

## FAULT TREE ANALYSIS AND FAILURE RATE CALCULATIONS IN MACHINERY

T. MALM<sup>1</sup>, J. HÉRARD<sup>2</sup>

<sup>1</sup> VTT Industrial Systems, P.O. Box 1307, FIN-33101 Tampere, Finland

<sup>2</sup> SP, P.O. Box 857, SE-501 15 Borås, Sweden

### Abstract

*Failure rates for a load-limiting device were calculated by using fault trees and 5 different component failure rate sources, 2 failure distribution sources and 4 calculation methods. The results were then compared. The results deviate from each other and reasons for deviation are reported. Also some common reasons for deviation of calculations are presented. One essential point in safety calculations is that if a specific information is not available for the calculation then a worst case scenario should be applied. There are several reasons why failure rate calculations of two systems may deviate and therefore it is important to use the same sources and calculation methods when comparing failure rates.*

### Introduction

The paper describes a comparison of failure rate (FR) calculations of dangerous failures for safety-related electrical control systems (SRECS) in machinery. The calculated FR covers only stochastic (random) hardware failures. The nature of common cause, design and software failures is such that their FR can only be estimated and they are neglected in this study.

This presentation is one result of a joint project between VTT Industrial Systems and SP. The Finnish part of the project was funded by The Finnish Work Environment Fund, VTT and the companies KCI, Sandvik Tamrock, Metso Minerals and Bronto Skylift. The Swedish part of the project was funded by VINNOVA and SP.

Qualitative safety analysis has often been considered to be adequate for SRECS in which the failure modes can be well defined. For complex systems, a quantitative analysis gives more confidence in the analysis. For example the standard IEC 61508 requires a quantitative approximation when the safety integrity level (SIL) for a system is specified. A large SRECS may include several subsystems and if the FR for the subsystems is known, then it is possible to calculate the complete FR. In the design phase it is recommended to allocate FR expectations to different parts of the system and calculate a so-called safety budget.

### Nature of the failure

The probability of a failure for components is a time dependant function and it resembles a so called bathtub curve. At first there may be some quality problems in the product and therefore the failure rate is high. This period lasts usually less than 1000 hours. The useful life period comes after this, and the failure rate stays constant. In many cases the failure rate tends to increase slightly with time, but this phenomenon is usually ignored. This is the failure rate value that is practical to use in equations, and one advantage is also that it is a constant. This period lasts often several years. The constant failure rate number does not show how long the component lasts, but it shows only how often the object fails per time unit at its middle age. In safety related systems the components are usually removed from use before the wear-out period during which the failure rate increases significantly. [4], [2]

MTTF or MTTF<sub>d</sub>, mean time to dangerous failure, (where <sub>d</sub> stands for dangerous) are constant failure rate values used in safety calculations. When the failure rate is constant then the relation between failure rate ( $\lambda$ ) and MTTF is:

$$\lambda = 1/MTTF \quad (1)$$

## Fault trees and reliability calculations

There are several ways to calculate the FR for the safety performance of SRECS. Fault tree analysis (FTA) was used in the project, but most of the aspects presented here are also applicable for other methods. The initial data related to component FR and failure distributions of failure modes are needed to make the calculations. After this partial probabilities in the fault tree can be calculated by using e.g. analytical equations, simulation or reliability functions with fixed probabilities.

Reliability function describes the probability that the object has succeeded in performing its task within a specific time. At start ( $t=0$ ) the value is 1 (=the object operates perfectly) and in the eternity the value is zero (the object has failed). The reliability function for a constant failure rate in exponential distribution is:

$$R(t) = e^{-\lambda t} \quad (2)$$

In the equation  $\lambda$  means failure rate (failures/hour) and  $t$  is time in hours. [2]

In these FTA calculations only OR- and AND-gates are considered. Here are some remarks for solving the equations.

For OR gate the total reliability is:

$$R(t)_{\text{tot}} = R_1(t) * R_2(t) * \dots * R_n(t) = e^{-\lambda_1 t} * e^{-\lambda_2 t} * \dots * e^{-\lambda_n t} = e^{-(\lambda_1 + \lambda_2 + \dots + \lambda_n) t} \Rightarrow \lambda_{\text{total}} = \lambda_1 + \lambda_2 + \dots + \lambda_n \quad (3)$$

In the equation  $R(t)_{\text{tot}}$  means the reliability in the output of the gate and  $R_1(t), R_2(t) \dots$  are the inputs to the gate,  $\lambda_1, \lambda_2, \dots, \lambda_n$  are failure rates at the input. [2]

The reliability function for AND gate is following:

$$R(t)_{\text{tot}} = 1 - (1 - R_1(t)) * (1 - R_2(t)) * \dots * (1 - R_n(t)) \quad (4)$$

If one combines equations (2) and (4) it can be seen that the result is a complex time-dependent function. The MTTF value can be estimated by integrating reliability function  $R(t)$  from zero to eternity. This gives an average value over all time. It is not possible to calculate reliability values during a specific time period by using the single MTTF value, because the failure rate is not a constant, but a time dependant function. [4]

$$MTTF = \int_0^{\infty} R(t) dt \quad (5)$$

By using equations (2) and (4) for calculating  $R(t)_{\text{tot}}$ , and integrating equation (5), and then finding the equivalent numerical series, the formula can be expressed also in the following way: [2]

$$MTTF_{\text{total}} = 1/\lambda_1 + 1/\lambda_2 + \dots + 1/\lambda_n - (1/(\lambda_1 + \lambda_2) + 1/(\lambda_1 + \lambda_n) + \dots + 1/(\lambda_{n-1} + \lambda_n)) + \dots + (-1)^{n-1} / (\sum \lambda_n) \quad (6)$$

Equations (4), (5) and (6) do not consider the cases of a failure occurring within a certain time period. In some cases the failure is revealed if the triggering faults do not happen in a specific critical order. In some cases the failures are revealed during a periodic test function or under normal operation. It is also possible that a failure is revealed immediately after it has occurred. All these cases result in a specific reliability function.

## Calculation plan

### CID description

CID is made for monitoring crane functions and to initiate some safety functions. The main function is to limit hoisting in a case of overload, but it also measures e.g. number of hoists, cumulative operation time, loads, supply voltage, motor temperature and possible wear out of brakes. Some of the inputs

can cause alarm for the driver and some can prevent hoisting. CID is constructed of computer-based technology and it consists of a lot of parameters, which must be set by the manufacturer.

### Tasks

This report is concentrating on one fault tree: Unexpected start-up in two-step control. Actually this covers the failure of a stop function. The calculations are made to compare different sources of failure rate values and to compare different methods in estimating the MTTF. Figure 1 shows the tasks that are used in making the FTA calculations.

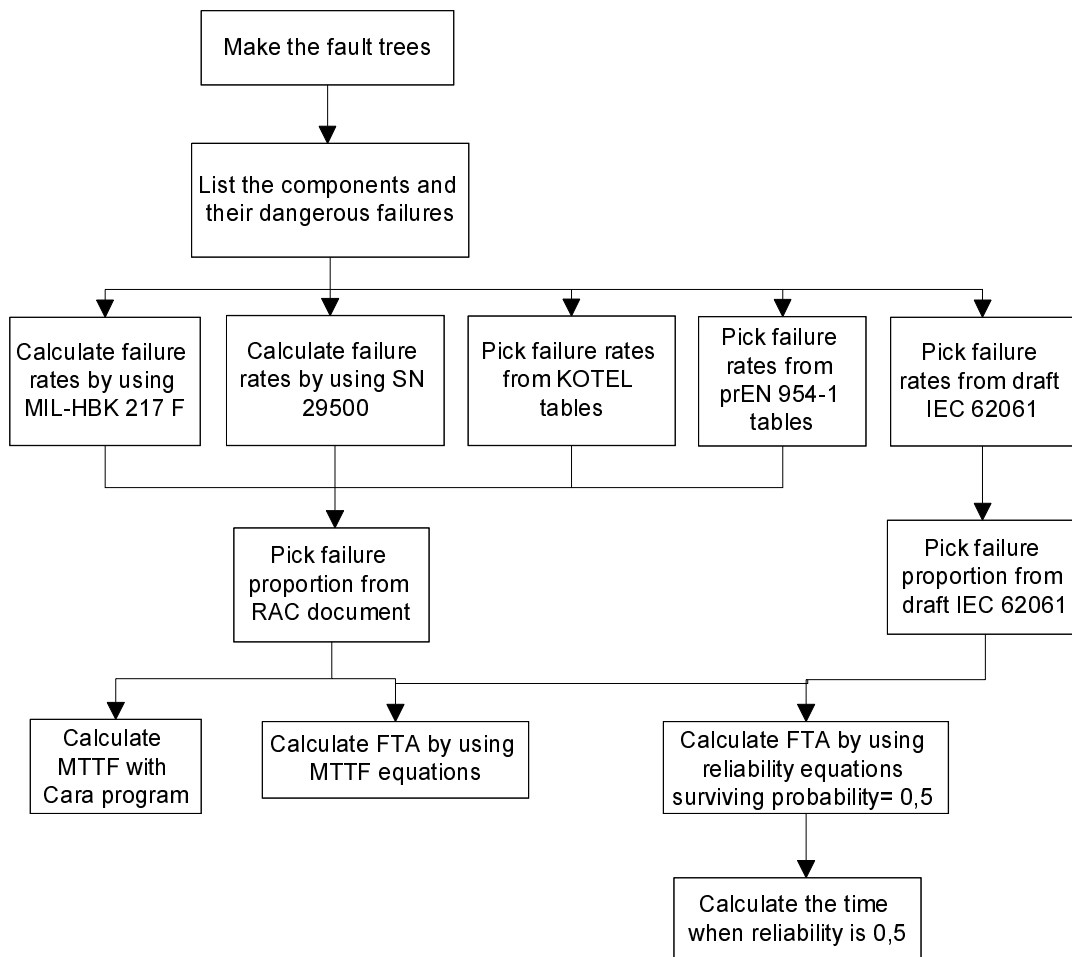


Figure 1. The tasks in calculating the FTA.

### Initial values

MTTF values are gathered from different sources and calculated separately in order to compare the differences in FTA results. The more specific values are calculated according to MIL-HBK 217F [6] and SN 29500 [9]. For these calculations some component and environmental values are needed. Such values are component type, component class, component temperature and component load. All these values are estimated according to general use in measurement circuits (not heavy use). However, in real applications the conditions may vary, and wrong environmental values in equations may cause over 100 fold results.

Experimental values are gathered from the KOTEL report. The component data has been collected between 1993 and 1995 from maintenance reports of two companies. The amount of service hours for each component type is something between  $10^8$  to  $10^{11}$  hours. The failure rate for each component type is calculated by using statistical methods and 60 % certainty factor. Therefore the calculated failure rate is never zero even if no failures were detected. [5]

Initial values are gathered also from standard drafts IEC 62061 and ISO 13849-1, which, however, were not complete at the time of calculation the calculation. In ISO 13849-1 there was no data for any integrated circuits and in IEC 62061 there was no data for processors [3], [7]. When no data was available for a certain component, the worst values related to other components were used. Therefore, the calculations related to the standards give only an approximation.

When the failure rate for each component is known, the dangerous failures are set forth by the FTA and the distribution related to any specific failure mode is gathered from the RAC document: Failure Mode/Mechanism Distributions. In IEC 62061 there is a data on the failure distribution. The initial values in the document are calculated by multiplying the constant hazard rate and the proportion value. Finally we obtain the failure rates for dangerous failures.

For integrated circuits it is difficult to estimate failure rates of dangerous failures since there are so many failure modes. In most cases, e.g. only one specific short circuit in a certain pin may initiate a hazardous situation. The component may have 112 pins and an enormous variety of failure modes. If data about failure rate covering all failure modes for the component were used the result per a single failure mode would be negligible. This would not be right since the complex integrated circuit has internal electronic switches, which have a fair failure rate ( $\neq 0$ ). Therefore the estimated distribution value for each failure mode related to any specific pin(s) is chosen so that e.g. the total (related to any pins) short circuit or open circuit distribution value of the component is used for all pin combinations in order to have reasonable values and to be on the safe side.

### Calculation results

A fault tree for an unexpected start-up was calculated by using four calculation methods and five different sources. Table 1 shows the calculation results. Here are some explanations to the table 1:

- MTTF calc.: Equations 1, 2, 3, 4 and 6 have been used to estimate the MTTF.
- Surviving prob. 0,5: MTTF is estimated by calculating the time when the reliability function value is 0,5.
- Cara MTTF: Cara is a commercial FTA program, which estimates the time for the first failure by simulating the fault tree. The used time period for calculation was  $10^{14}$ . The time was chosen so that it is clearly longer than MTTF for any component. Then several failures exist during the simulation period. The selected time period affects the results.
- Simplified FT: In this case there are only relays in the fault tree. This was made because in the fault tree the failures related to the relays play an essential role. The result gives the probability to critical relay failure. If the top event occurs the CPU can still operate and it detects the failure. The calculations are made according to "MTTF calc."

*Table 1. Results of calculations, which were performed by using different calculation methods and initial values.*

	Kotel (h)	SN 29500 (h)	MIL-HBK 217F (h)
MTTF calc.	$7,2 \cdot 10^9$	$4,3 \cdot 10^9$	$9,5 \cdot 10^8$
Surviving prob. 0,5	$5,6 \cdot 10^9$	$3,6 \cdot 10^9$	$7,3 \cdot 10^8$
Cara MTTF	$5,7 \cdot 10^9$	$3,2 \cdot 10^9$	$7,3 \cdot 10^8$
Simplified FT	$7,2 \cdot 10^9$	$2,9 \cdot 10^9$	$9,5 \cdot 10^8$

### Summary of calculation results

When comparing the data it was noticed that the most pessimistic data is provided by standard drafts IEC 62061 and ISO 13849-1. The results vary from  $10^{-6}$  to  $10^{-5}$ . However, neither of the databases was complete. Also some pessimistic assumptions were used to cover empty spots in the standards. Since the standards give initial values for safety-related calculations, the values need to be on the safe

side i.e. pessimistic. The second most pessimistic values are in MIL-HBK 217 followed by SN 29500. The most optimistic values are usually in the KOTEL database. According to literature the MIL-HBK 217F gives too pessimistic results [4], [5].

The calculations show that the input values have a determining effect on the final results. Therefore it is not possible to compare reliability or safety of two devices if the failure rate sources are different. SN 29500 and MIL HBK 217F need e.g. information about component type and operating condition information for calculations.

## Discussion

When making the quantitative analysis there are several sources of errors that increase the uncertainty of the results. Such sources of uncertainty are, among others, component data, estimated operational conditions, calculation model (FTA), calculation method (e.g. analytical equations or simulation) and finally the interpretation of the results. The analyser has to be careful when interpreting the calculated results. If the results are used to compare different systems then the used data, calculation methods and assumptions should be identical.

The results would be more comparable with the use of common methods and a common database. This is a goal for the future. In safety-critical applications the calculations need to be on the safe side. In other words one should always make a pessimistic approximation of the FR.

Reliability estimations can be related to the IEC 61508 standard. Then one must keep in mind that to reach a certain SIL level one must conform to all the requirements of the level, not only to the probability requirements of a hardware failure. When calculating the probability of dangerous failures per hour also factors like diagnostic coverage (DC) and common cause factor ( $\beta$ ) have to be considered.

Several factors cause uncertainty in the reliability calculations. Quite often the absolute values are not exact, but the values can well be compared to other values resulting from similar calculations. If the results are used only for comparison then many of the uncertainty factors are minimised. Table 2 shows the main factors affecting uncertainty in reliability estimations.

*Table 2 Factors which cause uncertainty in failure rate calculations. The factors are related to component failure rates, component failure distributions and system models.*

<b>Cause for uncertainty</b>	<b>Means to better results</b>
Component quality is not always the same. This causes deviation to the reality.	Quality problems are usual in the beginning. A trial period should last so long that all quality problems are detected.
Failure models are approximations of the real components.	Consider which data is most suitable or an experimental data should be used. Physics of failure method considers different failure mechanisms first separately. The method gives good results if the input data is accurate. [1]
How to treat electromechanical components, which age mainly according to switching number and load, not time.	Consider which data is most suitable. If the usage differs from general case it should be considered when choosing the failure rates for the components.
Components develop continuously and all models do not consider this. On the other hand, new components may have new failure mechanisms.	It is better to use an updated database in calculations. It is also possible to test the components and calculate the failure rate values from the test results.
If one uses data from different sources, the most pessimistic values dominate the results.	It is recommended to use the same source for all components. If this is not possible, the difference between the sources should be considered.
Most of the failure distribution data is not accurate. Failure mechanisms in different circumstances affect the failure modes and the models do not always consider this.	If the distribution proportion is not known and one wants to be on the safe side value 100% can be used. For some unusual failures also value 50% is commonly used.

<b>Cause for uncertainty</b>	<b>Means to better results</b>
It is difficult to estimate a failure distribution for integrated circuits, which may have complex critical failures (e.g. short circuit between certain pins).	To be on safe side the value for a general short circuit should be used for any short circuit in the integrated circuit. The same principles can be used also for other failure modes.
The environment of the system may be unpredictable	A worst case environment should be used in calculations to be on safe side.
The circuit architecture is usually not considered in the models.	Protective components, circuit layout and proper enclosure increase the life length of the system although they may increase the amount of components.
The fault tree or system model is simplified and this may cause errors	Check that the model covers the worst case situations.
The equations used for calculating failure rate for the complete system may have been different. MTTF may refer e.g. to simulation result to first critical failure, integral of reliability function from 0 to $\infty$ or certain reliability figure.	When comparing different systems the same calculation method should be used. E.g. in simulation process several parameters need to be defined. These definitions affect the results. [8]
Usually single figures are used to estimate the reliability of a system. However, the shape of the reliability function may differ from others and this may give a misleading result.	When comparing two systems consider also are the reliability function shapes similar. If the reliability function has a special shape, complete reliability functions may show more comparable results than single reliability figures (e.g. MTTF).
How to combine failure rates of sub-functions? The functions may depend on each other.	The failure rates of sub-systems need to be independent to have correct answers. If there are dependencies between summed failure rates, the result may be pessimistic.

## References

- [1] Alanen, J., Nevalainen, O., Palmén, H. Dependability of Electronics. Smart - Käke. Report VTT-AUT3 C-9907 January 2001.
- [2] Dhillon, B. & Singh, C. Engineering Reliability - New Techniques and Applications. A Wiley - Interscience publication. New York. 1981. 339 p.
- [3] draft IEC 62061. Safety of Machinery - Functional safety of electrical, electronic and programmable control systems for machinery. 44/380/CD 2002. 90 p.
- [4] Høyland, A. & Rausand, M. System Reliability Theory. John Wiley & Sons, Inc. New York. 1994. 518 p.
- [5] KOTEL 234. Failure rate of electronic components (In Finnish). KOTEL Ry. 1998. 17 p.
- [6] MIL-HBK 217F. Military Handbook - Reliability Prediction of Electronic Equipment. Department of Defence. Washington DC. 1991.
- [7] prEN ISO 13849-1:2002. Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO/DIS 13849-1:2002).
- [8] The Limitations of Using the MTTF as a Reliability Specification. Relia Software. Quarter 2 2000. Website: <http://www.reliasoft.com/newsletter/2Q2000/mttf.htm>.
- [9] SN 29500-1 Failure rates of components. Expected values, general. Siemens.