MŰEGYETEM 1782

Critical Embedded Systems

Reliability modelling with fault trees

Introduction to the usage of the **TopEvent FTA** tool

András Vörös

Rebeka Farkas

Version: 2.0

Budapest University of Technology and Economics
Department of Measurement and Information Systems

1 Introduction

Reliability modelling is becoming an increasingly important task in the design of today's IT infrastructures. As the services have more and more tasks, failures are becoming more costly for companies. The table below contains data of a study from 2003, which shows the cost of service outage in some industries:

Case study	Yearly income	Cost of outage	Cost/hour
Energy industry	6.75 billion $	4.3 million $	1624 $
„High tech”	1.3 billion $	10.2 million $	4,167 $
Health care	44 billion $	74.6 million $	96,632 $
Travel	850 million $	2.4 million $	38,710 $
Finance (USA)	4.0 billion $	10.6 million $	28,342 $

In order to be able to estimate the costs (and dangers) in advance, we need the means of reliability modelling and the underlying mathematics.

2 Modelling formalisms (overview)

There are two major approaches to calculate the reliability (and related) properties of the systems: simulation and analytical methods.

The advantage of simulation is that any model can be analysed, there are not so tight constraints (distributions, modelled behaviours) like the ones that characterize the analytic solvability. However, the major drawback is that the obtained information is limited: in many cases it cannot be decided whether enough simulation cases have been executed.

The analytical solution has the advantage that it gives accurate results. However, it cannot be used for many models, especially for dynamic models.

The various approaches and options are shown in the following figure:

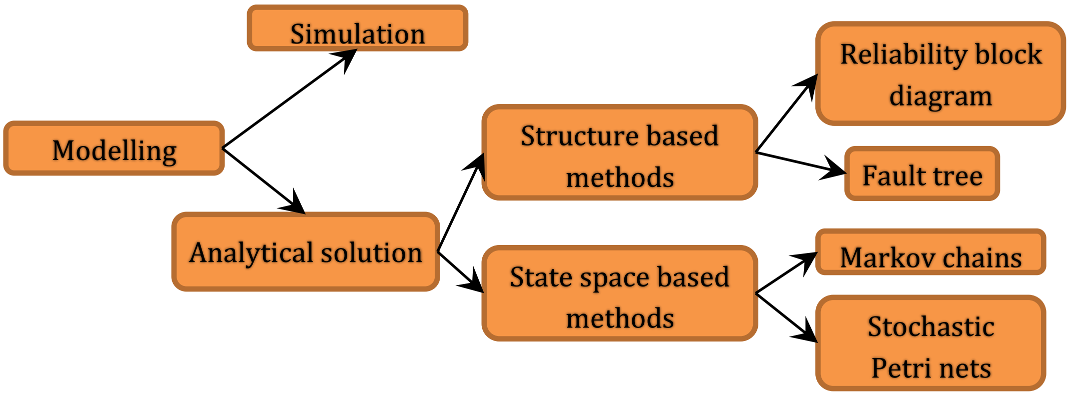

Figure 1. Reliability modelling overview

3 Modelling example

In the following section the concept of fault tree modelling is introduced with the help of the tool **TopEvent FTA**. In addition we review the analysis capabilities of such approaches.

3.1 Example infrastructure

We are going to design the fault tree model of a simple computer infrastructure. Our example is a simple network infrastructure providing web and other services.

The infrastructure consists of the following components: one cluster of web servers, one cluster of SQL (database) servers and the Disk subsystem providing services for the database servers. This solution is redundant regarding the web servers and SQL servers which increases the availability: if one of the web servers or the SQL servers is out, the service is still on. In the following we are going to analyse the causes of the outage of the full service (provided by the infrastructure).

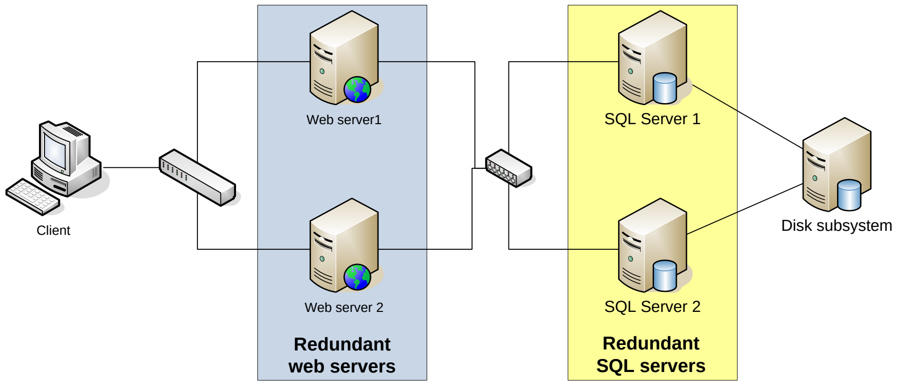

Figure 2. web infrastructure

3.2 Designing the fault tree

We start the design by choosing the top level event: this is the outage of the service. In order to be able to run the service, we need at least: one working web server, one working SQL server and the working disk subsystem.

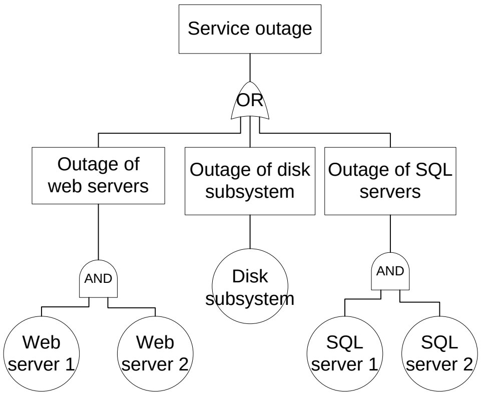

Figure 3. Fault tree of web infrastructure

In the following we show the fault tree model of Figure 3 designed in the tool *TopEvent FTA*:

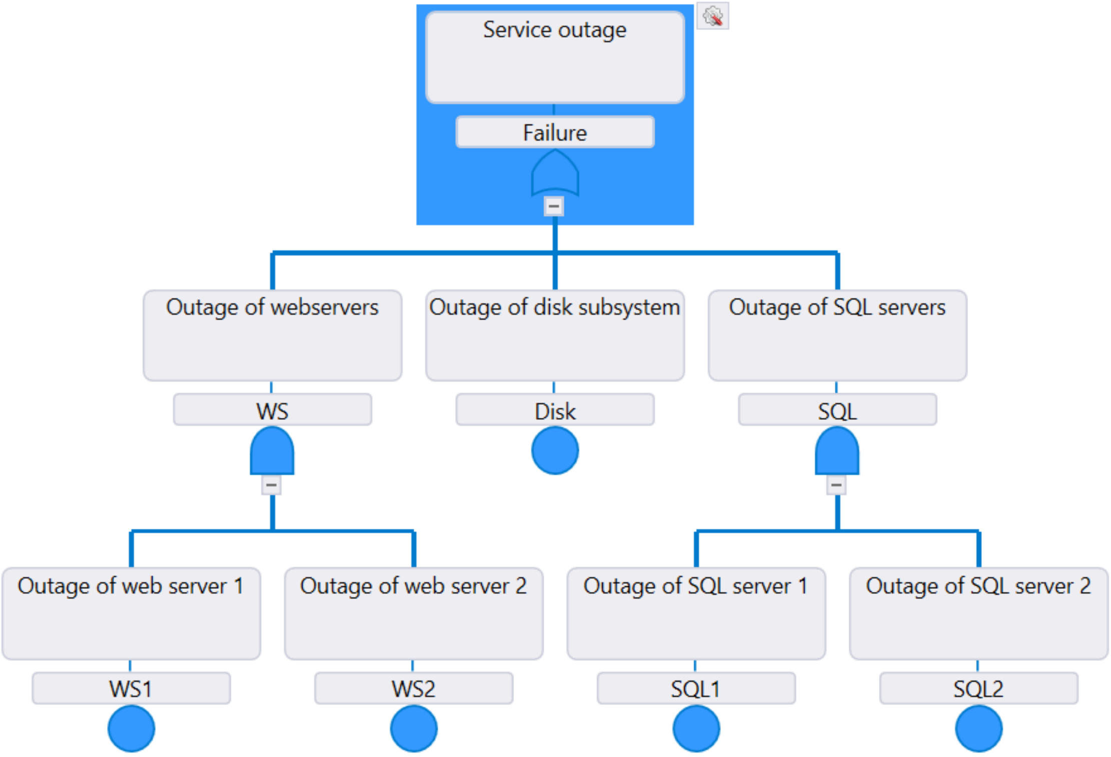

Figure 4. Fault tree of the infrastructure in *TopEvent FTA*

As the figure shows, the SPOF (Single Point of Failure) of the system is the disk subsystem: the outage of the disk subsystem is enough in itself to cause system level outage.

3.3 Measurements

We are going to model the reliability of the components by exponential distribution (with parameter λ), where the expected value (or expectation, mathematical expectation, EV, mean, or first moment) of the failure is 1/ λ.

The components have the following reliability parameters:

component	λ
web server	0.05
SQL server	0.01
disk subsystem	0.2

Using *TopEvent FTA*, we can set these parameters in the *Models* window, double clicking on the *Function* cell of each model. The *Model type* is unrepairable.

After setting all parameters the evaluation can be performed by clicking *Evaluate Fault Tree* in the *Fault Tree* tab of *TopEvent FTA.* Set *Mission time* to 8 units. Click on *Evaluate Fault Tree.*

In the upper part of the appearing window the fault tree can be seen with the *Unavailability* values of each nodes, the value at the root node representing the unavailability of the system. In the lower part the *Unavailability curve* of the system can be seen, as depicted in Figure 5. (The *Unavailability* of a system at a moment of time is the probability of the system not working in that moment.)

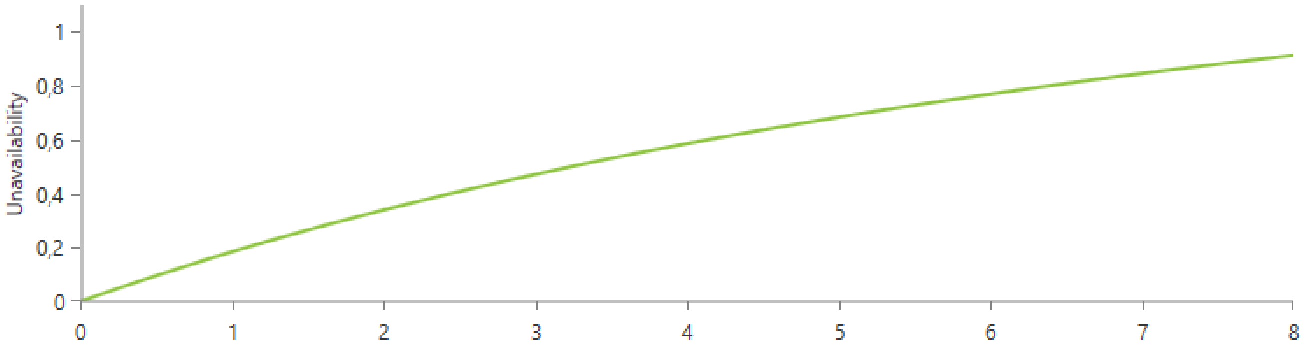

Figure 5. Unavailability curve of the infrastructure

It is also possible to depict the unavailability of a subsystem by clicking on the corresponding node of the fault tree (or selecting it from the list above).

The unavailability values in each time units can be seen by clicking on *Grid* above the diagram. It is possible to export these values to spreadsheet *.txt, .csv,* or *Excel* file in the *Unavailability* tab of the program that can be reached from the *Project Explorer.*

As identified from the fault tree, the SPOF is the disk subsystem in our infrastructure. We would like to increase the availability; a straightforward approach is to use a redundant disk subsystem. In the following we are going to examine the reliability of a modified system: we are going to use a redundant disk subsystem, where there will be two of them. The modified fault tree is depicted in the following figure: we are going to use an AND gate joining the events of the failure of the SQL server 1 and SQL server 2. As they provide the service in a redundant way: any one of them is working means that the service of the disk system is up.

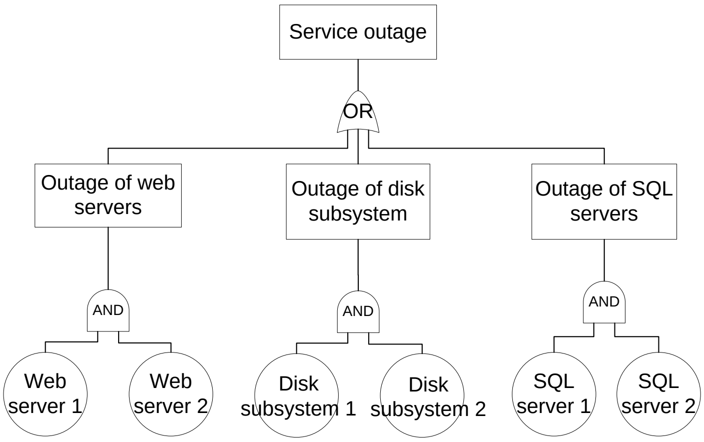

Figure 6. Modified fault tree

Executing the same evaluation on the modified tree produces a lower *unavailability* on the top node and a different curve.

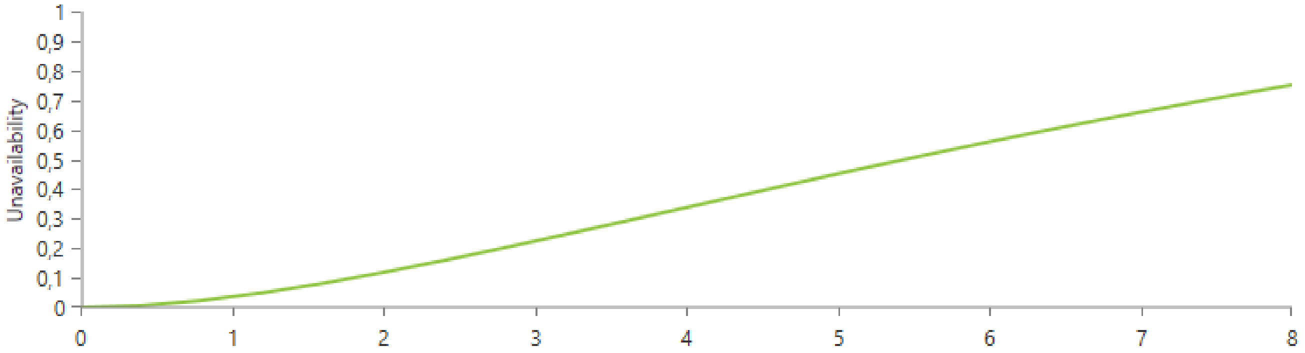

Figure 1. Unavailability curve of the modified infrastructure

3.4 Extra task

Modify the fault tree model and further increase the redundancy by using one more disk subsystem! Analyse the reliability curve: how does the added disk subsystem modified the reliability? Does it have the same effects as it was for the second one?