Approximate dynamic fault tree calculations for modelling water supply risks

Approximate dynamic fault tree calculations for modelling water supply risks

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

[a] Department of Civil and Environmental Engineering, Chalmers University of Technology, SE-412 96 Gothenburg, SWEDEN. E-mail: andreas.lindhe@chalmers.se; Tel: +46 31 772 2060; Fax: +46 31 772 2107

[b] Department of Mathematical Sciences, University of Gothenburg and Chalmers University of Technology, SE-412 96 Gothenburg, SWEDEN. E-mail: tommy.norberg@chalmers.se

[c] Department of Civil and Environmental Engineering, Chalmers University of Technology, SE-412 96 Gothenburg, SWEDEN. E-mail: lars.rosen@chalmers.se

* *Corresponding author*

ABSTRACT

Traditional fault tree analysis is not always sufficient when analysing complex systems. To overcome the limitations dynamic fault tree (DFT) analysis is suggested in the literature as well as different approaches for how to solve DFTs. For added value in fault tree analysis, approximate DFT calculations based on a Markovian approach are presented and evaluated here. The approximate DFT calculations are performed using standard Monte Carlo simulations and do not require simulations of the full Markov models, which simplifies model building and in particular calculations. It is shown how to extend the calculations of the traditional OR- and AND-gates, so that information is available on the failure probability, the failure rate and the mean downtime at all levels in the fault tree. Two additional logic gates are presented that make it possible to model a system's ability to compensate for failures. This work was initiated to enable correct analyses of water supply risks. Drinking water systems are typically complex with an inherent ability to compensate for failures that is not easily modelled using traditional logic gates. The approximate DFT calculations are compared to results from simulations of the corresponding Markov models for three water supply examples. For the traditional OR- and AND-gates, and one gate modelling compensation, the errors in the results are small. For the other gate modelling compensation, the error increases with the number of compensating components. The errors are, however, in most cases acceptable with respect to uncertainties in input data. The approximate DFT calculations improve the capabilities of fault tree analysis of drinking water systems since they provide additional and important information and are simple and practically applicable.

Keywords: dynamic fault tree (DFT), drinking water, risk assessment, Markov model, Monte Carlo simulation, uncertainty.

1. INTRODUCTION

The need of proper risk assessments of drinking water systems is emphasised within the drinking water sector. Furthermore, the World Health Organization [1] points out the importance of considering the entire supply system, from source to tap. Methods for assessing risks to entire drinking water systems are, however, limited and the complexity of the systems provides challenges. Lindhe *et al.* [2, 3] showed how a method based on dynamic fault tree (DFT) analysis can be used to model entire drinking water systems in a correct way and provide results that support decisions on risk reduction.

Fault tree analysis is performed to analyse system reliability and it is commonly used in risk assessments. A major purpose of a fault tree analysis is to assist in the calculation of the failure probability for systems including different subsystems and components. It has, however, been concluded by several authors that traditional static fault trees are not able to correctly model the dynamic behaviour of fault-tolerant systems including, for example, spare components and dynamic redundancy [e.g. 4, 5]. To overcome this limitation, DFTs have been developed in which logic gates designed to model the dynamic behaviour are introduced [e.g. 4, 6, 7]. Compared to traditional static fault trees the DFTs are more computationally demanding and different techniques for solving them have therefore been developed [e.g. 8, 9, 10]. It should, however, be noted that also techniques used to calculate traditional fault trees are associated with limitations [e.g. 11, 12].

Traditionally, DTFs have been solved by using Markov models. When the number of events in a fault tree increases, the number of states and transition rates in the corresponding Markov model increase rapidly and the calculations can become time consuming. To simplify the calculations a modularized approach can be used. This means that the fault tree model is divided into smaller parts and parts including dynamic gates are solved by transforming them into Markov models and static parts are solved using traditional fault tree calculations [5, 13]. Other approaches that have been developed to further simplify DFT calculations and/or provide additional results are numerical integration techniques [8], Bayesian network modelling [14-16] and a Monte Carlo simulation-based approach [6]. The approach presented and evaluated in this paper is based on a Markovian approach but approximate DFT calculations are used in combination with Monte Carlo simulations. This approach implies that generic equations are devised for the logic gates and the calculations are preformed using Monte Carlo simulations.

A dynamic approach to fault tree modelling, where the temporal aspects of system events are included in the calculations, provide additional and needed information when analysing water supply risks. Norberg *et al.* [17] and Lindhe *et al.* [2] described how to extend the calculations of the traditional logic gates using a Markovian approach where each basic event is described using a failure rate and a mean downtime. The method includes two variants of the common type AND-gate that make it possible to consider the ability of drinking water systems to compensate for failures. This dynamic approach provides a wider decision support than traditional fault trees. It provides an improved capability to take into account compensation and makes it possible to calculate not only the failure probabilities, but also the failure rate and the mean downtime at all levels in the fault tree. Lindhe *et al.* [2] further described how to combine these results with information on consequences (number of people affected) to calculate risk levels. Due to a substantial complexity in performing exact calculations of failure probabilities, failure rates and downtimes, an approximate approach using Monte Carlo simulation that does not require complete simulations of the DFT was suggested by Norberg *et al.* [17]. Lindhe *et al.* [2] describe how to apply the approach when modelling water supply risks. The logic gates needed to model water supply risks were converted into Markov models and generic equations were devised. This facilitates simple model building and Monte Carlo

simulations make it possible to consider uncertainties in the calculations. Fault tree models of drinking water systems easily become extensive. If DFT calculations of such models can be performed using standard software and if expert knowledge in Markov processes is not required, then such a method becomes very useful.

The overall aim of this paper was to provide a quality control of the DFT method presented by Lindhe *et al.* [2]. Specific objectives were to present the basis for the approximate DFT calculations and evaluate the capability of the calculations in predicting the true probability of failure, failure rate and mean downtime of a drinking water system. The evaluation was made by comparing the approximate calculations to results from simulations of the complete Markov model for three fault tree examples from a public drinking water system.

The remainder of the paper is divided as follows. In Section 2 we recall the concept of failure probability. In Section 3 it is shown how to extend the calculations for two basic types of logic gates in a fault tree. The argumentation is extended to two auxiliary gates that have been found useful when modelling water supply risks. In Sections 4 and 5, three fault tree examples from a municipal drinking water system are studied. Finally, in Section 6 the results are discussed and the main conclusions are presented.

2. PROBABILITY OF FAILURE IN DYNAMIC SYSTEMS

Input to fault tree calculations are probabilities P for basic events F_i , where F_i denotes failure of subsystem or component i. We here assume, as is often done, that the basic events are independent. If for any i, F_i represents the event that subsystem i is down at a particular point in time, then $P(F)$ is the probability that the system is down at that particular point in time. Note that $P(F)$ also may be referred to as the unavailability. In the stationary case, $P(F)$ as well as all $P(F_i)$ does not depend on time. Assuming ergodicity, $P(F)$ can be thought of as the ratio between the Mean Downtime (MDT) and the Mean Time Between Failures (MTBF),

$$P(F) = \frac{\text{MDT}}{\text{MTBF}} \qquad (1)$$

Note that MTBF = MTTF + MDT, where MTTF denotes Mean Time To Failure. Thus, the probability $P(F)$ is not always sufficiently informative, since two systems with very different dynamic behaviour can have the same $P(F)$. In this paper it is showed how the fault tree calculations can be extended so that also estimates of MTTF and MDT are calculated at the top level as well as at each intermediate level. This of course requires knowledge of MTTFs and MDTs for all basic events. Estimates are then recursively calculated at each level of the fault tree. These estimates are calculated under the assumption that the input processes are independent and Markovian with only two states, up and down. This means that the failure rate is assumed to be constant and equal to 1/MTTF. A similar remark applies to the rate at which the process recovers from failure. At intermediate levels and at the top, the rates are typically not constant. The calculations, however, assume constant input rates and yield constant output rates. Thus, there are errors that when propagated to the top level may be quite substantial. However, in applications with large parameter uncertainties the main errors in the final result are, according to the author's experiences, often mainly due to the errors in the assumed parameter values for the basic events. In such cases, the enlargement of the traditional fault tree calculations presented and evaluated in this paper provide a considerable and valuable insight into the dynamics of the studied system.

3. DYNAMIC FAULT TREES

The reader is referred to, for example, Rausand and Høyland [18] for a basic introduction to fault tree analysis from a risk perspective in reliability analysis. Events in a fault tree are combined using logic gates and the two most common ones are the OR- and the AND-gate. Starting from the top event the gates are used to describe the causes of each event and they are repeatedly applied until a suitable level of detail is obtained. We will refer to a gate with top, or output, event F and basic events F_i as a subsystem consisting of components, all of which are either up or down at a particular point in time. In this section the mathematical foundation is presented for the common type OR- and AND-gates, and two variants of the AND-gate introduced in this paper. Thus, it is shown how the equations necessary for performing approximate DFT calculations have been devised. State diagrams are presented to graphically illustrate what Markov process each logic gate corresponds to. The two variants of the common type AND-gate presented here are similar to what in DFT applications often are referred to as SPARE-gates [e.g. 10].

A subsystem modelled using an OR-gate is up (functioning) as long as every component is up. Similarly, a subsystem modelled using an AND-gate is up as long as at least one of its components is up. In structural reliability, the OR-gate corresponds to a serial structure, while the AND-gate corresponds to a parallel structure. If the basic events are independent (which will be assumed throughout), then, for the OR-gate,

$$P(F) = 1 - \prod_i \left(1 - P(F_i)\right) \tag{2}$$

while for the AND-gate,

$$P(F) = \prod_i P(F_i) \tag{3}$$

In drinking water applications an OR-gate may be used to model a situation where insufficient raw water quality can be caused by either runoff during heavy precipitation or accidental contamination. An AND-gate may be used to model that the supply of water from a pump station including two pumps, only is interrupted if both pumps fail, i.e. are in down state at the same time.

3.1 The OR-gate

Replace each basic event of the gate by a Markov process having two states, up (1) and down (0). Let λ_i and $1/\mu_i$ denote the failure rates and the mean downtimes, respectively, for these basic Markov processes. Then, Equation (1) implies

$$P(F_i) = \frac{\lambda_i}{\lambda_i + \mu_i} \tag{4}$$

Note that μ_i corresponds to repair rates. Rausand and Høyland [18] provide an introduction to continuous time Markov chains in reliability. In Figure 1 the state diagram of the combined Markov process is shown for an OR-gate including two components. Suppose the system is up, then the time to the next failure is exponential with rate

$$\lambda = \sum_i \lambda_i \tag{5}$$

The system mean downtime, $1/\mu$, now follows from (2), (4) and the general fact

$$P(F)=\frac{\lambda}{\lambda+\mu} \quad \Leftrightarrow \quad \frac{\mu}{\lambda}=\frac{1-P(F)}{P(F)} \tag{6}$$

and is given by

$$\mu=\left(\sum_i \lambda_i\right)\frac{\prod_i \mu_i}{\prod_i(\lambda_i+\mu_i)-\prod_i \mu_i} \tag{7}$$

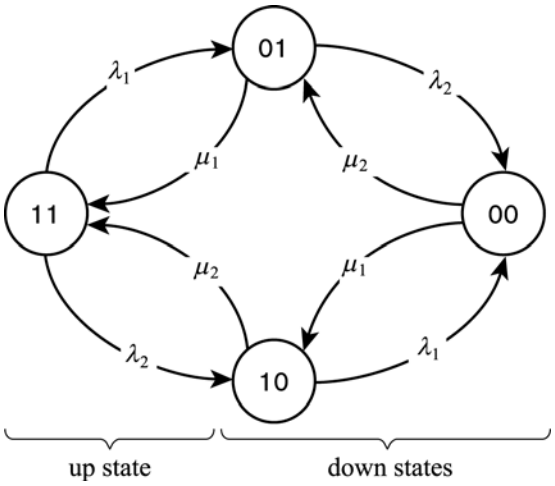

Figure 1 *State diagram of a Markov process representing an OR-gate including two components. The process is down, i.e. in failed state, if at least one component is down.*

3.2 The AND-gate

For the AND-gate, we see from (3) and (4) that

$$P(F)=\prod_i \frac{\lambda_i}{\lambda_i+\mu_i} \tag{8}$$

The state diagram of the AND-gate is shown in Figure 2. The mean downtime $1/\mu$ follows from

$$\mu=\sum_i \mu_i \tag{9}$$

and the failure rate now follows from (6) and is

$$\lambda=\left(\sum_i \mu_i\right)\frac{\prod_i \lambda_i}{\prod_i(\lambda_i+\mu_i)-\prod_i \mu_i} \tag{10}$$

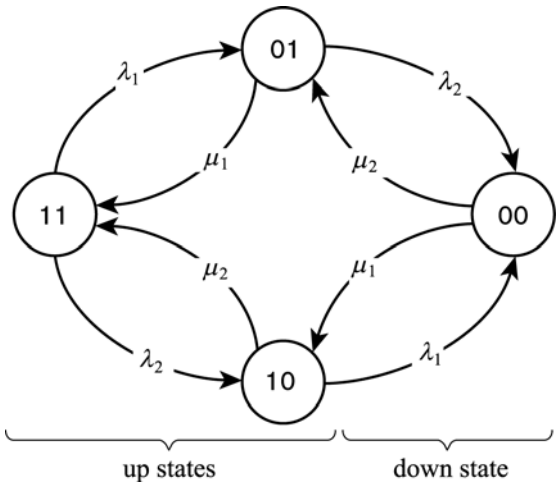

Figure 2 *State diagram of a Markov process representing an AND-gate including two components. The process is down when all components are down.*

3.3 The first variant of the AND-gate

The state diagram of the first AND-gate variant is shown in Figure 3. The gate can, for example, model a drinking water system where interruptions in the supply from the treatment plant to the consumers may be compensated for by two service reservoirs in the distribution system. The service reservoirs can only compensate for a limited time since only a certain amount of water can be stored. Furthermore, sometimes there is no water in the service reservoirs due to, for example, a high water demand or maintenance work and they can thus fail on demand. The system is up (water is supplied) as long as the main subsystem is up (state 1) or down while at the same time the first or second compensating/backup component (service reservoir) is up (state 01 and 001); it is down when in state 0; λ_1 and $1/\mu_1$ denote the failure rate and mean down time of the system, q_2 and q_3 are the probabilities of failure on demand for the compensating components and their uptimes are exponential(λ_2) and exponential(λ_3), respectively.

When $q_3 = 1$ the state diagram in Figure 3 is reduced to only include one compensating component and state 001 is then excluded. In the derivation below, we make the simplifying assumption that $q_3 = 1$. The balance equations are

$$\begin{aligned} p_1\lambda_1 &= p_{01}\mu_1 + p_0\mu_1 \\ p_{01}\left(\mu_1 + \lambda_2\right) &= p_1\lambda_1\left(1-q_2\right) \\ p_0\mu_1 &= p_1\lambda_1 q_2 + p_{01}\lambda_2 \end{aligned}$$

where p_1 and p_{01} are the stationary probabilities for the system to be in either of its up states, and p_0 is the probability that the system is in its only down state. Solving for p_0 is straightforward. Hence,

$$P\left(F\right) = \frac{\lambda_1}{\lambda_1 + \mu_1}\frac{\lambda_2 + q_2\mu_1}{\lambda_2 + \mu_1} \tag{11}$$

More generally, it can be proved that

$$P\left(F\right) = \frac{\lambda_1}{\lambda_1 + \mu_1}\prod_{i\neq 1}\frac{\lambda_i + q_i\mu_1}{\lambda_i + \mu_1} \tag{12}$$

if the main subsystem has several independent backups. The rate at which the system recovers from its down state 0 is μ_1. Hence

$$\mu = \mu_1 \tag{13}$$

Now λ can be calculated by inserting (12) and (13) in (6).

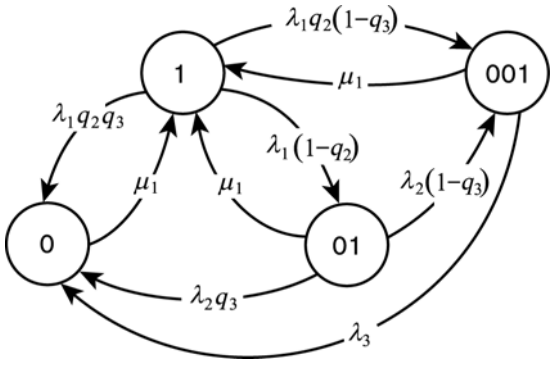

Figure 3 State diagram of a Markov process representing the first AND-gate variant including one main component and two compensating/backup components. In states 01 and 001 failure is compensated for by the two backup components. The process is down while in state 0.

3.4 The second variant of the AND-gate

The second variant of the AND-gate can, for example, model the situation where insufficient raw water quality is compensated for by extra capacity in the drinking water treatment plant. The extra capacity is not always available and the treatment plant may thus fail on demand. The treatment plant may also fail during the time it is compensating and recover and start to compensate again. The state diagram is shown in Figure 4. The system down states are 0 and 00; λ_1 and $1/\mu_1$ denotes the failure rate and mean downtime for the initiating failure of insufficient raw water quality, q_2 is the probability of failure on demand for the treatment plant whereas its up- and downtimes are independent and exponential(λ_2) and exponential (μ_2), respectively.

A straightforward analysis of the balance equations yields

$$p_0 = \frac{\lambda_1 q_2}{\lambda_1 + \mu_1}$$

$$p_{00} = \frac{\lambda_1(1-q_2)}{\lambda_1 + \mu_1}\frac{\lambda_2}{\lambda_2 + \mu_1 + \mu_2}$$

Hence,

$$P(F) = \frac{\lambda_1}{\lambda_1 + \mu_1}\frac{\lambda_2 + q_2(\mu_1 + \mu_2)}{\lambda_2 + \mu_1 + \mu_2} \tag{14}$$

Note next that

$$\mu = \frac{p_1\lambda_1 q_2 + p_{01}\lambda_2}{P(F)} \tag{15}$$

where p_1 and p_{01} are the stationary probabilities for being in the up states, given by

$$p_1 = \frac{\mu_1}{\lambda_1 + \mu_1}$$

$$p_{01} = \frac{\lambda_1(1-q_2)}{\lambda_1 + \mu_1} \frac{\mu_1 + \mu_2}{\lambda_2 + \mu_1 + \mu_2}$$

For interpretation of (15), note that the numerator equals the frequency ω_F of system failures and combine with the general fact $P(F)\mu = \omega_F$. For further details see e.g. Rausand and Høyland [18]. Finally, λ follows from (14), (15) and the general formula (6). Note that there is an error in the description of the second AND-gate variant by Norberg *et al.* [17].

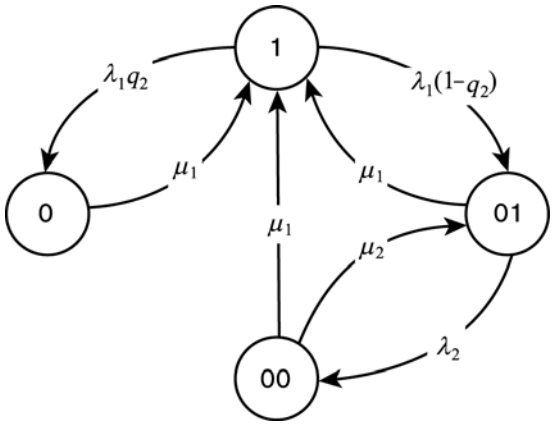

Figure 4 State diagram of a Markov processes representing the second AND-gate variant including one compensating component. The initiating failure is compensated for in state 01 and the process is down while in state 0 or 00.

3.5 Remarks on the dynamic fault tree calculations

The calculations in a fault tree are performed from bottom to top. The data (i.e. results) at one level is used as input to the calculations at the level immediately above. Our approach presumes that the input data to one level consist of Markovian failure (up) and repair (down) rates. The calculated rates, however, are not necessarily Markovian. Still, the calculations at the next level presume that they are. Clearly, this introduces an error making it wrong to assume that rates calculated at the top or at any intermediate level are Markovian.

In other words, denote by λ the calculated rate of failure at the, say, top level. Let T be a typical uptime and denote by $\rho(t)$ its failure rate. Then T is not necessarily exponential(λ) and it needs not to be true that $\rho(t) = \lambda$. However, in many instances λ is a reasonably good approximation of $\rho(t)$. Here we assume $\rho(t) = \lambda$ and we analyse the results to see how this affects the results.

A similar remark applies to the mean downtime $1/\mu$. Notice, however, that the probability of failure $P(F)$ is calculated exactly at each level and that

$$P(F) = \frac{\lambda}{\lambda + \mu} \qquad (16)$$

by construction always is true. This remark applies of course only to fault trees that only include the traditional OR- and AND-gates.

4. EXAMPLES

The need of approximate DFT calculations was identified when risks to a public drinking water system were analysed. Subsystems and components in a drinking water system are interconnected and failure in one part of the system may be compensated for by other parts of the system. Furthermore, it is often easier to characterise failure events using up- and downtimes compared to direct estimations of failure probabilities.

Lindhe *et al.* [2] used the approximate DFT calculations to analyse the entire drinking water system in Gothenburg, Sweden [see also 3, 19]. A schematic description of the raw water supply and the two treatment plants in Gothenburg is presented in Figure 5. In addition, the system includes an extensive distribution system used to supply the approximately 500,000 consumers with water. To model the system a fault tree was constructed by means of the four logic gates presented in this paper. In total, the fault tree included approximately 120 basic events and 100 logic gates. Three parts of the Gothenburg fault tree model are presented here and used to analyse and evaluate the approximate DFT calculations. The overall approach and the generic structure of the entire fault tree model are also presented shortly.

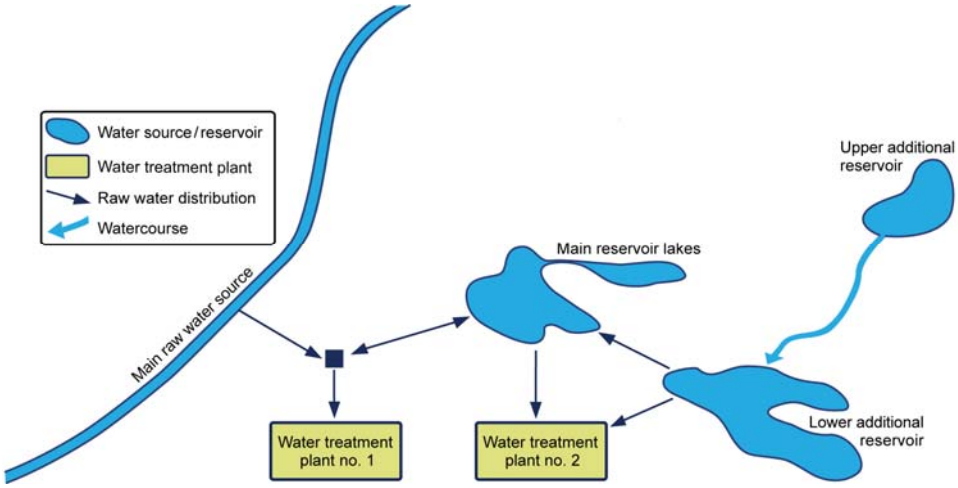

Figure 5 *Schematic description of the raw water supply and the two treatment plants included in the drinking water system in Gothenburg.*

The fault tree of the Gothenburg system was constructed to model situations where no water is delivered to the consumer and also situations where water is delivered but does not meet water quality standards, i.e. two top events were used. The fault tree was divided into three main parts representing the raw water system, the treatment system and the distribution system. The reason for this division was to be able to show how much each part of the system contributes to the total risk and thus make it possible to identify where in the system measures for reducing the risk are needed most. The variants of the common type AND-gate were used to properly model the ability to compensate for failure in different parts of the system. In addition to calculating the probability of failure and the dynamic behaviour of the system, also the risk was calculated. Two different risk levels were determined and expressed in terms of Customer Minutes Lost: (i) the number of minutes per year the average consumer is not supplied with water; and (ii) the number of minutes per year the average consumer is supplied with water not complying with water quality standards. The risk levels were calculated based on the probability of failure and the proportion of consumers affected [2]. Historical data as well as expert judgements were used to estimate input parameters and uncertainties of the estimates.

We refer to Lindhe *et al.* [2] for further description of analysing drinking water systems using DFTs. Lindhe *et al.* [3] and Rosén *et al.* [19] present how DFTs can be used to evaluate risk-reduction measures.

4.1 Example 1

The three fault tree examples used in this paper are presented in Figure 6. The first example illustrates how the main water sources in the Gothenburg system can become unavailable, i.e. water cannot be supplied to the treatment plant connected to this water source. This may in the end cause an interruption in the supply to the consumers. The fault tree includes only traditional OR- and AND-gates. The water source becomes unavailable if the raw water quality is considered insufficient (events 1.1-1.5) or technical components fail (events 1.6-1.13). Insufficient quality can be caused by different events related to, for example, precipitation and accidental release of contaminants. As can be seen in the fault tree there are two systems for transferring water to the pump station (gate D), which both have to fail to cause an interruption in the transfer of water.

4.2 Example 2

The second fault tree example (Figure 6) describes the situation where raw water of insufficient quality is supplied to one of the system's treatment plants. The insufficient quality in this example is caused by measureable parameters, i.e. parameters that are routinely analysed by the water utility. Two initiating events were identified: (i) the quality deviation is detected but no action is possible or enough to prevent failure (event 2.1); and (ii) the quality deviation is not detected (event 2.3). For both failure types it is possible that the quality deviation can be managed by the normal operation of the treatment plant (events 2.2 and 2.4) and thus a drinking water fulfilling existing quality standards can be produced. The ability of the treatment plan to compensate for insufficient raw water quality was modelled using the second variant of the AND-gate. Hence, it was considered that when the treatment plant is compensating for failure, events may occur that prevent this ability. However, the treatment system may recover and start to compensate again before the initiating failures (events 2.1 and 2.3) are solved. Furthermore, it was considered that the extra capacity to compensate for failures may be unavailable when needed. Input data to the two compensating events were defined based on information about variations in the treatment plant operation.

4.3 Example 3

The third fault tree example (Figure 6) models quantity failures that originate from one of the two water treatment plants (WTP 1). Failure at WTP 1 can occur due to failure related to the raw water inlet (event 3.1), failure of treatment processes (events 3.2-3.4) or extraordinary events (event 3.7) such as fire. Failure in any of the three treatment processes was assumed to cause a quality deviation which, if it is detected and the water utility decides to stop the delivery (events 3.5 and 3.6), causes a supply shortage. For the two latter events only the probability of failure was considered, since they are not dynamic events.

Although failure occurs at WTP 1 the consumers are not affected as long as other parts of the system are able to compensate for the failure (events 3.8-3.10). To model the possibility of compensation the first variant of the AND-gate was used. It is possible for WTP 1 itself to compensate if stored water at the plant is available. The non-affected treatment plant (WTP 2) can compensate for failure by means of increased production and drinking water reservoirs. Also reservoirs in the distribution system can be used to prevent failure. The first variant of

the AND-gate was used because only a certain amount of water can be stored and when this is all used, no compensation is possible and the ability cannot be recovered until the initiating failure is remediated.

4.4 Input data and calculations

For the three fault tree examples, historical data and expert judgments by water utility personnel were used to define credibility densities (i.e. densities representing uncertainties) for the basic events [2]. Expert judgements were given as the 5^{th} and 95^{th} percentiles (P05 and P95). Data for all basic events in the examples are presented in Table 1 (see reference number next to each basic event in Figure 6). Variables λ and μ were modelled as exponential rates using Gamma distributions and variable q was modelled using a Beta distribution.

For the approximate DFT calculations the generic equations (Section 3) were used to solve the fault trees and calculate the results at all levels, top and intermediate, in the fault tree. The calculations were performed using Monte Carlo simulations; one of the aims of this approach was to enable uncertainty analysis. The results of these simulations are compared to continuous time simulations of the corresponding Markov process representing the entire fault tree being modelled. For the Monte Carlo simulations 5,000 iterations were run and vales for the input variables are sampled from the densities in Table 1 and densities for the output results are generated. The Markov simulations are repeated the same number of times as the number of iterations in the Monte Carlo simulation. For each Markov simulation a set of input parameters is sampled from the credibility densities defined in Table 1, and the system is then run for at least 10,000 cycles (i.e. up- and downtimes) at the top level. The calculations and simulations were performed in the same way for all three examples, except for the specified number of up- and downtimes which differed due to varying computational demand. The number of cycles was, however, considered more than sufficient in all examples.

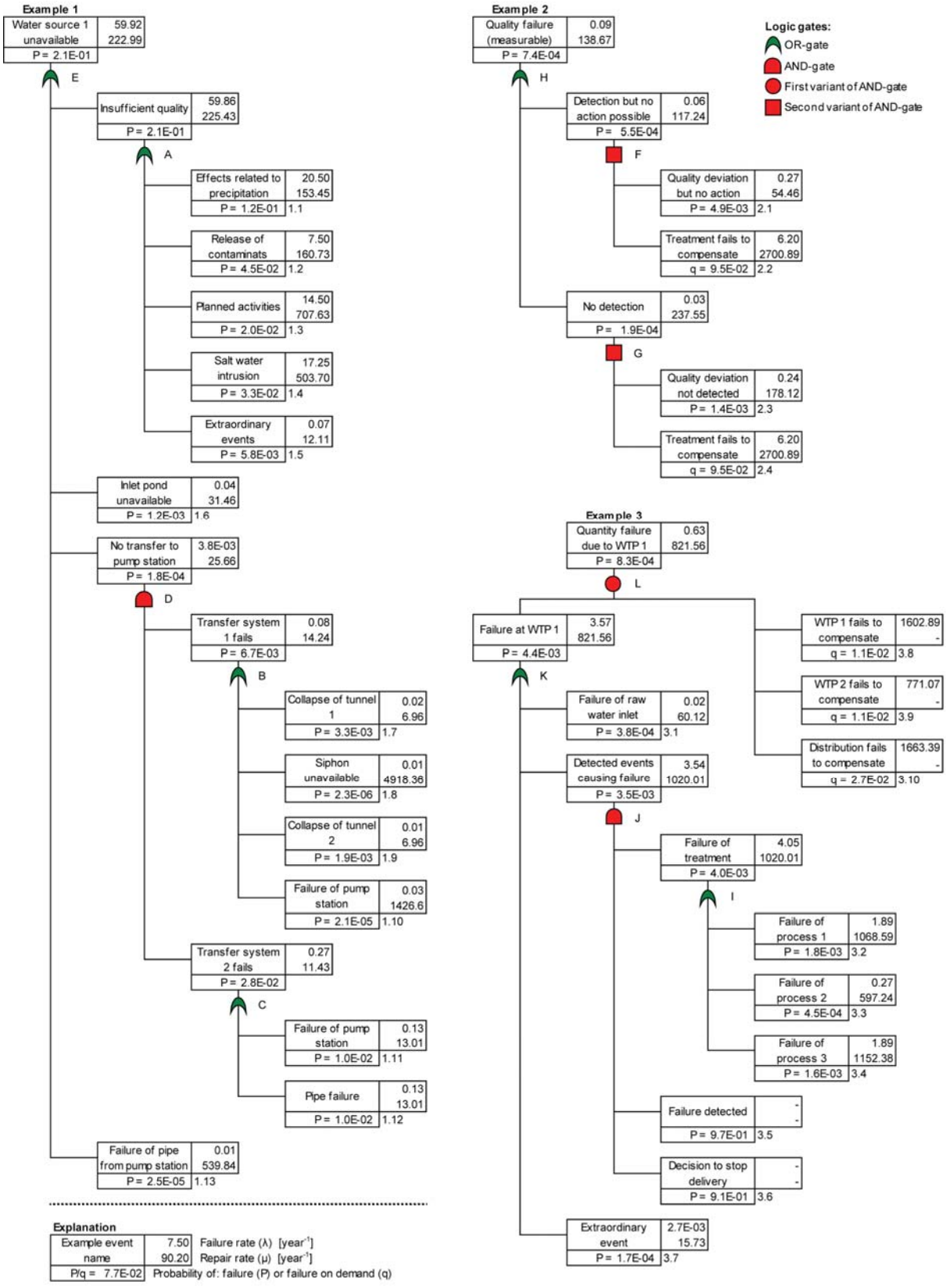

Figure 6 The three fault tree examples used to evaluate the approximate DFT calculations. The input data are presented in Table 1 and the values presented in the fault trees are the expected values.

Table 1 *Input data for the basic events in the three fault tree examples. The mean value and the 5th and 95th percentiles (P05 and P95) are presented for the failure rate (λ), the repair rate (μ) and the probability of failure on demand (q).*

		λ [year^{-1}]			μ [year^{-1}]			q		
Ref.	Basic event	Mean	P05	P95	Mean	P05	P95	Mean	P05	P95
1.1	Effects related to precipitation	20.5	16.9	24.4	153	127	182			
1.2	Release of contaminats	7.5	5.4	9.9	161	116	212			
1.3	Planned activities	14.5	11.5	17.8	708	562	867			
1.4	Saltwater intrusion	17.3	14.0	20.8	504	408	607			
1.5	Extraordinary events	0.070	0.005	0.200	12.1	3.0	26.1			
1.6	Inlet pond unavailable	0.039	0.005	0.100	31.5	6.1	73.0			
1.7	Collapse of tunnel 1	0.023	0.010	0.040	7.0	3.0	12.2			
1.8	Siphon unavailable	0.011	0.005	0.020	4 918	52	17 520			
1.9	Collapse of tunnel 2	0.013	0.005	0.025	7.0	3.0	12.2			
1.10	Failure of pump station	0.029	0.020	0.040	1 427	183	3 650			
1.11	Failure of pump station	0.134	0.050	0.250	13.0	4.1	26.1			
1.12	Pipe failure	0.134	0.050	0.250	13.0	4.1	26.1			
1.13	Failure of pipe from pump station	0.013	0.005	0.025	540	52	1 460			
2.1	Quality deviation but no action	0.27	0.10	0.50	54.5	26.1	91.3			
2.2	Treatment fails to compensate	6.20	3.19	10.03	2 701	1 035	3 914	0.095	0.050	0.150
2.3	Quality deviation not detected	0.24	0.17	0.33	178	52	365			
2.4	Treatment fails to compensate	6.20	3.19	10.03	2 701	1 035	3 914	0.095	0.050	0.150
3.1	Failure of raw water inlet	0.02	0.01	0.04	60.1	18.3	121.7			
3.2	Failure of process 1	1.89	0.50	4.00	1 069	730	1 460			
3.3	Failure of process 2	0.27	0.10	0.50	597	365	876			
3.4	Failure of process 3	1.89	0.50	4.00	1 152	876	1 460			
3.5	Failure detected							0.97*	0.95*	0.98*
3.6	Decision to stop delivery							0.91*	0.85*	0.95*
3.7	Extraordinary event	0.003	0.001	0.005	15.7	3.0	36.5			
3.8	WTP 1 fails to compensate	1603	1095	2190				0.011	0.005	0.020
3.9	WTP 2 fails to compensate	771	54	2204				0.011	0.005	0.020
3.10	Distribution fails to compensate	1663	876	2655				0.027	0.010	0.050

* The value represents the probability of failure since the event is not modelled using up- and downtimes.

5. RESULTS

5.1 Example 1

The first fault tree example is characterised by only including traditional OR- and AND-gates (Figure 6). In Figure 7 the credibility (i.e. uncertainty) densities for the approximate DFT calculations and the Markov simulations are compared at the top level (gate E) for $P(F)$, λ and μ respectively. The three pairs of credibility densities clearly show that the approximate calculations are consistent with the complete Markov simulations. Almost no differences can be seen when comparing the densities.

To further evaluate the results, rejection rates were calculated showing the proportion of the values from the approximate DFT calculations that fall outside the 95 percent confidence interval of the Markov simulated values. The rejection rates for λ and μ are 0.053 and 0.051 respectively. These rates are close to 0.05 and well within a 95 percent symmetric prediction interval based on the Central Limit Theorem for Binomial frequencies. The approximate calculations thus provide results that are in good agreement with the Markov simulations.

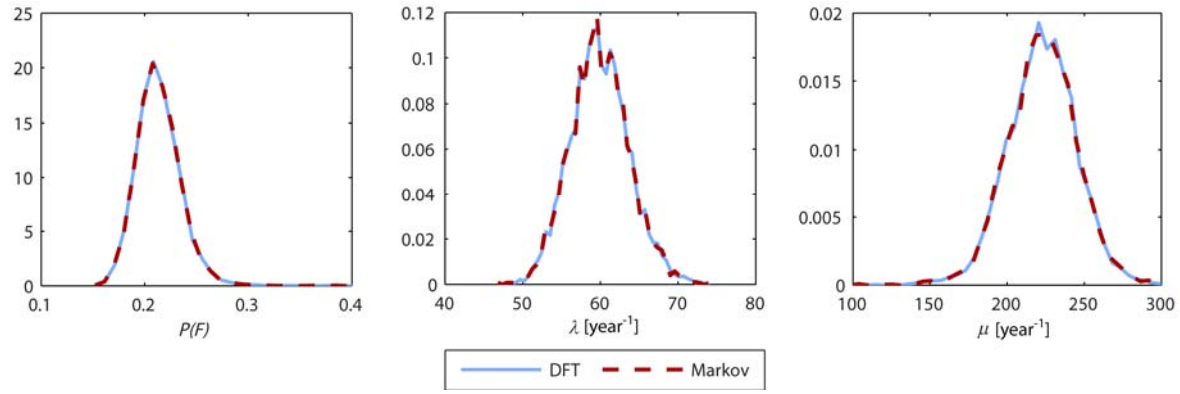

Figure 7 *Credibility densities for the approximate dynamic fault tree (DFT) calculations and the complete Markov simulations for P(F), λ and μ respectively.*

The input data for the basic events are assumed to be Markovian failure (up) and repair (down) rates. The question is, however, if the up- and downtimes at the top event are exponential(λ) and exponential(μ) respectively. In Figure 8 two graphs are presented showing the up- and downtimes from the Markov simulations and the corresponding exponential distributions defined by the mean failure rate and repair rate values from the approximate DFT calculations. As can be seen from Figure 8, there is a good agreement for the uptime but the downtime is not exponential.

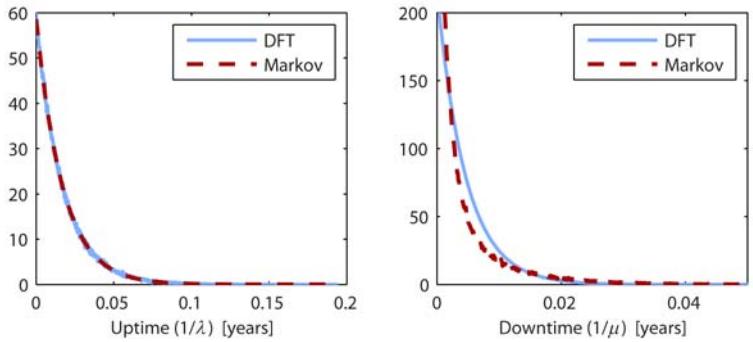

Figure 8 *Comparison to see if the up- and downtimes at the top event are exponentially distributed with rates λ and μ respectively. The up- and downtimes from the Markov simulations are plotted and compared to reference densities, based on the mean values from the approximate dynamic fault tree (DFT) calculations.*

5.2 Example 2

The second fault tree example includes one traditional OR-gate and two second-variant AND-gates (Figure 6). In Figure 9 the credibility densities for the approximate DFT calculations and the complete Markov simulations are presented at the top event (gate H) and compared for $P(F)$, λ and μ respectively. As was the case also for the first example, almost no differences can be seen in the results from the approximate calculations and the Markov simulations.

The rejection rates were calculated to 0.056 and 0.050 for λ and μ respectively. Both are within a 95 percent symmetric prediction interval based on the Central Limit Theorem for Binomial frequencies, thus confirming what is shown in the graphs in Figure 9. However, note that the rejection rate for λ is on the upper boundary of the interval. This may indicate that the error in the approximate DFT calculation of λ is detectable in large simulations.

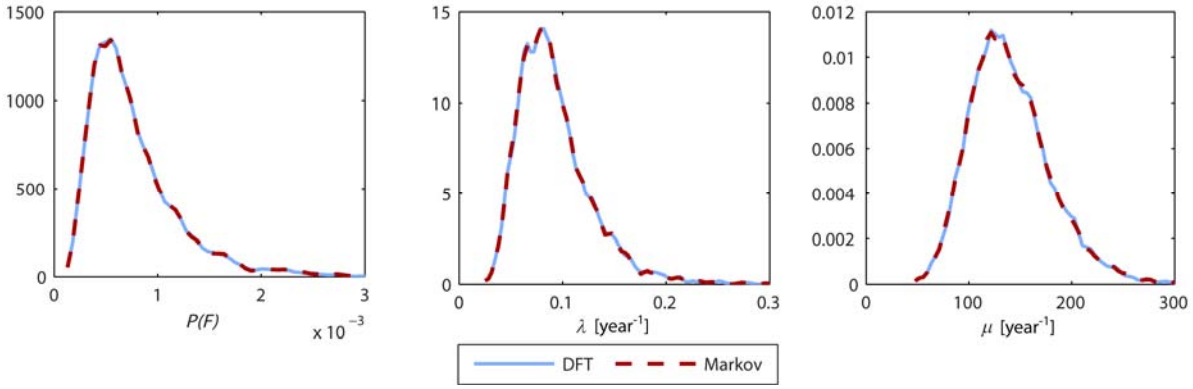

Figure 9 *Credibility densities for the approximate dynamic fault tree (DFT) calculations and the complete Markov simulations for P(F), λ and μ respectively.*

In Figure 10 the up- and downtimes are presented for the Markov simulations and a reference density based on the mean values from the approximate calculations. The graphs in Figure 10 do not match perfectly, especially not for the downtime. Hence, the up- and downtimes cannot be assumed to be exponentially distributed.

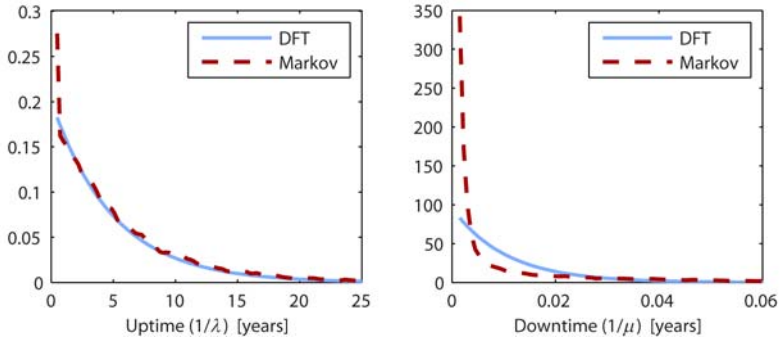

Figure 10 *Comparison to see if the up- and downtimes at the top event are exponentially distributed with rates λ and μ respectively. The up- and downtimes from the Markov simulations are plotted and compared to reference densities, based on the mean values from the approximate dynamic fault tree (DFT) calculations.*

5.3 Example 3

The third fault tree example includes traditional OR- and AND-gates but differs from the other examples since it includes also the first variant of the AND-gate (Figure 6). As shown in Figure 6 the fault tree includes three different events/components that may compensate for failure (events 3.8-3.10). It is concluded that the number of compensating events affects the error in the results. Therefore, this fault tree was simulated including only one compensating event (3.8), including two events (3.8 and 3.9) and including all three events. We refer to these three variants as example 3a, b and c respectively. The credibility densities (Figure 11) for the approximate DFT calculations and the Markov simulations are compared at the top level (gate E) for $P(F)$, λ and μ respectively. The densities show that when one compensating event is included the results are in good agreement (Figure 10a-c), but when two, and in particular three, compensating events are included the errors increase (Figure 10d-f and g-i respectively).

For all three variants of example 3 the probability of failure is underestimated and the rates λ and μ are overestimated using the approximate calculations. The mean probability of failure is underestimated by 4, 32 and 57 percent for examples 3a, b and c respectively. The mean

values for the rate λ are overestimated by 9, 18 and 27 percent respectively for the three cases. The largest errors occur in the rate μ where the approximate calculations give a mean value twice as big as the Markov simulations for example 3c. For examples 3a and b the rate μ is overestimated by 13 and 64 percent respectively.

For example 3a the errors are small, especially when considering the uncertainties in the estimates caused by uncertainties in the input data. When two or three compensating events are included the errors are not negligible. However, considering the uncertainties in the input data the results give a reasonably good indication of the true value for the probability of failure and the failure rate.

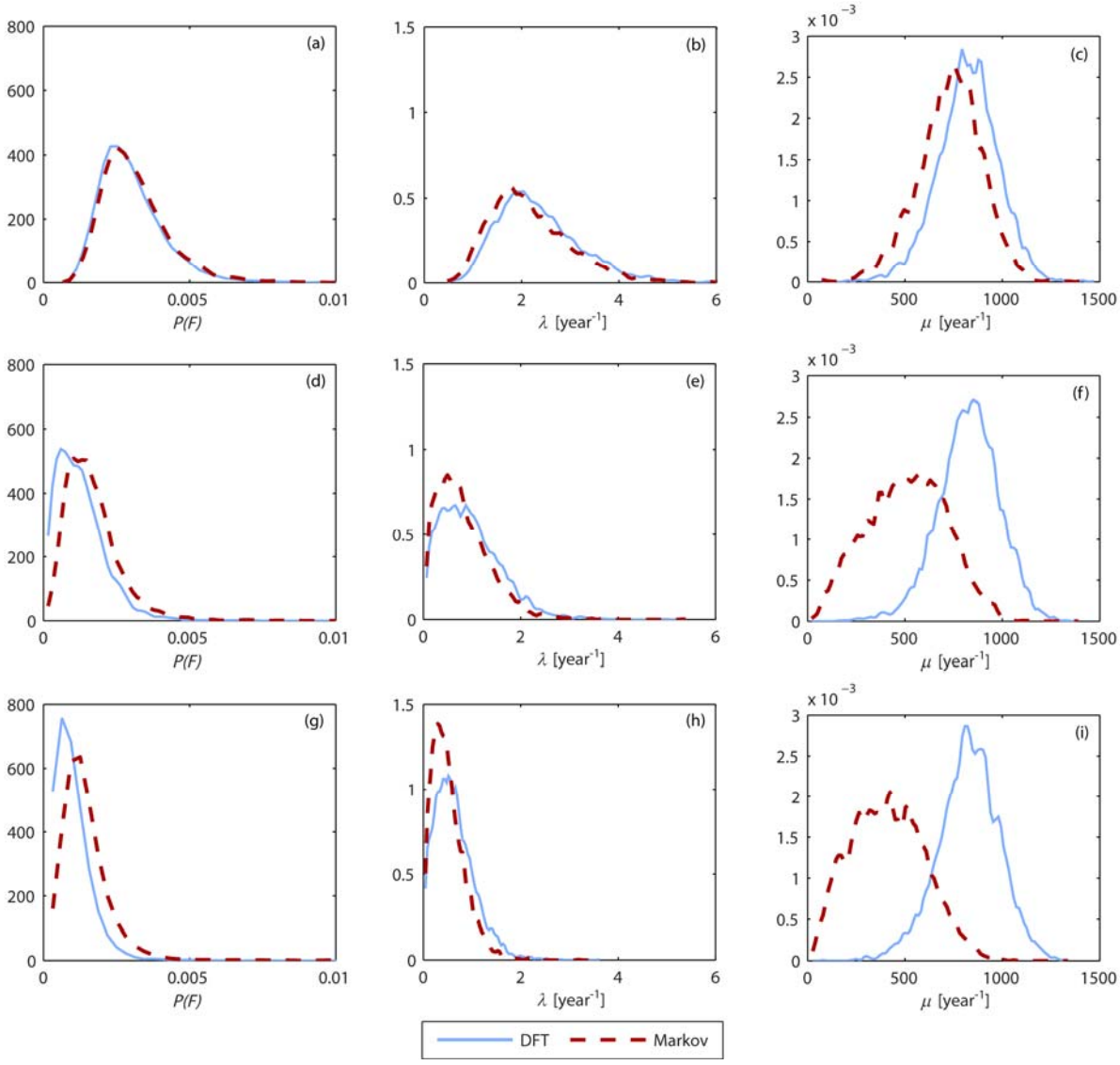

Figure 11 Credibility densities for the approximate dynamic fault tree (DFT) calculations and the complete Markov simulations for P(F), λ and μ respectively. Figures a-c represent the case when only one compensating event was included in the model, for d-f the model included two compensating events and for g-i all three events were included.

As for examples 1 and 2 (Figures 8 and 10) the up- and downtimes for example 3 cannot be considered to be exponentially distributed. The results are similar for all three variants of example 3.

6. DISCUSSION AND CONCLUSIONS

When only traditional OR- and AND-gates were used, the approximate DFT calculations gave almost no errors in the results. For the second variant of the AND-gate, the results were also in very good agreement with the Markov simulations. For the first variant of the AND-gate only small errors were observed when one compensating event/component was included. However, when two or three compensating events were included, the errors were not negligible. Hence, the number of compensating events should be kept to a minimum to not cause severe errors in the results.

One of the ideas with the approximate calculation was to enable uncertainty analysis by performing Monte Carlo simulations. Considering the uncertainties in the input data for the examples presented here, and the application by Lindhe *et al.* [2], the errors in the results can be accepted. The entire fault tree used by Lindhe *et al.* [2] includes fifteen second-variant AND-gates and of the first variant there are three with one compensating event, two with two compensating events and two with three compensating events. The first variant AND-gates are all placed at a high level in the fault tree and a sensitivity analysis presented by Lindhe [20] showed that the input parameters to these gates are not the ones contributing most to the uncertainties in the results at the top level. The errors in the results are considered acceptable when compared to the uncertainties in the results caused by uncertainties in the input parameters.

To correctly model a system it may be necessary to include more than one compensating event/component in a first variant AND-gate. In such cases, the fault tree model should be structured to correctly represent the analysed system but uncertainty analysis should be performed to determine what basic events contribute most to the uncertainties in the results. If the events representing the compensating components have a relatively small effect on the uncertainties in the results, the model can be used. However, to handle situations where the effect is significant, several compensating events could, if possible, be described as one event. Another solution is to model this small part of the fault tree using Markov simulations and use the results as input to the approximate DFT calculations. It is a future task to provide a proper way to combine several compensating events into one that can be used as input in a fault tree model.

As shown in all three examples, the up- and downtimes are not exponential(λ) and exponential(μ) respectively. Consequently, the calculated rates cannot be used to calculate the probability of, for example, failure during a specific time period. However, the possibility to estimate not only the probability of failure, but also the failure rate and the mean downtime at each intermediate level provides valuable information on the system's dynamic behaviour. Two subsystems may have the same probability of failure but different failure rates and downtimes. Properties like these are important to know about when analysing a system and evaluating risk-reduction measures.

To understand the function of system, it is important to not only study the top event in the fault tree but also the intermediate events. When a fault tree model is constructed, information on intermediate events also simplifies model evaluation. An additional reason for using up- and downtimes, or the corresponding rates λ and μ, is that it is often easier to estimate these parameters instead of directly estimating the probability of an event. Information on component failure and other events in drinking water systems is often available in the form of rates or times. Also the elicitation of expert judgements may be easier if rates and times are used instead of probabilities.

Compared to complete Markov simulations the approximate DFT calculations make the model building easier and reduce the computational burden remarkably. This is especially true

for extensive fault tree models. Software for performing Monte Carlo simulations is required but the fault tree model and the calculations can be built and performed using common spreadsheet software.

The variants of the AND-gate make it possible to consider the inherent ability of a system to compensate for failure. Hence, drinking water systems can be modelled in a correct manner that in most cases is not possible if only traditional OR- and AND-gates are used. The application of approximate DFT calculations in the case studies presented by Lindhe *et al.* [2, 3] and Rosén *et al.* [19] showed that the calculations facilitate the work of modelling water supply risks and evaluating the effect of risk-reduction measures. Compared to traditional fault tree calculations the dynamic calculations provide additional and useful information when analysing drinking water systems. Information on up- and downtimes at all levels in the fault tree facilitates system evaluation. The approximate DFT calculations have been applied to model water supply risks but they are most likely also applicable and useful in other fields.

The main conclusions of this paper are:

- For the traditional OR- and AND-gates, and the second variant of the AND-gate, there are only very small errors in the results of the approximate DFT calculations.
- For the first variant of the AND-gate the errors in the DFT results increase with the number of compensating events/components included. Hence, the number of compensating events modelled using the first variant AND-gate should be kept to a minimum, preferably only one. When several compensating events are needed to model a system correctly, uncertainty analysis should be performed to see how the events affect the results.
- By combining the approximate DFT calculations with Monte Carlo simulations, uncertainty analysis is enabled. It is shown that the errors in the approximate calculations are in most cases small and acceptable when considering uncertainties in input data and results.
- The approximate DFT calculations facilitate simple model building and calculations that are less computationally demanding than Markov simulations.
- When a system is analysed it is not only the results at the top level that should be evaluated. Information on failure probabilities, failure rates (or uptimes) and mean downtimes at all levels in the fault tree are important in the evaluation of the system.

The work has shown that approximate DFT calculations in combination with Monte Carlo simulations provides a practically applicable technique for analysing risks to drinking water systems, including modelling and evaluation of risk-reduction measures. The variants of the common type AND-gate make it possible to model entire drinking water systems, from source to tap, in a correct way.

ACKNOWLEDGEMENTS

The work presented in this paper has been performed with support from the Swedish Water and Wastewater Association and the City of Gothenburg. The work has partly been carried out within the framework of the TECHENAU project (Technology Enabled Universal Access to Safe Water – www.techenau.org), funded by the European Commission (contract no. 018320).

REFERENCES

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

[2] Lindhe A, Rosén L, Norberg T, Bergstedt O. Fault tree analysis for integrated and probabilistic risk analysis of drinking water systems. Water Research. 2009;43:1641-53.

[3] Lindhe A, Rosén L, Norberg T, Bergstedt O, Pettersson TJR. Cost-effectiveness analysis of risk-reduction measures to reach water safety targets. Water Research. 2011;45:241-53.

[4] Dugan JB, Bavuso SJ, Boyd MA. Dynamic fault-tree models for fault-tolerant computer systems. IEEE Transactions on Reliability. 1992;41:363-77.

[5] Vesely WE, Stamatelatos M, Dugan JB, Fragola J, Minarick J, Railsback J. Fault Tree Handbook with Aerospace Applications. Washington: NASA Office of Safety and Mission Assurance; 2002.

[6] Durga Rao K, Gopika V, Sanyasi Rao VVS, Kushwaha HS, Verma AK, Srividya A. Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. Reliability Engineering & System Safety. 2009;94:872-83.

[7] Cepin M, Mavko B. A dynamic fault tree. Reliability Engineering & System Safety. 2002;75:83-91.

[8] Amari S, Dill G, Howald E. A new approach to solve dynamic fault trees. Annual Reliability and Maintainability Symposium 2003: IEEE; 2003. p. 374-9.

[9] Boudali H, Crouzen P, Stoelinga M. A Compositional Semantics for Dynamic Fault Trees in Terms of Interactive Markov Chains. In: Namjoshi KS, Yoneda T, Higashino T, Okamura Y, editors. Automated Technology for Verification and Analysis. Heidelberg: Springer; 2007. p. 441-56.

[10] Durga Rao K, Sanyasi Rao VVS, Verma AK, Srividya A. Dynamic Fault Tree Analysis: Simulation Approach. In: Faulin J, Juan AA, Martorell Alsina SS, Ramírez-Marquez JE, editors. Simulation Methods for Reliability and Availability of Complex Systems. London: Springer; 2010. p. 41-64.

[11] Cepin M. Analysis of truncation limit in probabilistic safety assessment. Reliability Engineering & System Safety. 2005;87:395-403.

[12] Epstein S, Rauzy A. Can we trust PRA? Reliability Engineering & System Safety. 2005;88:195-205.

[13] Huang C-Y, Chang Y-R. An improved decomposition scheme for assessing the reliability of embedded systems by using dynamic fault trees. Reliability Engineering & System Safety. 2007;92:1403-12.

[14] Boudali H, Dugan JB. A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering & System Safety. 2005;87:337-49.

[15] Boudali H, Dugan JB. A continuous-time Bayesian network reliability modeling, and analysis framework. IEEE Transactions on Reliability. 2006;55:86-97.

[16] Marquez D, Neil M, Fenton N. Improved reliability modeling using Bayesian networks and dynamic discretization. Reliability Engineering & System Safety. 2010;95:412-25.

[17] Norberg T, Rosén L, Lindhe A. Added value in fault tree analyses. In: Martorell S, Guedes Soares C, Barnett J, editors. Safety, Reliability and Risk Analysis: Theory, Methods and Applications. European Safety and Reliability Association 2008 and 17th Society for Risk Analysis Europe Conference, Valencia, 22-25 September: Taylor & Francis Group; 2009. p. 1041-8.

[18] Rausand M, Høyland A. System reliability theory: models, statistical methods, and applications. 2nd ed. N.J.: Wiley-Interscience; 2004.

[19] Rosén L, Lindhe A, Bergstedt O, Norberg T, Pettersson TJR. Comparing risk-reduction measures to reach water safety targets using an integrated fault tree model. Water Science and Technology: Water Supply. 2010;10:428-36.

[20] Lindhe A. Risk Assessment and Decision Support for Managing Drinking Water Systems [PhD Thesis No. 3119]. Gothenburg: Chalmers University of Technology; 2010.