Calculating the "Probability of Failure on Demand" (PFD) of complex structures by means of Markov Models

Andreas Hildebrandt
Pepperl+Fuchs GmbH
Königsberger Allee 87

D-68307 Mannheim

Abstract - For the assessment of the "Safety Integrity Level" (SIL) in accordance with the standard EN 61508 it is among other things also necessary to calculate the "Probability of Failure on Demand" (PFD) of a safety related function. Thereto a set of equations is given in the standard mentioned above. If no appropriate formula is available, the calculation of the PFD can be done by means of a so called Markov Model. Especially for heterogeneous systems the Markov Model is an appropriate method to do the calculation of the PFD without the need of using a special formula.

To show how to define the various states of a Markov Model and how to derive the appropriate transition probabilities from given device specifications, the PFD of a one channel system is calculated by using a Markov Model. It is shown that the result of the Markov Model is in accordance with the formula given in standard EN 61508.

In a second step a Markov Model for a 1 out of 2 – System (1oo2) is presented. For multi channel systems the common cause failures have to be considered. It is shown that this leads to additional states in the Markov Model because the return to the initial state is different for common cause failures and failures of individual channels.

Finally several calculation results produced with the Markov Model mentioned above are compared with those derived from the formulas given in the standard. This is done by choosing the same failure rates for both channels so that the system becomes homogenous. For dangerous undetected failures (λ_{DU}) the results of the Markov Model are equal to those derived from the formula given in the standard. For dangerous detected failures (λ_{DD}) the results of the Markov Model are only half the values of the formula. This is due to a simplification of the formula which leads to an inaccuracy that is usually negligible.

Index Terms — EN 61508, PFD, Probability of Failure on Demand, Heterogeneous Structure, Homogenous Structure, Markov Model, Common Cause Failure, Dangerous Detected Failure, Dangerous Undetected Failure, 1oo2 – System, CARMS.

I. INTRODUCTION

For the assessment of the "Safety Integrity Level" (SIL) in accordance with the standard EN 61508 it is among other things also necessary to calculate the "Probability of Failure on Demand" (PFD) of a safety related function. Thereto a set of equations is given in the standard mentioned above. Depending on the structure of the safety related loop (single channel or multi channel with or without voting) one of these equations can be used.

Unfortunately some variants of structures are missing in the standard. In this case the calculation of the PFD can be done by means of a so called Markov Model. Especially for heterogeneous systems the Markov Model is an appropriate method to do the calculation of the PFD without the need of using a special formula.

Even though the understanding of a Markov Model is not very difficult in principle the definition of the various states and the corresponding transition probabilities can be a little bit tricky. Mainly the consideration of the common cause failures leads to additional difficulties and will be discussed in detail.

Within the scope of this paper a Markov Model for a heterogeneous 1 out of 2 – System is presented and the results of this model are compared with the results derived by a formula given in the EN 61508.

The following chapter will start with a one channel system to explain the handling of a Markov Model in principle. Later on a heterogeneous two channel system will be discussed.

Last but not least an example for a heterogeneous 1oo2 – system is presented.

II. CREATING A MARKOV MODEL FOR A SIMPLE ONE CHANNEL STRUCTURE (1OO1-SYSTEM)

For a one channel system the calculation of the PFD is usually not done by means of a Markov Model but with a formula given in the standard EN 61508. Nevertheless a one channel system is a good example to explain the application of a Markov Model. In addition the verification of the Markov Model is quite simple in this case because the formula of the 1oo1 – Structure is well understood and can be easily used as a benchmark.

Starting with a properly working system the first step is to determine the different kinds of failures which can happen. Depending on the failure, the system will move from the initial state to a different state. For a one channel system there are only two different kinds of failures possible:

1) *Detected Fault:* The fault will be detected by periodical diagnostic. After detecting the fault it takes the mean time to repair (MTTR) to restore the system. Due to the repair the system will go back to the initial state # 0.

2) *Undetected Fault:* The fault will be detected by the proof test. As long as no proof test is performed the system is down. Therefore the mean down time will be half the proof test time T_1 plus the mean time to repair MTTR if an undetected failure occurs (in other words, the mean down time is T_1 / 2 + MTTR). After repair the system goes back to the initial state #0.

The transition probability from the initial state (state #0) to the state #1 and state #2 is given by λ_{DD} and λ_{DU} respectively. The probability for the way back is the reciprocal of the mean down time. In case of a detected fault the mean down time is MTTR. For an undetected fault it is (T_1 / 2 + MTTR). This leads to the Markov Diagram shown in Figure 1.

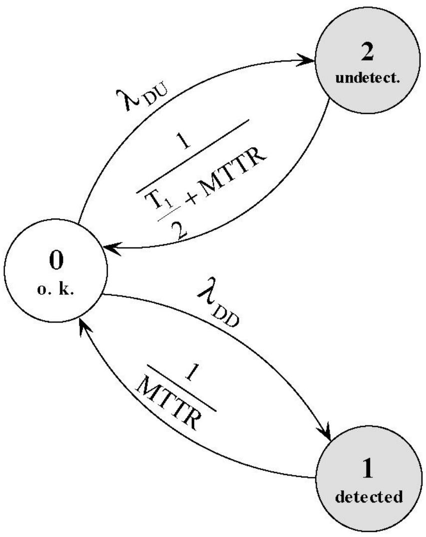


Fig. 1

The corresponding probability matrix is given as:

$$P_{1oo1} = \begin{bmatrix} 1-\lambda_{DD}-\lambda_{DU} & \lambda_{DD} & \lambda_{DU} \\ \frac{1}{MTTR} & 1-\frac{1}{MTTR} & 0 \\ \frac{1}{0.5\cdot T_1 + MTTR} & 0 & 1-\frac{1}{0.5\cdot T_1 + MTTR} \end{bmatrix}$$

Note: The sum of probabilities in each line must be one. Therefore the elements of the diagonal were calculated accordingly.

The steady state probability of each state can easily be calculated by matrix multiplication:

$$\vec{S}_\infty = \lim_{n\to\infty}\left[P^T_{1oo1}\right]^n \cdot \vec{S}_0$$

The evaluation of this formula is usually done with the help of an appropriate software tool like MATHCAD, MAPLE, CARMS [1] or something like this.

A different method to solve the Markov Model is a set of equations [2]. This leads to the following result for the steady state of the one channel system (1oo1) mentioned above:

$$PFD_{Markov} = \frac{\lambda_{DU}\cdot\left(\frac{T_1}{2}+MTTR\right)+\lambda_{DD}\cdot MTTR}{\lambda_{DU}\cdot\left(\frac{T_1}{2}+MTTR\right)+\lambda_{DD}\cdot MTTR+1}$$

If the numerator is significantly smaller than one the equation above passes over to:

$$PFD_{Markov} \approx \lambda_{DU}\cdot\left(\frac{T_1}{2}+MTTR\right)+\lambda_{DD}\cdot MTTR$$

In other words in case of low failure rates ($\lambda \cdot t << 1$) the result of the Markov Model turns into the equation given in the standard EN 61508.

III. CREATING A MARKOV MODEL FOR A HETEROGENOUS TWO CHANNEL STRUCTURE (1OO2-SYSTEM)

In case of a SIL 3 requirement it is often possible to use two SIL 2 devices in parallel. In order to minimize the probability for a so called common cause failure it is a good idea to use different kinds of devices for each channel. In this case the failure rates for channel #1 and channel #2 are different in general. Unfortunately there are no formulas for heterogeneous systems available up to now. Therefore the calculation of the PFD has to be done with the help of alternative methods. A commonly used method to calculate the PFD of complex structures is the Markov Model.

As mentioned above there is no need to do the calculation of the PFD for a one channel system by means of a Markov Model but this is going to change if the PFD of a multi channel system must be calculated. In case of a homogenous system there are still some formulas available as long as the number of channels is not too high. However for heterogeneous structures there are no formulas given in the standard IEC 61508 even if it is only a two channel system. Therefore the use of a Markov Model is advisable.

The evaluation of the appropriate Markov Model can be done analogous to the considerations described in chapter II. The main difference to a one channel system is the fact that for multi channel systems the so called "common cause failure" has to be taken into account. Moreover the Mean down time of the system in case of two independent undetected dangerous faults is no longer (T_1 / 2 + MTTR) but (T_1 / 3 + MTTR). For an undetected common cause failure the system behaves like a single channel system and as a result of this, the mean down time is (T_1 / 2 + MTTR) as ever. This leads to the Markov Diagram shown in Fig. 2 (for an enlarged figure see appendix A).

The corresponding probability matrix is given in Appendix B. The Markov Model for the heterogeneous system can also be used for a homogeneous structure by equating the failure rates from channel #1 with the failure rates of channel #2. In this case the results from the Markov Model are comparable to the results of the formula for the two channel system given in the standard EN 61508.

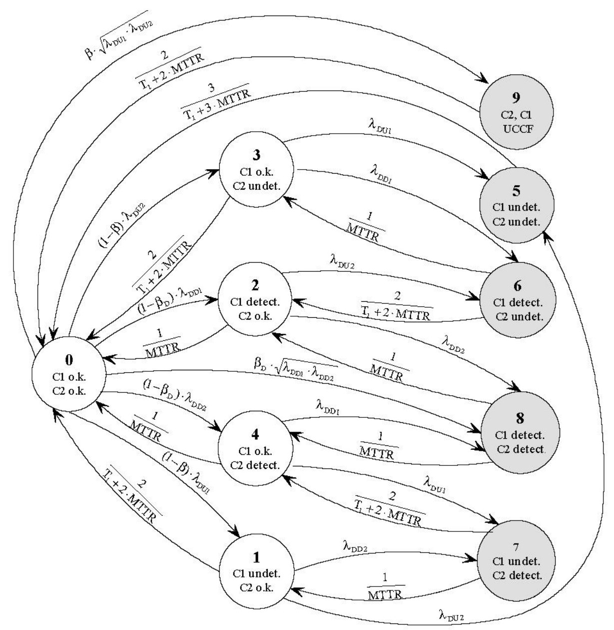


Fig. 2

IV. EXAMPLE: HETEROGENEOUS TWO CHANNEL LEVEL CONTROL SYSTEM

Assume a SIL 3 level control system with two different SIL 2 transmitters. The failure rates of the transmitter #1 and #2 are given as:

$\lambda_{DU1} = 2{\cdot}10^{-7}$ 1/h $\qquad \lambda_{DD1} = 7{\cdot}10^{-6}$ 1/h
$\lambda_{DU2} = 7{\cdot}10^{-9}$ 1/h $\qquad \lambda_{DD2} = 2{\cdot}10^{-5}$ 1/h

(Transmitter #2 has a good diagnostic coverage. Therefore the failure rate for the undetected faults becomes lower and the failure rate for the detected faults increases)

The factors β and β_D for the common cause failures are assumed to be 1% because the diversity is quite good due to the heterogeneous system design. The proof test interval T_1 is defined as 1 year and the mean time to repair MTTR as 8 hours. (Default value of the EN 61508)

Obviously the PFD of the system must be within the values for a homogeneous system built up with two identical transmitters of type #1 or type #2 respectively. That means it is quite easy to calculate the limit values for the best case and the worst case by using the formula for the homogeneous 1oo2 – system given in the standard EN 61508. For the example mentioned above the results are:

$$\mathrm{PFD}_{\mathrm{worstcase}} = 1{,}05 \cdot 10^{-5} \approx 1 \cdot 10^{-5}$$
$$\mathrm{PFD}_{\mathrm{bestcase}} = 1{,}97 \cdot 10^{-6} \approx 2 \cdot 10^{-6}$$

Remark: Due to a simplification in the formula given in the standard EN 61508 for the 1oo2 system, the influence of the detected failures on the PFD is twice as high as it is in reality. Therefore the calculated PFD is too pessimistic if the contribution of the detected failures to the PFD becomes substantial. From there the actual value for the PFD under best case condition is about $1.1{\cdot}10^{-6}$ which is approximately half the calculated value.

For the heterogeneous 1oo2 system the PFD calculated by means of the Markov – Model shown in Fig. 2 comes to:

$$\mathrm{PFD}_{\mathrm{heterogen}} = 5{,}26 \cdot 10^{-6} \approx 5 \cdot 10^{-6}$$

As expected this value is within the limits for the PFD given by the best case and worst case condition, that means:

$$\mathrm{PFD}_{\mathrm{bestcase}} < \mathrm{PFD}_{\mathrm{heterogen}} < \mathrm{PFD}_{\mathrm{worstcase}}$$

V. NOMENCLATURE

SIL	Safety integrity level.
SIF	Safety instrumented function.
SIS	Safety instrumented system.
SFF	Safe failure fraction
PFD	Probability of failure on demand
PDH	probability of dangerous failure per hour (1/h)
λ_S	failure rate of safe failures (1h)
λ_D	failure rate of dangerous failures (1h)
λ_{DD}	failure rate of detected dangerous failures (1h)
λ_{DU}	failure rate of undetected dangerous failures (1h)
t_{CE}	channel equivalent mean down time (h)
MTTR	mean time to restoration (h)
T1	proof-test interval (h)
β	fraction of undetected failures that have a common cause
β_D	fraction of detected failures that have a common cause
C1	Channel #1
C2	Channel #2
UCCF	undetected common cause failure

VI. REFERENCES

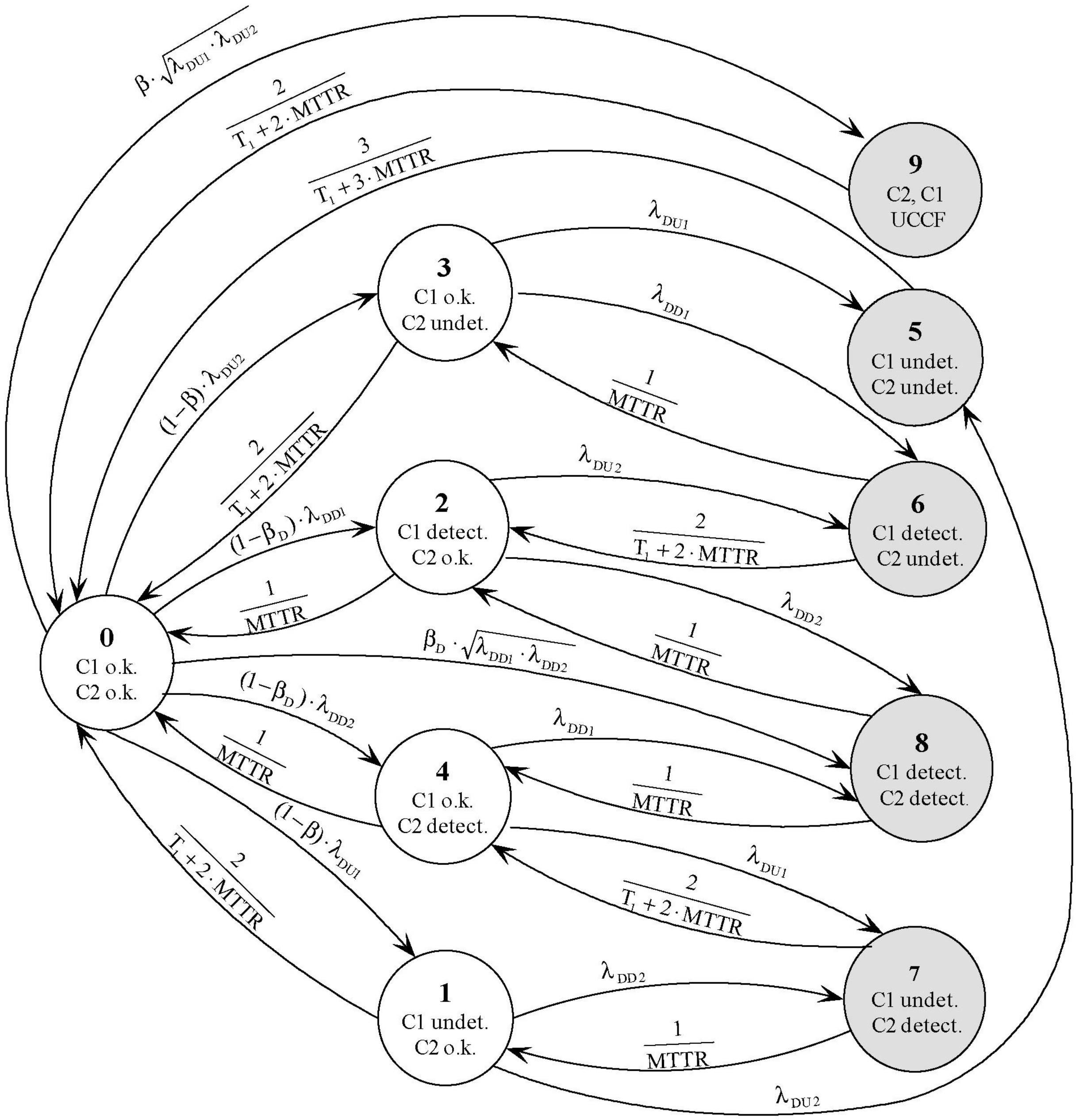
[1] Jan Pukite, Paul Pukite, “Modelling for Reliability Analysis”, IEEE Press, ISBN 0-7803-3482-5 http://umn.edu/~puk/carms.html

[2] William M. Goble, “Control Systems Safety Evaluation and Reliability”, ISBN 1-55617-636-8, www.isa.org

VI. VITA

The author graduated from University of Kaiserslautern, Germany in 1990 and gets the PhD Degree in 1996. Since then he is with Pepperl+Fuchs GmbH, Mannheim, first as a design engineer, later on head of the product release department and now leader of the department “training and committee work”. He is author of several previous papers and is a member of the DKE Standards subcommittee UK921.3 He is chairman of the ZVEI working group EMC.

Appendix A



Markov – Diagram for a heterogeneous 1oo2 system

Appendix B

$$P = \begin{pmatrix}
0 & (1-\beta)\lambda_{DU1} & (1-\beta_D)\lambda_{DD1} & (1-\beta)\lambda_{DU2} & (1-\beta_D)\lambda_{DD1} & 0 & 0 & 0 & \beta_D \cdot \sqrt{\lambda_{DD1} \cdot \lambda_{DD2}} & \beta \cdot \sqrt{\lambda_{DU1} \cdot \lambda_{DU2}} \\
\frac{2}{T_1 + 2 \cdot MTTR} & 0 & 0 & 0 & 0 & \lambda_{DU2} & 0 & \lambda_{DD2} & 0 & 0 \\
\frac{1}{MTTR} & 0 & 0 & 0 & 0 & 0 & \lambda_{DU2} & 0 & \lambda_{DD2} & 0 \\
\frac{2}{T_1 + 2 \cdot MTTR} & 0 & 0 & 0 & 0 & \lambda_{DU1} & \lambda_{DD1} & 0 & 0 & 0 \\
\frac{1}{MTTR} & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_{DU1} & \lambda_{DD1} & 0 \\
\frac{3}{T_1 + 3 \cdot MTTR} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \frac{2}{T_1 + 2 \cdot MTTR} & \frac{1}{MTTR} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \frac{1}{MTTR} & 0 & 0 & \frac{2}{T_1 + 2 \cdot MTTR} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \frac{1}{MTTR} & 0 & \frac{1}{MTTR} & 0 & 0 & 0 & 0 & 0 \\
\frac{2}{T_1 + 2 \cdot MTTR} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

Probability Matrix

Note: The sum of the probabilities in each line must be one. Therefore the elements of the diagonal have to be calculated accordingly (elements of the diagonal are still missing in the matrix above).
E. g. for row number k that means:

$$P_{k,k} = 1 - \sum_{i=0}^{9} P_{k,i}$$