Added value in fault tree analyses

Tommy Norberg, Andreas Lindhe & Lars Rosén

Chalmers University of Technology
University of Gothenburg
Göteborg
SWEDEN

Reliability of complex systems

- Göteborg Water
- Fault tree analysis
  - Probability of failure is

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

  - Inherent ability to compensate failures
- Dynamic approach needed

Fault trees

Fault trees are built by logic gates,
the main types of which are the OR gate,

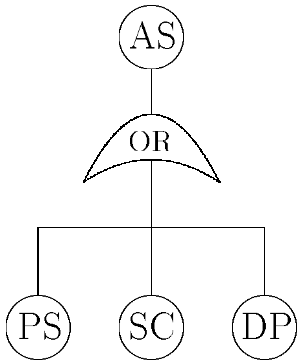
$$F = \bigcup_i F_i$$

and the AND gate,

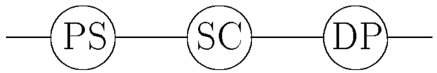
$$F = \bigcap_i F_i$$

Structural reliability

The OR gate corresponds to a series system.



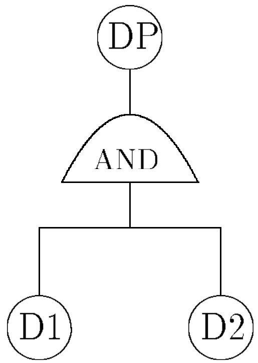
$\Leftrightarrow$



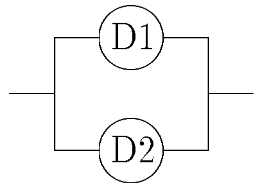
$$F^c_{\text{AS}} = F^c_{\text{PS}} \cap F^c_{\text{SC}} \cap F^c_{\text{D}}$$

Similarly,

The AND gate corresponds to a parallell system.



$\Leftrightarrow$



$$F^c_{\mathrm{DP}} = F^c_{\mathrm{D1}} \cup F^c_{\mathrm{D2}}$$

Independence

If the base events, i.e F_i's, are independent, then, for the OR gate,

$$P(F) = 1 - \prod_i (1 - P(F_i))$$

and, for the AND gate,

$$P(F) = \prod_i P(F_i)$$

Independence will be assumed below.

Probability of failure

Assuming ergodicity, $P(F)$ can be thought of as the ratio between the Mean Down Time (MDT) and the Mean Time Between Failures (MTBF),

$$P(F) = \frac{\mathrm{MDT}}{\mathrm{MTBF}}$$

where

$$\mathrm{MTBF} = \mathrm{MUT} + \mathrm{MDT}$$

and MUT is short for Mean Up Time.

In a dynamic analysis at least two members of the triplet

$$P(F),\ \mathrm{MUT},\ \mathrm{MDT}$$

need to be assessed.

Markovian base component rates

In a two-state Markovian model of base component i,

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

where λ_i is its failure rate, and $1/\mu_i$ is its mean down time.

Markovian sub-system rates

For the sub-system comprising a logic gate, assume that it has constant failure rate λ, and write $1/\mu$ for its mean down time. Then

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

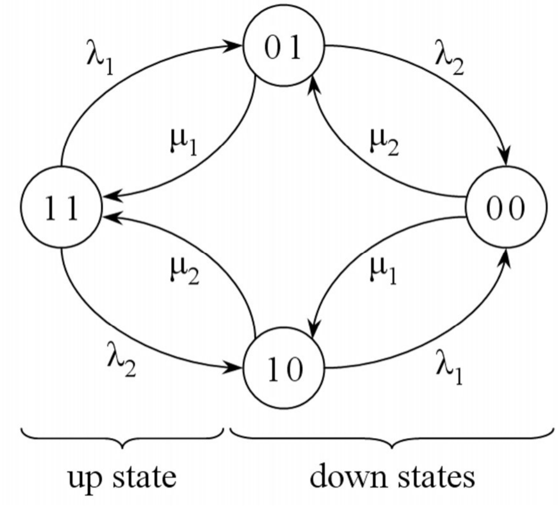
Clearly, neither λ nor μ is necessarily constant.

Also, if two of

$$P(F),\ \lambda,\ \mu$$

are known, so is the third.

The OR gate



State diagram of a Markov Process representing an OR gate with two basic events. The MP is down if at least one base MP is down.

We conclude, for the OR gate,

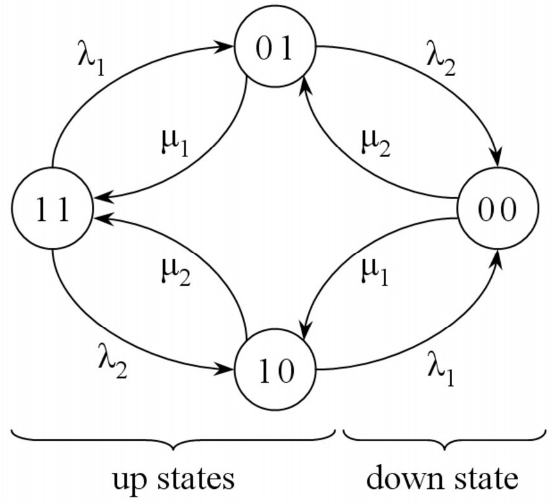
$$P(F) = 1 - \prod_i \frac{\mu_i}{\lambda_i + \mu_i}$$

$$\lambda = \sum_i \lambda_i$$

And also,

$$\mu = \frac{1 - P(F)}{P(F)}\,\lambda$$

The AND gate



State diagram of a Markov Process representing an AND gate with two basic events. The MP is down when all base MPs are down.

We conclude, for the AND gate,

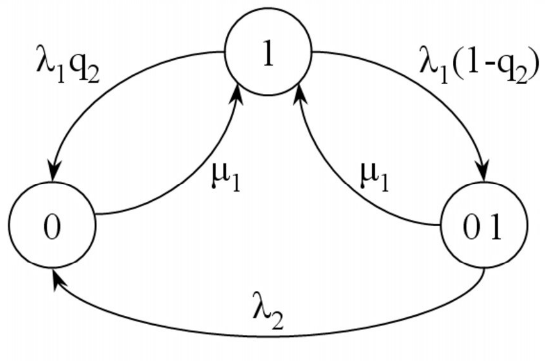
$$P(F) = \prod_i \frac{\lambda_i}{\lambda_i + \mu_i}$$

$$\mu = \sum_i \mu_i$$

And also

$$\lambda = \frac{P(F)}{1 - P(F)}\,\mu$$

Dynamic AND-variant 1



State diagram of an MP representing a dynamic variant of the AND gate. The MP is down while being in state 0.

For the AND1 gate with an arbitrary number of 'reservoirs',

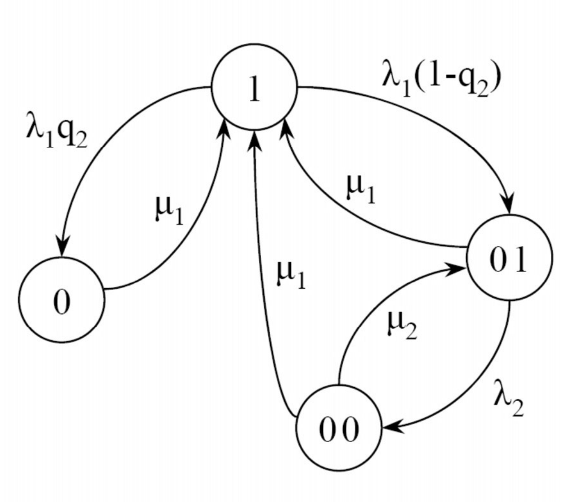
$$P(F) = \frac{\lambda_1}{\lambda_1 + \mu_1} \prod_{i \neq 1} \frac{\lambda_i + q_i \mu_1}{\lambda_i + \mu_1}$$

$$\mu = \mu_1$$

and, again,

$$\lambda = \frac{P(F)}{1 - P(F)} \, \mu$$

Dynamic AND-variant 2



State diagram of an MP representing a 2nd dynamic variant of the AND gate. The MP is down while being in state 0 or 00.

For the AND2 gate with one 'reservoir',

$$P(F) = \frac{\lambda_1}{\lambda_1 + \mu_1} \frac{\lambda_2 + q_2(\mu_1 + \mu_2)}{\lambda_2 + \mu_1 + \mu_2} = 1 - (p_1 + p_{01})$$

where

$$p_1 = \frac{\mu_1}{\lambda_1 + \mu_1} \quad \text{and} \quad p_{01} = \frac{\lambda_1(1 - q_2)}{\lambda_1 + \mu_1} \frac{\mu_1 + \mu_2}{\lambda_2 + \mu_1 + \mu_2}$$

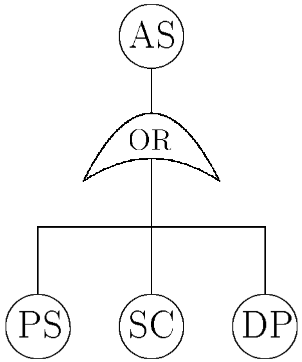
are the stationary probabilities for being in the up states 0 and 01, respectively.

Moreover,

$$\lambda = \frac{p_1 \lambda_1 q_2 + p_{01} \lambda_2}{1 - P(F)}$$

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

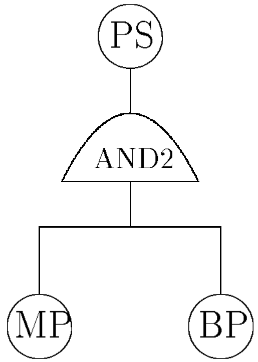
Example: Alarm System



An Alarm System that consist of a Power Supply, a Supervisong Computer and a Detector Package.

A dynamic analysis is needed. Of particular importance is the frequency of stops that last for more than 12 hours.

The Power Supply



$\lambda_1 = 0.002$ $\quad$ $\lambda_2 = 0.11$
$1/\mu_1 = 4$ $\quad$ $1/\mu_2 = 0.5$
$q_2 = 0.1$

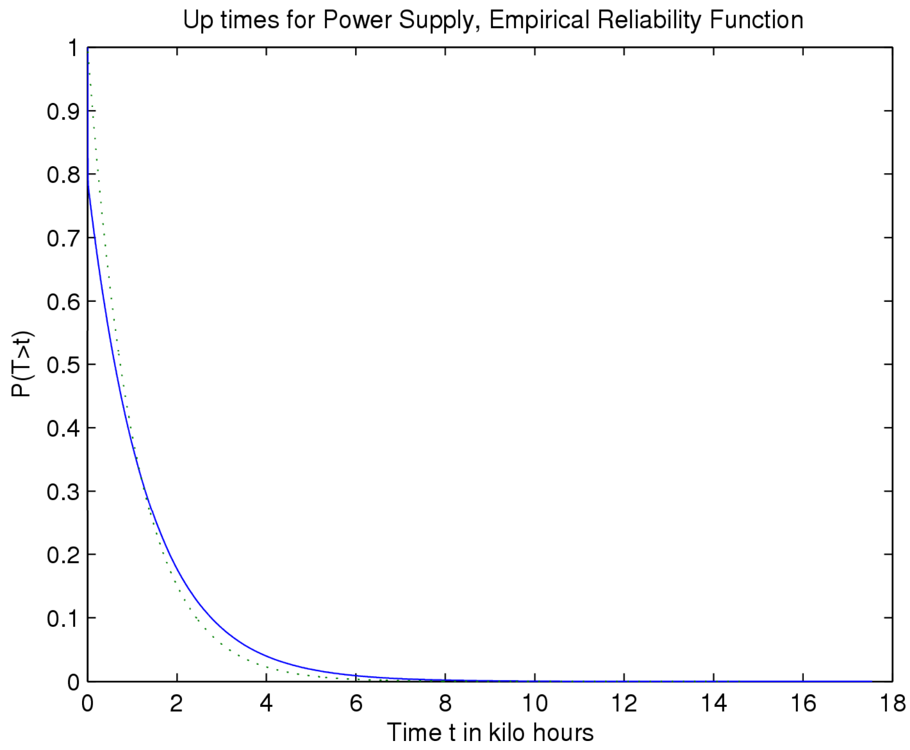
Fault tree representation of the Power Supply. Its components are the Main Power (MP) and the Back-up Power (BP) sub-systems.

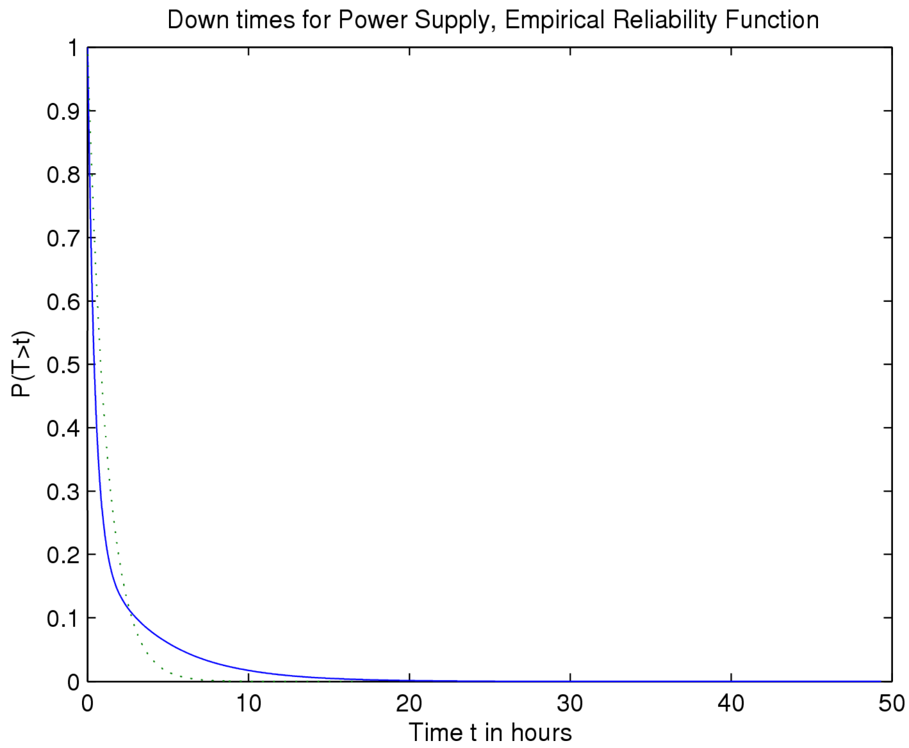
The time unit is hours.

Results for the Power Supply sub-system

	DFT calculations	Simulation		
		LCL	EST	UCL
$10^3 P(F)$	1.127	1.123	1.127	1.132
$10^3 \lambda$	0.9475	0.9447	0.9470	0.9494
$1/\mu$	1.190	1.187	1.192	1.196
$10^3 \lambda_{\mathrm{LS}}$	0.409		0.0099	

where $\lambda_{\mathrm{LS}} = \lambda e^{-12\mu}$.

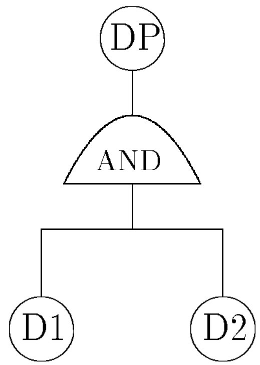

Up times for Power Supply, Empirical Reliability Function
P(T>t)
Time t in kilo hours
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
2
4
6
8
10
12
14
16
18


Down times for Power Supply, Empirical Reliability Function
P(T>t)
Time t in hours
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
10
20
30
40
50

The Supervising Computer

$$\lambda = 0.0001$$
$$1/\mu = 100$$
$$10^3 P(F) = 9.901$$
$$10^3 \lambda_{\mathrm{LS}} = 0.099$$

The Detector Package

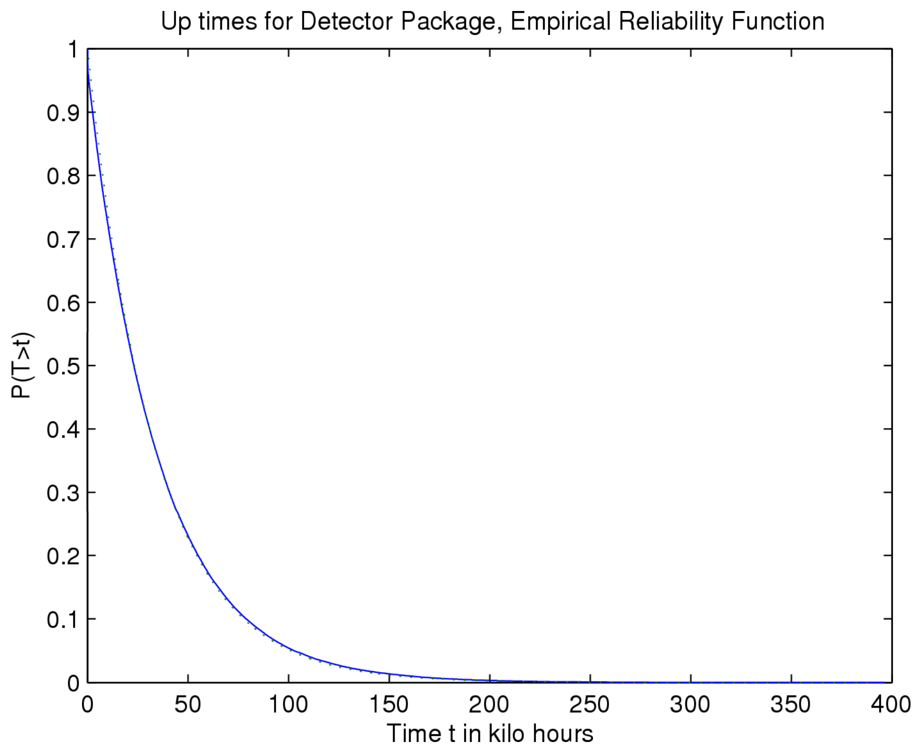


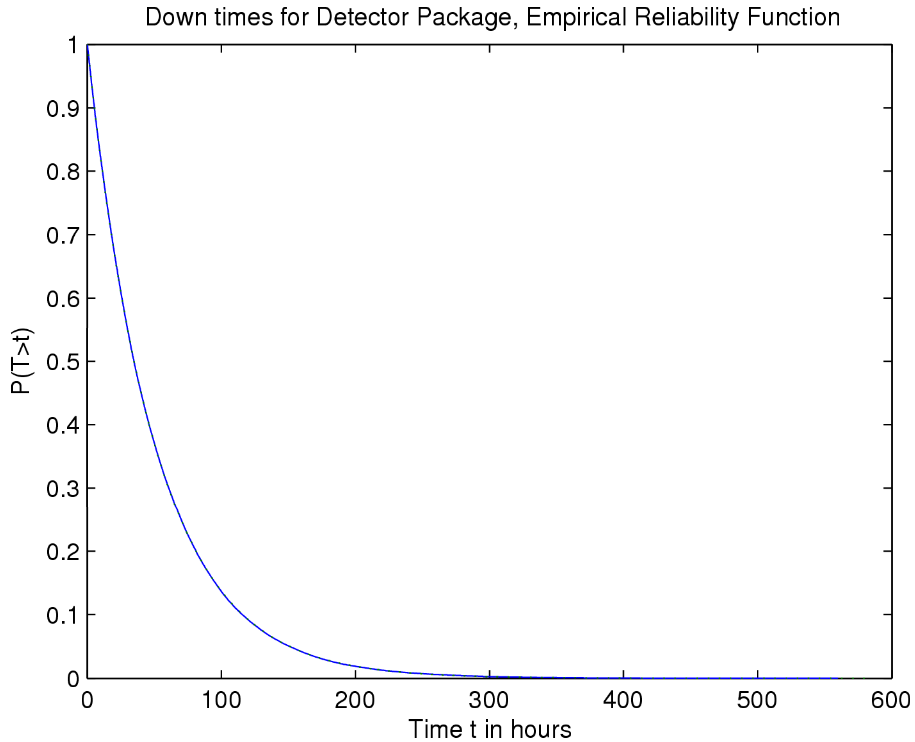
$$\lambda_1 = \lambda_2 = 0.0004$$
$$1/\mu_1 = 1/\mu_2 = 100$$

Fault tree representation of the Detector Package consisting of two identical detectors connected in parallell.

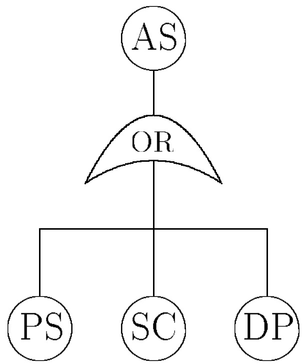
Results for the Detector Package sub-system

	DFT calculations	Simulation LCL	Simulation EST	Simulation UCL
$10^3 P(F)$	1.479	1.482	1.492	1.501
$10^3 \lambda$	0.02963	0.02948	0.02967	0.02987
$1/\mu$	50	50.04	50.36	50.67
λ_{LS}	0.029		0.023	


Up times for Detector Package, Empirical Reliability Function
P(T>t)
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
50
100
150
200
250
300
350
400
Time t in kilo hours


Down times for Detector Package, Empirical Reliability Function
P(T>t)
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
100
200
300
400
500
600
Time t in hours

The complete Alarm System

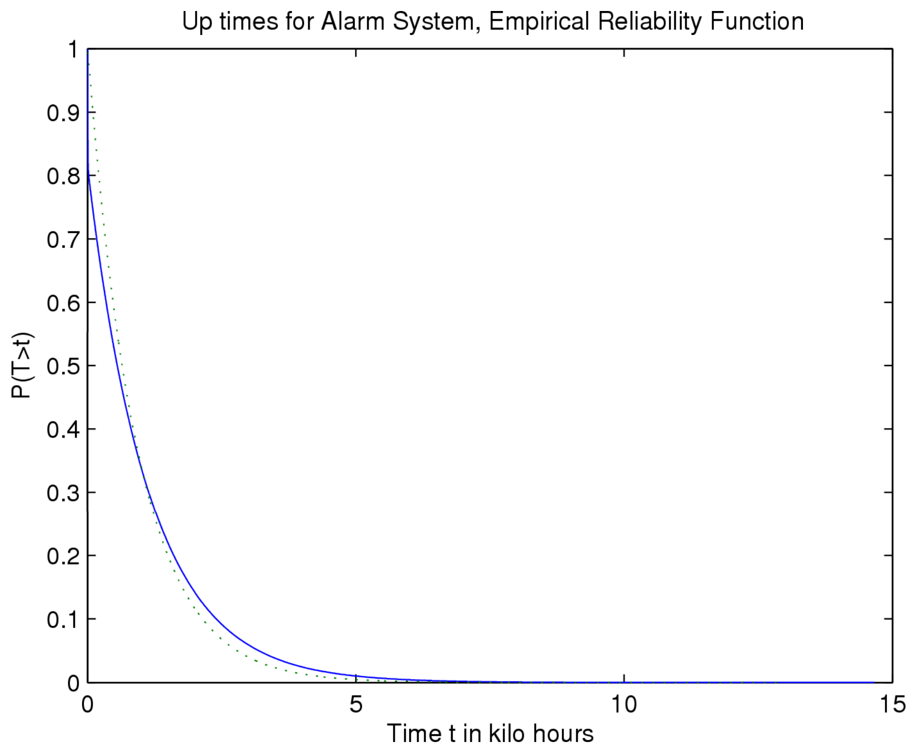


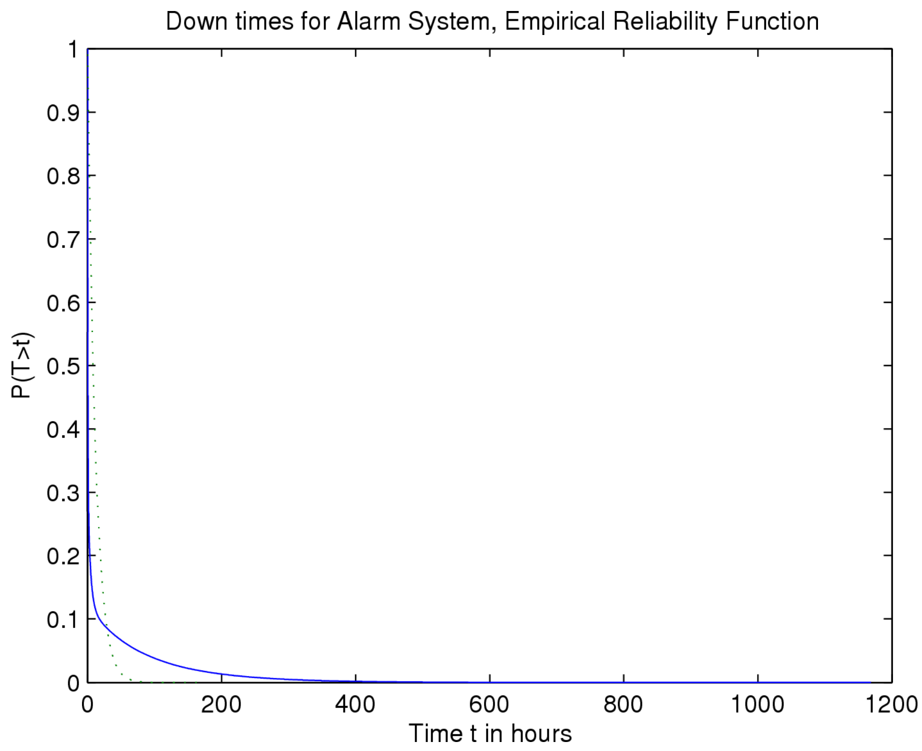
$10^3\lambda$	0.948	0.1	0.0296
$1/\mu$	1.19	100	50
$10^3 P(F)$	1.13	9.9	1.48

The complete Alarm System consist of a Power Supply, a Supervising Computer and a Detector Package.

Results for the Alarm System

	DFT calculations	Simulation		
		LCL	EST	UCL
$10^3 P(F)$	12.48	12.43	12.52	12.62
$10^3 \lambda$	1.078	1.074	1.076	1.079
$1/\mu$	11.72	11.69	11.78	11.87
$10^3 \lambda_{\mathrm{LS}}$	0.99		0.123	


Up times for Alarm System, Empirical Reliability Function
P(T>t)
Time t in kilo hours
0
5
10
15
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1


Down times for Alarm System, Empirical Reliability Function
P(T>t)
Time t in hours
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
200
400
600
800
1000
1200

Major conclusions

- The extended (dynamic) gate calculations can provide accurate values of both
  - the mean failure rate λ, and
  - the mean down time $1/\mu$

  at the top level.
- It is wrong to draw conclusions assuming that the rates λ and μ are constant at the top level of the tree.
- The technique allows for gate constructions that are not possible in standard fault trees.

Further comments

- Markovian assumption need not be correct.
- At least one of the gate output rates λ, μ is not Markovian.
- Still, they are assumed to be Markovian in the calculations at the next level.
- The thus induced error propagates through the levels of the tree.
- The parameter uncertainties are often gross.

References

- Bedford, T. and R. Cooke (2001). *Probabilistic Risk Analysis: Foundation and methods.* Cambridge.
- Lindhe, A., L. Rosén, T. Norberg, O. Bergstedt (2008). Integrated probabilistic risk analysis of a drinking-water system: A fault-tree analysis. Submitted to Water Research.
- Rausand, M. and A. Høјland (2004). *System Reliability Theory. Models, Statistical Methods, and Applications.* Wiley.

Plus two papers by Joanne Bechta Dugan *et al.* (1992, 2000) in IEEE Transactions on Reliability, which we have not yet read!