On Threshold Optimization in Fault Tolerant Systems

Jan Åslund, Erik Frisk, Fredrik Gustafsson

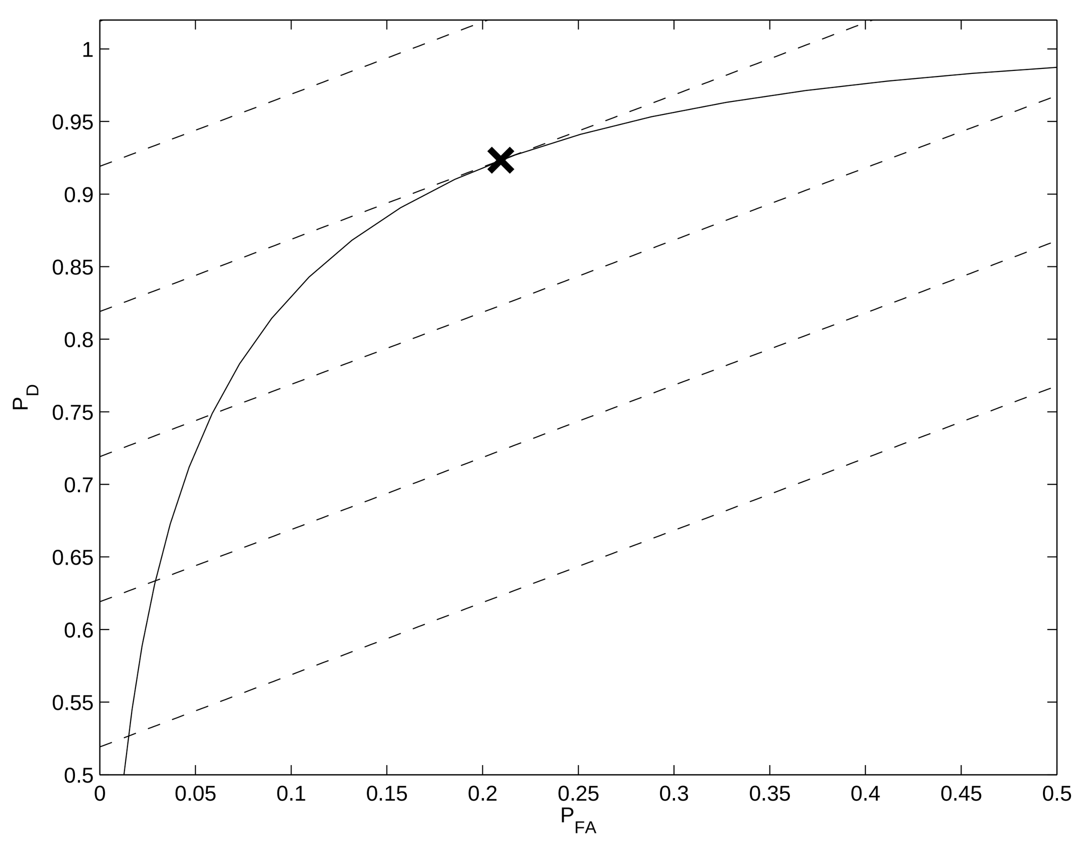
Mattias Krysander, Lars Nielsen

Introduction

Fault tolerant systems are considered, where a nominal system is monitored by a fault detection algorithm, and the nominal system is switched to a backup configuration in case of a detected fault. Conventional fault detection is in the classical setting a trade-off between detection probability and false alarm probability. To obtain a good compromise it is important to take into account performance of the diagnosis system, reliability of the components, and system configuration.

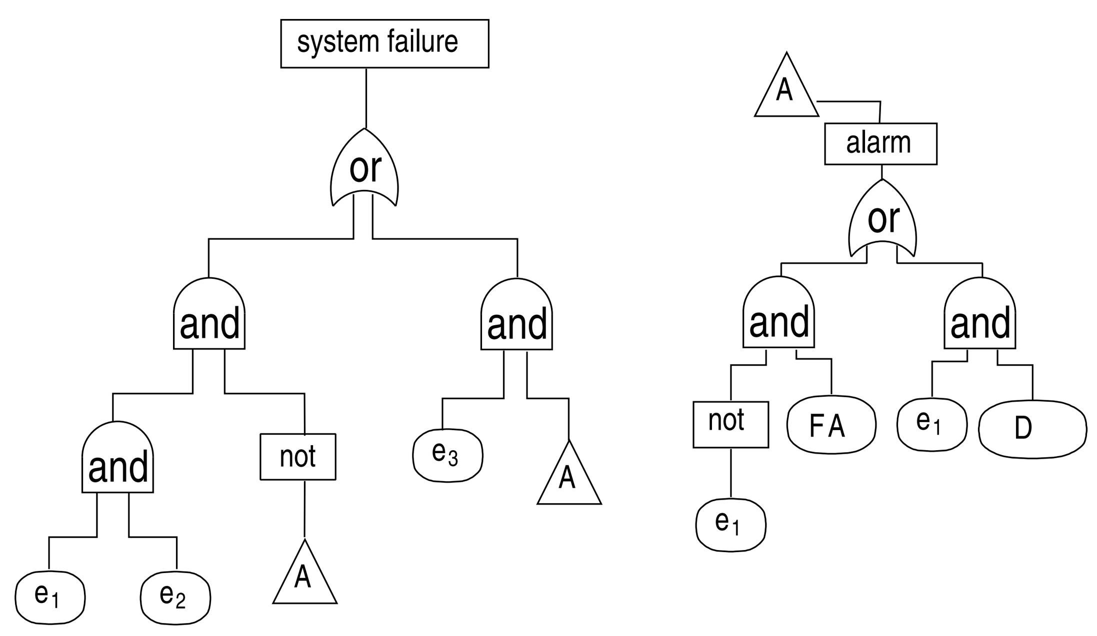
Diagnosis system performance

Performance of a fault detector can be visualized by plotting the probability of detection P_D against the probability of false alarm P_{FA}. The curve is parameterized by a detection threshold h. The solid line corresponds to an optimal maximum-likelihood detector for simple hypotheses.



Reliability and system configuration

A fault tree is used to model the interaction between diagnosis performance and component reliability in a system configuration. The figure below show an example of a fault tree.



The triangle A shows the logic for an alarm event where event e_1 corresponds to a failure in the supervised component. Events e_1 and e_2 correspond to failures of components in the nominal system and e_3 in a backup system.

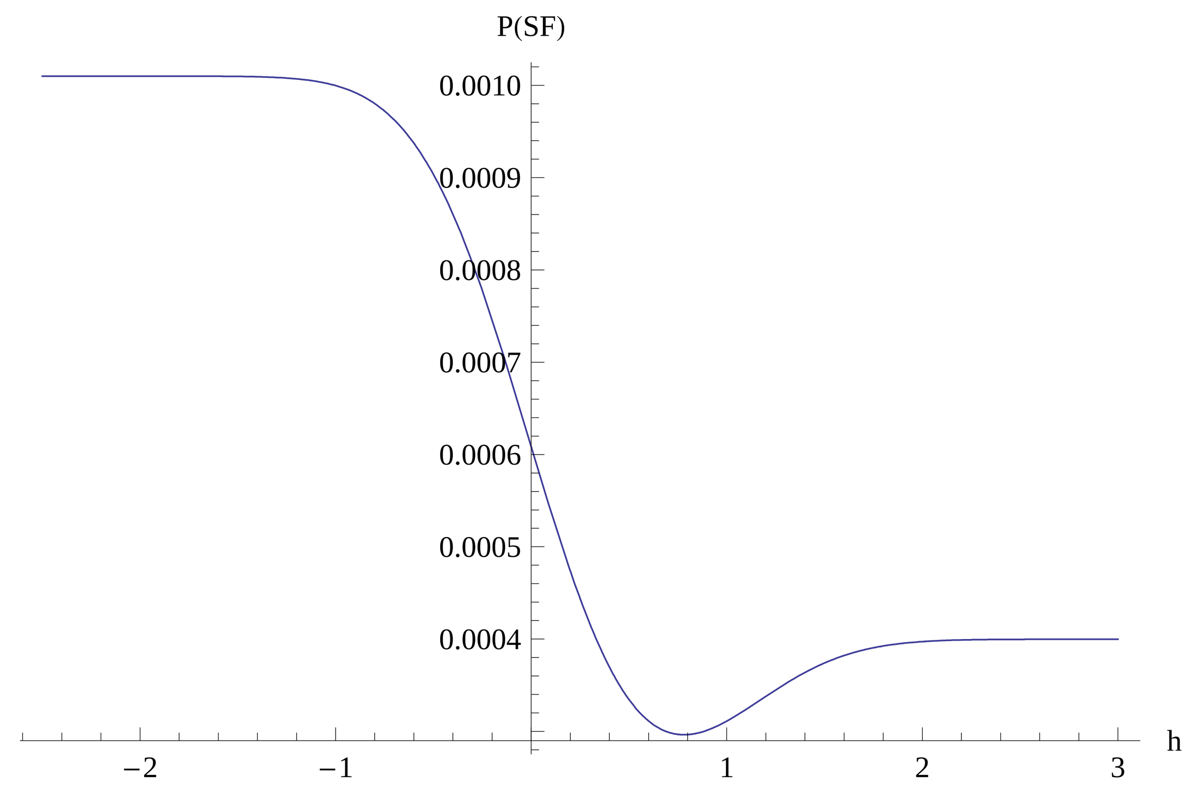
For any system described by a fault tree, the probability of system failure (SF) is given by an expression in the form:

$$P(\mathrm{SF}) = \alpha P_{FA} - \beta P_D + \gamma$$

where α, β, and γ are functions of component reliabilities and system configuration only.

Threshold optimization

The figure shows how the probability for system failure depends on the detection threshold h.



Minimizing this probability is equivalent to solving

$$\min_h \lambda P_{FA}(h) - P_D(h)$$

where the parameter $\lambda = \alpha/\beta$ includes all necessary information about the supervised system, the backup system, and the fault tolerant control strategy that is needed in the optimization problem.

Properties of the optimal solution

The dashed lines in the first figure are level lines of $P(SF)$. The gradient of the lines is equal to λ and it can be seen that the optimal detection threshold is given by the condition

$$\frac{dP_D}{dP_{FA}} = \lambda$$

In the figure, the optimal point is marked with an **x**.

For a one-sided test with simple hypothesis, an optimal test quantity is

$$T(y) = \frac{P(y|\mathrm{Fault})}{P(y|\mathrm{No\ Fault})}$$

With this test quantity the optimal threshold is equal to the parameter λ, i.e. the system should be switched to the backup configuration if $T(y) > \lambda$.

Further results

- Details on how component reliabilities and system configuration influence the parameter λ.
- Analysis of degenerate cases where the diagnosis system can not increase system reliability.

Results are published in:

[1] J. Åslund, J. Biteus, E. Frisk, M. Krysander, and L. Nielsen Safety analysis of autonomous systems by extended fault tree analysis nternational Journal of Adaptive Control and Signal Processing, 21(2-3):287–298, 2007.

[2] F. Gustafsson, J. Åslund, E. Frisk, M. Krysander, and L. Nielsen On Threshold Optimization in Fault tolerant Systems In *IFAC World Congress*, Korea, 2008.