how an undesired event, i.e. *top event*, may occur due to occurrence of other events. The causes of each event are developed until a required level of detail is reached. Events that are subdivided into its causes are called *intermediate events* and at the end of each branch the *basic events* are found. The interaction between events is described using logic gates. The two most common logic gates are the OR- and AND-gate.

The OR-gate describes a series system where only one input events has to occur to cause system failure. The AND-gate describes a parallel system where all input events have to occur to cause the system to fail. To be able to consider the inherent ability of a system to compensate for failure Norberg *et al*. (2008) and Lindhe *et al*. (2008) identified and formulated two variants of the AND-gate. The first variant describes a situation where failure of one component may be compensated for by one or several other components during a limited time period. If no compensation is possible when the component fails the system fails directly, but if compensation is possible the system does not fail until all compensation is lost. The second variant of the AND-gate is similar to the first but with the important difference that when a compensating component has failed it may recover and start to compensate again.

By applying a Markovian approach (see e.g. Rausand and Høyland, 2004) Norberg *et al*. (2008) devised equations for calculating not only the probability of failure when using a fault tree but also the mean failure and mean downtime at each intermediate level of the fault tree. The equations used to calculate the output of each of the four logic gates are shown in Table 1, where P_F is the probability of failure, λ_i the mean failure rates, $1/\mu_i$ the mean downtimes and q_i the probabilities of failure on demand. The downtime corresponds to the time the system is in failure mode, i.e. does not function. Hence, variable u_i can be regarded as the repair rate. Failure on demand means that a component fails to compensate when needed, e.g. a reserve pump that cannot be started when the main pump brakes down. Failure during operation is the other type of failure and is represented by the failure rate, e.g. the reserve pump starts but after a time it as well brakes down.

Table 1 Equations used to calculate 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 mean failure rates, μ_i the mean repair rates ($1/\mu_i$ the mean downtimes) and q_i the probabilities of failure on demand.

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

Customer Minutes Lost (CML) and risk calculation

In addition to the variables calculated using the equations in Table 1, the risk (R) was estimated in terms of Customer Minutes Lost (CML). CML has previously been used in the drinking water sector, e.g. by

Blokker *et al*. (2005), who described the use of CML as a performance indicator in the Netherlands. This measure could be calculated by multiplying the mean failure rate (λ) by the mean downtime ($1/\mu$) and the number of people affected. However, to consider that the system may not fail when in failure mode, it can be shown that the expected value of CML should be calculated as $R = P_F \cdot C$, where P_F is the probability of failure and C the proportion of all consumers affected (Lindhe *et al*., 2008). By expressing C as a proportion of all consumers in Göteborg, the risk was estimated as the expected number of minutes per year the average consumer is affected.

Since it is not meaningful to estimate the number of people affected for the top event in the fault tree, it was estimated at a lower level for n different main types of events. The total risk, i.e. the total number of CML, was calculated by adding the risk posed by each main type of event together as

$$R = \sum_{i=1}^{n} P_{Fi} C_i \ .$$

To retain transparency CML was separately calculated for quality and quantity failures.

Uncertainties

To enable an uncertainty analysis all variables were modelled as probability density functions and the calculations were performed by means of Monte Carlo simulations (10,000 iterations). Variables λ and μ were modelled as exponential rates using Gamma distributions. The proportion of the consumers affected (C) as well as the probability of failure on demand (q) were modelled using Beta distributions. The main reason for using Gamma and Beta distributions was the fact that they are conjugate to the exponential and binomial models, respectively. Consequently, these distributions facilitate a Bayesian approach, in which hard data can be used for a mathematically formal updating of previous knowledge.

The probabilistic approach used in the analysis facilitates: (1) analysis of the uncertainties of each variable; (2) calculation of rank correlation coefficients, providing information on how much each variable in the fault tree affected the top event as well as the intermediate events; and (3) calculation of the probability of the risk to exceed specified criteria, i.e. acceptable levels of risk.

Case study Göteborg

System description

Göteborg is the second largest city in Sweden and approximately 500,000 people are supplied with drinking water by the local water utility, Göteborg Vatten. The system is solely based on surface water and the main raw water source is the Göta Älv river, a moderately polluted river (Westrell *et al.*, 2003). A schematic description of the raw water system in Göteborg is presented in Figure 1. In addition to the river, two interconnected lakes (reservoir lakes) are used for intermediate storage of raw water and to improve the water quality by natural sedimentation processes. Approximately half of the water taken from the river is transferred directly to treatment plant no. 1. The remaining part of the water is transferred via a rock tunnel to the reservoir lakes. From the reservoir lakes water is pumped to treatment plant no. 2, which cannot be supplied with water directly from the river. As the quality of the river water varies over time, the raw water intake is regularly closed for about 100 days per year (see e.g. Åström *et al.*, 2007). Decisions to close the raw water intake are based on online monitoring and reports from operating bodies upstream, e.g. industries and municipalities. Typical parameters monitored online are turbidity, conductivity, redox-potential and pH. In addition, microbial sampling is regularly carried out for analysis of faecal indicator bacteria. When the raw water intake at the riverside is closed, the reservoir lakes supply both treatment plants with water. By reversing the flow direction in the rock tunnel, water from the reservoir lakes can be transferred to treatment plant no. 1. To avoid water shortage in the reservoir lakes, water from an additional water source can be pumped to the reservoir lakes or directly to treatment plant no. 2.

The treatment plants have approximately the same production capacity and similar treatment processes, including chemical flocculation, sedimentation, filtration and disinfection. Online measurements and laboratory analyses are used to monitor the water quality at the treatment plants. The average drinking water demand is 165,000 m^3/d and varies normally between 120,000 – 210,000 m^3/d.

The maximum treatment capacity is 150,000 m^3/d for treatment plant no. 1 and 120,000 m^3/d for treatment plant no. 2. However, the treatment capacities are normally lower than the maximum due to maintenance work. Each treatment plant includes two major drinking water reservoirs used to ensure a continuous supply of drinking water.

The distribution network is approximately 1,700 km in length and to ensure sufficient pressure in network areas at high altitudes, the water head is raised through 66 booster stations. In addition 14 service reservoirs are used to meet peaks in the water demand. To monitor the water quality in the distribution system, measurements are made regularly at different locations, e.g. in pumping stations and private taps.

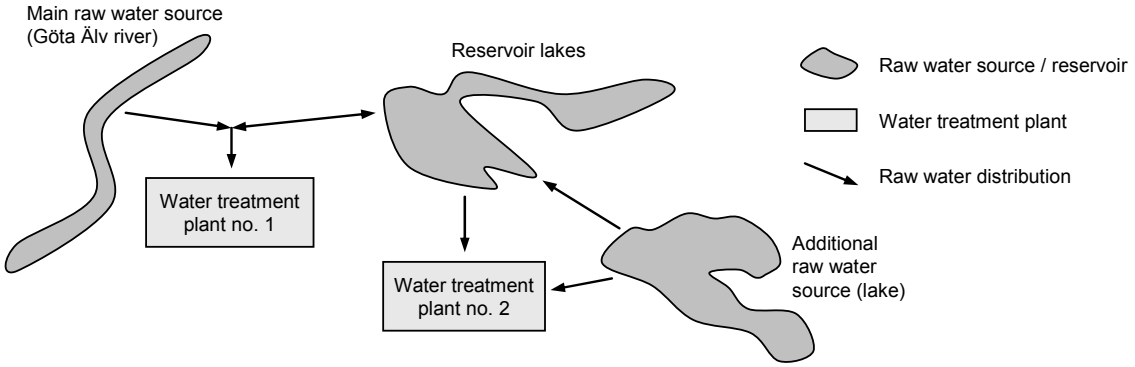

Figure 1 Schematic description of the raw water system in Göteborg.

Analysis procedure

The risk analysis was an iterative process with continuous updating of the fault tree structure and input data. The main steps in the analysis were: scope definition, system description, hazard identification, fault tree construction, evaluation of available data, expert judgements, risk estimation, uncertainty analysis and evaluation of results. A team of people with different knowledge about the system and the risk analysis method was set up to support the analysis work. The team included water utility personnel and researchers.

Hazard identification and fault tree structure

The identification of hazards was done simultaneously as the fault tree was constructed. It was an iterative process where events were identified and further developed until a required level of detail was obtained. The level of detail was considered sufficient when the fault tree properly corresponded to the system properties and when variables for the basic events could be estimated. All events did not have to be developed to the same level of detail to enable estimations of the required variables. Hence, the level of detail differed in the fault tree. In total, the fault tree was composed of 116 basic events, 100 intermediate events and 101 logic gates.

As illustrated in Figure 2 the drinking water system was divided into its three main sub-systems and supply failure may therefore occur due to events in the raw water, treatment or distribution system. Within each sub-system quantity or quality failures may arise and cause supply failure. Even though quantity and quality failure were included in the same fault tree, the results were presented separately for the two failure types in order to retain transparency. To consider that failure in one sub-system may be compensated for in other sub-systems, the first variant of the AND-gates was used, see Figure 2.

Raw water

As shown above the supply of raw water in Göteborg has a complex structure and several events may cause quality and quantity failures. However, there are also several possibilities to compensate for failure that need to be considered. Since the drinking water system in Göteborg includes two treatment plants, quantity and quality failures were assigned with respect to their possible impacts on these plants.

Quantity failure related to treatment plant no. 1 occurs if neither the river nor the reservoir lakes can be used to supply the treatment plant with raw water. However, for failure to occur, the drinking water reservoirs in the treatment plants and distribution system must also fail to compensate. Increased

production at the non-affected treatment plant may also enhance the ability to compensate for failure. It should be noted that the reservoirs and increased production can only prevent failure to occur for a limited period of time. Hence, the ability to compensate was modelled by means of the first variant of AND-gate. The events that may cause the water sources to become unavailable are related to failure of physical components (e.g. rock tunnels, pipes, pumps, siphons) or the actual quality of the raw water. Events affecting the raw water quality and guiding the water utility to close the raw water intake in the river are mainly related to precipitation, salt water intrusion from the sea and accidental releases of contaminants (Åström *et al.*, 2007). Quantity failure related to treatment plant no. 2 was modelled in a similar way as for treatment plant no. 1.

To model quality failures in the raw water system, measurable as well as non-measurable parameters causing an unacceptable water quality were considered. Supply of raw water of unacceptable quality to the treatment plants may be related either to non-detection of quality deviation or because no actions were possible, although the quality deviation was detected. However, unacceptable raw water quality may be compensated for in the treatment. To describe this process the second variant of AND-gate was used with *unacceptable raw water quality* and *treatment fails to compensate* as input events. For the latter event the probability that the unacceptable water quality can be compensated for at all, was represented by the probability of failure on demand (q). The mean failure rate (λ) and mean downtime ($1/\mu$) describe how often the treatment efficiency is affected and for how long. Information on the latter two variables was provided by the treatment part of the fault tree.

When quality failures related to the raw water were identified, the main focus was on microbiological hazards. In comparison to the other raw water quality parameters, faecal indicator bacteria has been found to regularly exceed the national quality standards for drinking water by far most (Göteborg Vatten, 2006).

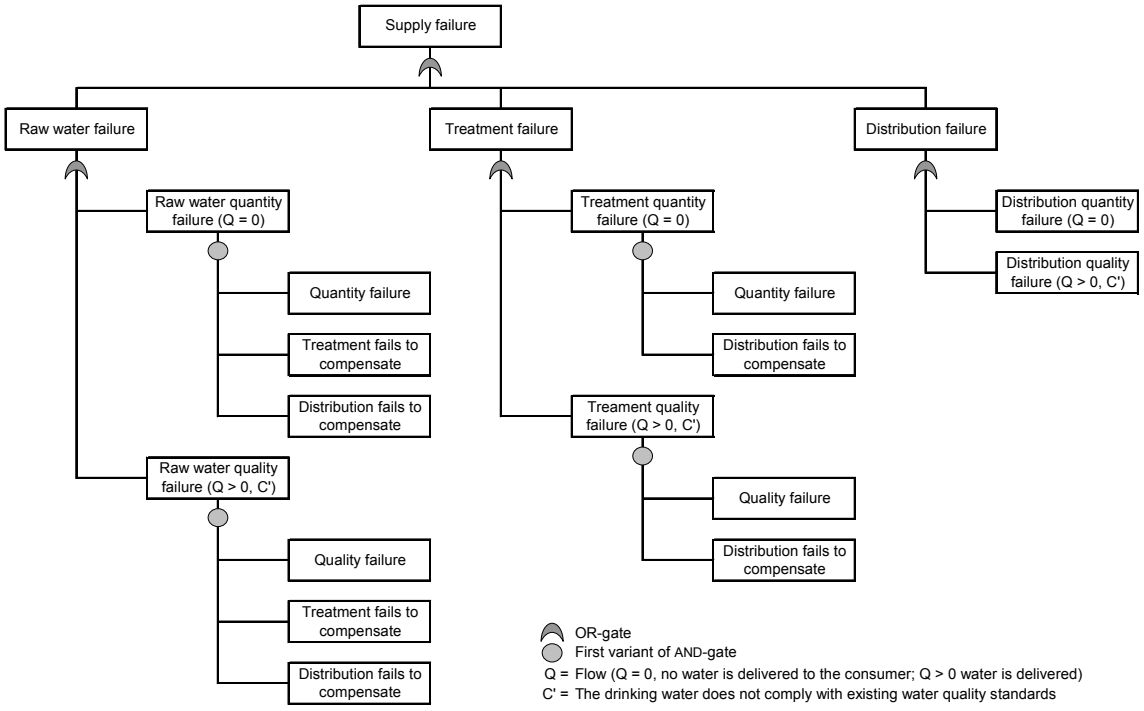

Figure 2 Schematic fault tree including the main events. All events were further developed in the analysis using also the traditional AND-gate and the second variant of it. The distribution system was assumed to not be able to compensate for quality failure in previous sub-systems but have been included here to illustrate the general thinking.

Treatment

As for the raw water, failures in the treatment were divided into those related to treatment plant no. 1 and 2, respectively. Quantity failure related to the treatment may occur due to physical damage of the treatment plant, making it impossible to transfer water, or due to failure of treatment processes resulting in unacceptable water quality. In the latter case the water utility has to detect the failure and decide to stop

the delivery. If the failure is not detected or the water utility decides not to stop the delivery, quality failure occurs. The focus when identifying quality failures in the treatment was on events that may jeopardise the ability to remove microbiological agents. This was reasonable since microbiological hazards in the raw water were considered as being the most important.

Quantity failures in the treatment may be compensated for by reservoirs in the treatment plants and distribution system. Quality failures, however, were not considered possible to compensate for.

Distribution

There are no subsequent sub-systems that may compensate for failure in the distribution, but the distribution itself may in some cases compensate for quantity failures. Quantity failures in the distribution may occur due to: water cannot be transferred from the treatment plants to the distribution system; breaks in water mains, distribution pipes or service connections; failure of pumps in specific delivery zones; or failure in private buildings. If water cannot be transferred from one or both treatment plants to the distribution system (i.e. failure of pumps or pipes), the reservoirs in the distribution system may compensate for a limited time period. Pump failure in a delivery zone may be compensated for if there is a reservoir in that specific zone. For both cases the first variant of AND-gate was used, because the reservoirs only contains a limited volume of water and cannot be filled up until the failed components have been repaired. For the water mains one pipe burst is not assumed reason enough to cause failure that affect the consumers. Instead, two pipe bursts have to occur at the same time or one pipe burst simultaneously with limited supply of water from the treatment plants, making it hard to retain prescribed pressure in the system.

Events that may cause quality failure in the distribution were divided into three types: quality deterioration due to microbial regrowth; intrusion of contaminants; and quality failure in private buildings. The first two types were divided into major and minor events, depending on the number of people affected. In this part of the fault tree no compensation was considered, since there are no barriers that may compensate for quality failures in the distribution.

Data analysis and expert judgements

The data needed for the fault tree analysis was based on hard data (e.g. measurements and statistics on events), expert judgements and combinations of these. Experts, mainly water utility personnel, were asked to estimate a probable highest and lowest value of the variable and this information was used as percentiles when estimating the probability distributions (Gamma and Beta). Also mean or median values were considered to make sure suitable probability distributions were obtained. When hard data was available, but not sufficient amount, expert judgements were used to supplement the data and enable an estimation of the variables. The use of hard data differed depending on the variable of interest. For some events the number of events that have occurred and their duration were available, and could be used to estimate the failure rate and downtime. When the ability to compensate for failure was studied, system properties could be used to calculate a probable highest and lowest value. Previous studies by the water utility and others were also used for the estimations.

Tolerability criteria

The City of Göteborg has prepared an action plan including performance targets regarding the supply of drinking water (Göteborg Vatten, 2006). These targets are politically established and can be considered as tolerable levels of risk. Thus, they were compared to the level of risk calculated by means of the fault tree. The targets evaluated within this study are related to the reliability of the supply, i.e. water quantity (Table 2). The comparison of the targets to the estimated level of risk is presented in the results section.

Table 2 Politically established performance targets used to compare to the estimated level of risk.

No.	*Performance target*
1.	Duration of interruption in delivery to the average consumer shall, irrespective of the reason, totally be less than 10 days in 100 years.
2.	Duration of interruption in delivery to the average consumer shall totally be less than six minutes per year, provided delivery from both water treatment plants.

Results

The fault tree analysis generated information on the probability of failure (P_F), mean failure rate (λ) and mean downtime ($1/\mu$) at all levels in the fault tree. In addition, also the expected value of CML (Customer Minutes Lost) was estimated for the average consumer. All results were presented separately for quantity and quality failures in order to retain transparency. In Table 3 the results are presented for the entire system (supply failure) and the three main sub-systems.

Table 3 Summary of the estimated variables of quantity and quality failure for the entire system (supply failure) and the three sub-systems. For all variables the 5-, 50- (median) and 95-percentiles are presented. The expected value of CML, i.e. risk, is calculated for the average consumer.

	Quantity failure			Quality failure		
	P_{05}	P_{50}	P_{95}	P_{05}	P_{50}	P_{95}
Supply failure						
CML [min·year^{-1}]	72	391	1 684	103	564	3 399
Probability of failure (P_F)	0.08	0.14	0.32	0.03	0.06	0.25
Mean failure rate (λ) [year^{-1}]	306	411	543	7	10	13
Mean downtime ($1/\mu$) [h]	2	3	10	27	56	281
Raw water failure						
CML [min·year^{-1}]	15	274	1 560	33	482	3 322
Probability of failure (P_F)	0.004	0.008	0.017	0.006	0.013	0.046
Mean failure rate (λ) [year^{-1}]	1.0	1,8	3.6	0.5	1.1	3.2
Mean downtime ($1/\mu$) [h]	32	37	47	70	112	187
Treatment failure						
CML [min·year^{-1}]	2	43	264	2	31	140
Probability of failure (P_F)	0.0004	0.0012	0.0031	0.0004	0.0008	0.0015
Mean failure rate (λ) [year^{-1}]	0.6	1.3	2.7	0.7	1.2	2.0
Mean downtime ($1/\mu$) [h]	6	8	12	4	6	9
Distribution failure						
CML [min·year^{-1}]	4	16	93	8	30	98
Probability of failure (P_F)	0.07	0.13	0.31	0.02	0.04	0.24
Mean failure rate (λ) [year^{-1}]	303	407	539	5	7	10
Mean downtime ($1/\mu$) [h]	2	3	9	20	52	346

Since the probability of failure represents the proportion of time the system is in failure mode, it can be used to calculate, for example, the expected number of days per year at least one consumer is exposed to quantity or quality failure. The mean failure rate can be used to calculate the mean time to failure ($1/\lambda$).

As a probabilistic approach was used, the probability of exceeding the performance targets presented in Table 2 could be calculated. The first target was translated to an acceptable level of 144 CML per year for the average consumer. This level was compared to the quantity-related CML for supply failure in Table 3. The median value (391 CML) clearly exceeds the acceptable level and the calculations resulted in a probability of exceeding the target of 0.84, see Figure 3. The second target, expressed as 6 CML per year for the average consumer, was compared to an estimated risk level of 7 CML (median value). The 5- and 95-percentiles were 2 and 29 CML respectively, and the probability of exceeding the target was 0.58 (Figure 3). The latter risk level is a combination of specific events and is not included in Table 3.

To analyse the uncertainties, rank correlation coefficients were calculated to show which events affected the results the most. For example, when the quality-related CML for the entire system was analysed, it

was concluded that the number of people affected by quality failure in the raw water system was most important. Furthermore, it was concluded that the failure rate and duration of some of the events causing unacceptable raw water quality also had a high impact on the results.

It should be noted that the results presented here are preliminary and based on the assumptions made when constructing the fault tree and estimating the variables. These assumptions need to be further analysed by involved experts before the results are used as a decision support.

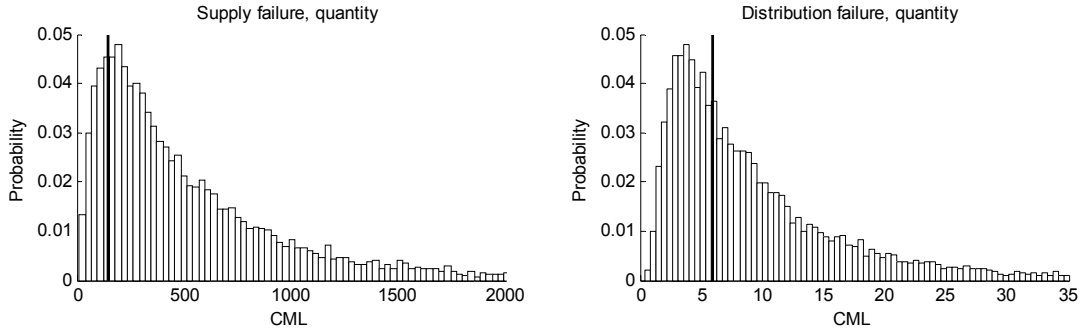

Figure 3 Uncertainty distributions of risk levels, expressed as the expected value of CML per year, compared to performance target no. 1 (left) and 2 (right). The performance targets (144 and 6 CML per year) are indicated by solid vertical lines. The probabilities of exceeding the targets are 0.84 for target no.1 and 0.58 for target no. 2.

Discussion

The fault tree analysis of the Göteborg systems provided information on risk levels as well as on the dynamic behaviour of the system. When comparing the calculated quantity and quality-related risk levels (expected value of CML) for the entire system with the results for the three sub-systems, it was concluded that the raw water system contributes most, while for the treatment and distribution a considerable lower contributions were observed.

When comparing the treatment and distribution, a difference in the character of the failures was observed. For example, quantity failures in the distribution occur frequently, have a short mean downtime and affect a small number of people. The same type of failures occurs much more seldom in the treatment, have a short mean downtime and have the potential to affect a larger proportion of the consumers. Hence, by studying not only the CML but also the failure rate and downtime, information is provided on the dynamic behaviour of the system. Two sub-systems may cause same risk but have different dynamic behaviours. Two sub-systems may also have the same probability of failure but different failure rates and downtimes.

As concluded above the large number of CML for the entire system (median 391) mainly originates from the raw water (median 274). In contrast, the high probability of failure and failure rate, as well as the short downtime, mainly originate from the distribution. This shows that the information on the top event in the fault tree should be studied together with information on lower levels, in order to obtain the true picture of the system.

One reason failures in the raw water system have a large affect on the total number of CML is because it is the first part of the supply chain, and consequently may affect a large proportion of the consumers. This is also valid for the treatment, but in this specific system failures in the treatment have a shorter mean downtime compared to those in the raw water system. In contrast to the other two sub-systems, failures in the distribution most often affect a small number of people.

The probabilistic approach used in the analysis made it possible to not only conclude if the mean or median value exceeds a specific target value or not, but also to what probability a target is exceeded. The comparison of the results to the politically established performance targets showed that both targets are exceeded with a probability of 0.84 and 0.58 respectively. This type of information raises an important question about the performance targets. The decision-maker does not only have to state an acceptable level of risk but also think about how certain he or she wants to be that it is not exceeded.

By carrying out uncertainty analyses at all levels in the fault tree, it was possible to identify which parts and events that contributed most to the uncertainties in the results. This is important information in order to assess where further information is most valuable to reduce the uncertainties in the results.

The CML related to quality failure does not say anything about the actual health risk. The applied method does not include any consideration to health effects from drinking water unfit for human consumption. However, the analysis provides quantitative results that are directly related to the health-based water quality standards. The resulting minutes a consumer is exposed to drinking of unacceptable quality can be used in a Quantitative Microbial Risk Assessments (QMRA) to calculate the actual health risk. Combining QMRA with the detailed system descriptions in the fault tree enables a focused search for best options to reduce the health risk.

It is important that a fault tree is not constructed to fit available data. Instead, the most important thing is that the fault tree gives a realistic representation of the actual system. Gathering of data and converting data to the right format is the next step of the analysis. It is also important to consider previous events as well as events that may occur in the future. Hence, it is important to encourage participating experts to explore possible future events.

When a fault tree has been constructed according to the method used here it is not only possible to estimate the current risk level. One of the advantages of the method is that the effects of possible risk-reduction options can be modelled and evaluated by means of the fault tree. By changing the input data or including new events, e.g. new possibilities to compensate for failures, the effect of different measures can be compared. Hence, it can be used as a decision support tool.

Conclusions

Based on the risk analysis, it was concluded that the probabilistic fault tree method can be used to:

- model entire drinking water systems, i.e. perform integrated analyses;
- estimate risk levels in terms of quantity and quality-related CML;
- understand the dynamic behaviour of the system;
- estimate the probability of exceeding acceptable levels of risk or other criteria;
- identify which events that contribute most to the uncertainties in the results, and consequently assess where further information is most valuable to reduce the uncertainties in the results;
- update the analysis when new information becomes available;
- model risk-reduction options and evaluate their efficiency; and
- facilitate discussions on risks to the system and how the system function.

An important further application of the method is to model risk reductions resulting from implementation of water safety measures in the system. This is further discussed by Rosén *et al*. (2008).

Acknowledgements

This study has been carried out within the TECHNEAU project (Technology Enabled Universal Access to Safe Water), funded by the European Commission (contract number 018320), and with support from the Swedish Water & Wastewater Association and the City of Göteborg. The authors would like to thank the City of Göteborg for a valuable and fruitful collaboration.

References

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

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

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

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

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

Lindhe, A., L. Rosén, T. Norberg and O. Bergstedt (2008). Fault tree analysis for integrated and probabilistic risk analysis of drinking water systems, Submitted to *Water Research*.

Norberg, T., L. Rosén and A. Lindhe (2008). Added value in fault tree analyses (*In press*), European Safety and Reliability Association 2008 and 17th Society for Risk Analysis Europe Conference, Valencia, 22-25 September.

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

Rosén, L., O. Bergstedt, A. Lindhe, T.J.R. Pettersson, A. Johansson and T. Norberg (2008). Comparing Raw Water Options to Reach Water Safety Targets Using an Integrated Fault Tree Model, Paper presented at the International Water Association Conference, Water Safety Plans: Global Experiences and Future Trends, Lisbon, 12-14 May.

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

Westrell, T., O. Bergstedt, T.A. Stenström and N.J. Ashbolt (2003). A theoretical approach to assess microbial risk due to failures in drinking water systems, *International Journal of Environmental Health Research*, *13* (2), 181-197.

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

Åström, J., T.J.R. Pettersson and T.A. Stenström (2007). Identification and management of microbial contaminations in a surface drinking water source, *Journal of Water and Health*, *5* (1), 67-80.