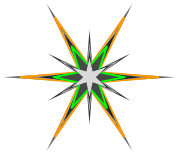


S T S A R C E S

Standards for Safety Related Complex Electronic Systems

Annex 6

Quantitative Analysis of Complex Electronic Systems using Fault Tree Analysis and Markov Modelling

Final Report of WP2.1

Michael Dorra & Dietmar Reinert

BIA
Berufsgenossenschaftliches
Institut für
Arbeitssicherheit

European Project STSARCES

Contract SMT 4CT97-2191

SUMMARY

The risk reduction provided by the operation of a safety system can be assessed in different manners. While EN 954-1 is using a qualitative scale of different categories IEC 61508 makes use of the Safety Integrity Level (SIL) as a quantitative measure. The latter is expressed by the probability of a dangerous failure of the safety related device. Thus a procedure is needed to take over the results of a qualitative analysis into a probabilistic evaluation. Markov models turned out to be the most appropriate tool because of their considerable capability of handling many of the technical features usually made use of by modern safety devices. Implementing a new feature enabled the models to reveal the interdependency of the online test rate, the rate of demands on the safety function and the Safety Integrity Level.

Markov models have been developed for several system arcitectures typical for the machinery sector. By altering the input data practical questions of interests can be answered concerning basic system design parameters such as diagnostic coverage (DC) or the need of a watchdog test. The evaluation results are able to demonstrate the influence of parameter variations and allow of a comparison between different system architectures.

The system architectures introduced in this report are proposed to be considered as "designated architectures" for the machinery sector. They can be assigned a category according to EN 954-1. The developed basic Markov models make it possible to draw a link between the categories of EN 954-1 and the Safety Integrity Levels of IEC 61508. It is not a fixed link because additional input information is needed beyond the category in order to determine the SIL. Arranged in a table some exemplary evaluation results may be used in order to simplify the SIL assessment in some cases. Whenever a manufacturer can prove that his system structure is in accordance with one of the designated architectures and that his quantitative parameters comply with the precalculated examples no new Markov modelling will be necessary.

Contents

Glossary

ASIC	Application specific integrated circuit
C	Diagnostic coverage (DC)
CAT	Category (according to EN 954-1)
CC	Current converter
CCF	Common cause factor (β)
CES	Complex electronic system
D	Drive
dang	dangerous
DC	Diagnostic coverage (C)
DCSC	Dual channel system with comparison
DCSMT	Dual channel system in mixed technology
E/E/PE	Electrical / electronic / programmable electronic
ES	Emergency stop (actuator)
EUC	Equipment under control
FTA	Fault tree analysis
IN	(Input of a) switch-off path of the drive
Ip, IP	(Input of the) switch-off path of the drive for the PED
Iw, IW	(Input of the) switch-off path of the drive for the watchdog
M	Motor
MTBD	Mean time between demands on the safety function
MTTF, $MTTF_d$	Mean time to dangerous failure
PDF	(Average) probability of a dangerous failure per hour
PED	Programmable electronic Device
PES	Programmable electronic safety related system
PFD	(Average) probability of failure on demand
PLC	Programmable logic controller
RC	Relay circuit
r_d	Demand rate on the safety function
r_r	Repair rate
r_t	Test rate
S	general sensor, rotation sensor
SCS	Single channel system
SCST	Single channel system with implemented tests
SIL	Safety integrity level (according to IEC 61508)
TCSC	Triple channel system with comparison
T_M	Mission time
T_r	Average repair time
T_t	Test interval
WD	Watchdog
β	Common cause factor (CCF)
λ	dangerous failure rate

1. Reasons for the need of reliability evaluations

1.1. Aims for the use of safety devices

The operation of many technical systems is involving risks of harm to people. The goal of the use of safety devices is to reduce these risks to an acceptable level. There is a wide range of various technical risk reducing measures. The investigations described in this report focus on complex programmable electronic safety related systems, commonly referred to as PES.

By providing one or more specified safety functions the safety device must make sure that a sufficient reduction of the risk is achieved whenever the equipment under control (EUC) is operated.

1.2. Contributions of the standards

One essential aspect in implementing a safety related system is considering the particular application in order to derive the needed risk reduction. A risk analysis has to be carried out for every potential hazardous event implied in operation of the EUC. Methods for obtaining the necessary risk reduction are presented in the standard IEC 61508-5 [1]

The other aspect is to ensure that the claimed risk reduction is actually attained by the safety device that will be applied. As a consequence the degree of risk reduction provided by a particular safety system has to be determined. The two standards EN 954-1 [2] and IEC 61508 [1] both are classifying electronic safety devices according to their respecting properties.

EN 954-1 [2] has chosen a qualitative approach by defining five categories (B, 1, 2, 3, 4) which differ in the reaction of the safety device after the occurrence of internal faults. Thereby requirements concerning technical realisation are established indirectly.

IEC 61508 [1] is distinguishing four different safety integrity levels (SIL 1 ... SIL 4) in order to provide a quantitative measure for grading a system's risk reducing capability. The latter is expressed by the probability of a dangerous failure of the safety related device.

Both standards describe technical means which can be implemented to improve the reliability of a safety related device. Said means include architectural measures, selection of appropriate system components, idle current principle, various kinds of online tests, etc.

It must be emphasised that these means are not intended to improve the availability of the equipment under control (EUC) being supervised by the safety device. In this context reliability signifies the probability of a safety device to be able to perform it's intended safety function(s).

Lists and descriptions of such techniques and measures can be found for example in EN 954-1 (chapter 5), EN 954-2 (to be published in 1999), IEC 61508-2 (annex A) and IEC 61508-7 (annex A).

As far as methods for fault detection are concerned, this is subject to the work of SP, Sweden (WP 2.2) [3].

1.3. The investigations of this report

Most of the reliability improvement techniques mentioned in the standards can be considered to be well-tried or at least well-known. Nobody will have any doubts that the implementation of these measures will improve the safety device's reliability, i.e. the probability of a safety device to be able to carry out the safety function(s) it has been developed for.

On the other hand it is difficult to assess quantitatively which degree of improvement is actually achieved by a particular feature implemented in a particular safety system. Moreover, in typical safety devices a junction of several technical means is found, for instance hardware redundancy in combination with a number of different component tests.

Therefore a mathematical tool is needed for evaluating reliability in order to find out which effect has been accomplished altogether.

The final goal of reliability evaluation techniques is to verify if a claimed safety integrity level (SIL) according to IEC 61508 [1] is actually met by a given complex electronic safety device.

This report will present the result of some basic investigations of simplified typical system architectures that can meet categories B, 1, 2, 3 and 4 according to EN 954-1 [2].

With this basic investigations it is possible to gain some information about the link between the categories of EN 954-1 [2] and the safety integrity level (SIL) according to IEC 61508 [1]. In parallel practical questions of interests concerning basic system design parameters such as self test rates, diagnostic coverage or the need of a watchdog test can be answered in respect of IEC 61508. Results of a quantitative reliability evaluation are able to demonstrate the influence of parameter variations and allow a comparison of different system architectures.

1.4. Fault tree analysis and Markov modelling

Besides Markov modelling reliability block diagrams and fault trees can be used for a quantitative analysis of a safety related system. The principle of a quantitative *fault tree analysis* (FTA) is described in [6] and, more detailed in [7].

However, for the evaluations presented in this document Markov modelling techniques [4], [5] have been chosen because of their considerable capability of handling many of the technical features usually implemented in modern safety devices. Especially periodic events like online tests can be modelled quite comfortably.

Nevertheless a *qualitative* fault tree analysis may be useful in connection with a Markov model. This will be demonstrated in chapter 7.2.

2. Short introduction to Markov modelling with respect of safety related systems

2.1. General

Markov models [4] are an efficient tool for evaluating the probability of the occurrence of states in which a system can dwell while a process is running. In principle this modelling technique is applicable to any type of process (e.g. biological, chemical or physical processes) as long as it meets certain requirements.

Concerning safety related devices, the considered system is given by the hardware of the device and the process is represented by the failures of the system's components, by online tests, system repair and demand on the safety function. All this is considered during the entire mission time T_M of the safety system, where "T_M" means a declared span of time during which the system is permitted to be used for safety related applications. The desired result of the Markov model application in this case is the probability of a dangerous failure of the system.

The Markov approach requires that a set of system states is established which covers any single state that might occur during the time under consideration. Furthermore, these states have to be mutual exclusive, i.e. at any time a particular sample of the device must be assignable to exactly one of the states.

Passing over from one state to another is described by transition probability. It is important to note that transition probability is always related to a specified time interval Δt. The complete set of all possible transitions is represented by a set of transition probabilities in connection with adjoined source and drain states. Together with the definitions of the states this information is sufficient to establish the Markov model.

Δt must be the same for all transition probabilities within the model. Since Δt affects the value of every single transition probability it must be chosen small enough in order to ensure that the sum of all transition probabilities exiting from any of the states is smaller than one. This is because probability by definition cannot exceed the value of one. Δt could be designated as the "time base" of the calculation.

The usual graphic manifestation of the model consists of a circle (or "bubble") for each state and connective arcs for the possible transitions. The circles are labelled by the names of the states (often abbreviations for descriptions of the states) and/or a number whereas the arcs are labelled by the pertinent transition probabilities.

Markov modelling implies that all transitions only depend on the transition probabilities and the present state probabilities and not on what has happened in the past. Therefore such a model is sometimes called "memoryless". Irrespective of the fact that a complex electronic system usually contains memory Markov modelling techniques can be applied because normally the memory contents has no influence on component failures.

2.2. Modelling random failures of components with constant failure rates

Mostly component failure rates can be assumed to be constant over time. This is usually correct if

- the mission time ends before the beginning of the wear-out area,
- additional early failures can be neglected or are eliminated by burn-in,
- the component itself does not contain any redundancy.

Then the transition probability due to random failures is given by

$$p_f = \lambda \cdot \Delta t ,$$

where λ is the failure rate and Δt is the time interval the transition probability is related to.

The Markov model for this simple failure process is shown in Figure 1.

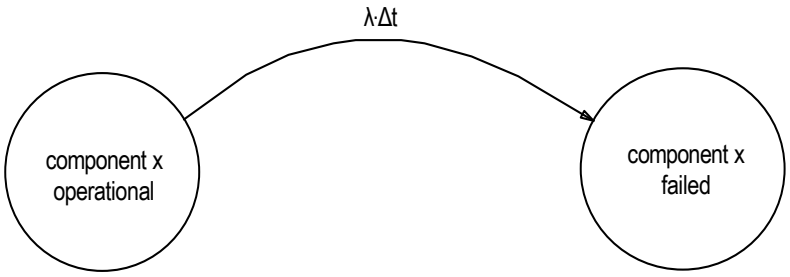


Figure 1: Failure of a component with constant failure rate

It is important to point out that our scope implies only *dangerous failures* of components or systems to be considered. When a dangerous failure of a component occurs, in many cases this will not cause a dangerous system failure, due to the system's inherent fail safe capability. However a component failure is said to be dangerous if the component thereby is no longer able to perform a subfunction which helps the system to carry out it's intended safety function, even if the safety function is maintained by other (redundant) system components.

Failures which only affect the availability of the process under control are out of the scope of this document's investigations.

2.3. Modelling common cause failures

Failures of components due to the same cause are called *common cause failures*. They can form a severe problem for safety systems using homogenous redundancy. In bibliography this item is also dealt with using the term *common mode faults* [6]. These effects can be taken account of in a Markov model by applying the so-called beta model. This model assumes that a fraction β of the failure rate affects all components of same type at the same time. β is a value between zero and one, usually much lower than 0.1. The residual fraction (1-β) must still be applied to each of the redundant components. Figure 2 demonstrates the Markov implementation for two redundant components or subsystems.

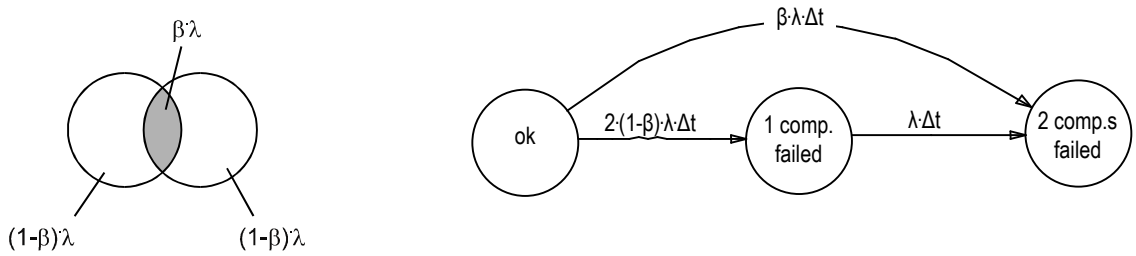


Figure 2: Markov representation of dual redundancy with common cause effect

In case of three redundant components the modelling technique must be extended. A decision has to be made whether the common cause always forces all three components to fail (simple β factor model of Figure 3) or whether it produces a certain fraction of dual failures as well (multiple greek factor model of Figure 3). In the latter case a new parameter γ would have to be introduced in order to determine the ratio between dual and triple failures. This ratio depends on the distribution

function of the stress which is causing the failures and on the distribution function of the component susceptibility towards the stress. For the most part these data will not be available.

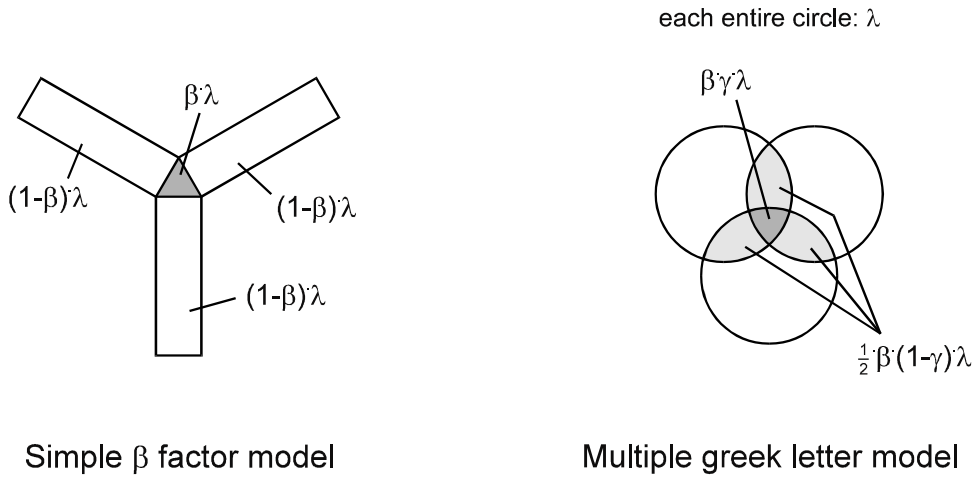


Figure 3: Models for failure rate stream partitioning for triple redundancy common cause failures

Therefore the simple β model is chosen as a worst case estimation for the common cause effect of a triple redundancy. This model applies exactly if the components show a sharp threshold of susceptibility towards stress. Figure 4 depicts the Markov implementation of this model.

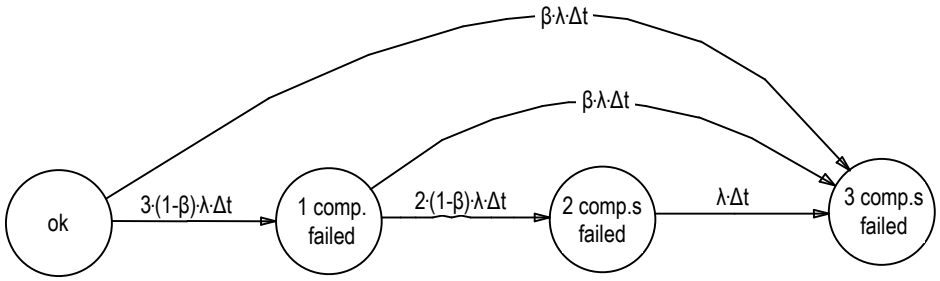


Figure 4: Markov representation of triple redundancy with common cause effect (simple β factor model)

It is important to apply the modelling techniques described above to any of the model states where two or more components of same type are still operational.

2.4. Modelling online tests

If a particular component of a system is periodically tested by means of an automatic system self test, it is spoken of an *online test*.

Usually online tests are not performed continuously but only at certain points of time, fixed by the test rate r_t. In addition, some tests are considerably time consuming, e.g. tests of large memories. Hence the test duration establishes an upper limit for the test rate and in some cases may result in a

rise of the hardware costs if the test has to be carried out very often. For that reason the test rate is an important design parameter not least in the manufacturer's view.

Therefore the Markov models presented in this document take account on the span of time which is needed for the detection of internal component failures (so far as provided by the system in question).

The time interval between two consecutive tests is named the *test interval* T_t. The probability that a test is carried out during the time interval ("time base") Δt is given by

$$p_t = \frac{\Delta t}{T_t} = r_t \cdot \Delta t, \qquad \text{where} \qquad r_t = \frac{1}{T_t} \qquad \text{is called the } \textit{test rate}.$$

The test can be either successful or not. There is a probability to detect a failure under the condition that a failure has occurred before. This *conditional probability* is called the *diagnostic coverage C* (or diagnostic coverage factor *DC*). *C* is a measure for the quality of a test. Therefore the probability that the test takes place is divided into two fractions:

The (transitional) probability that the test is able to detect the failure within the time interval Δt is

$$p_d = C \cdot r_t \cdot \Delta t,$$

whereas the probability that the test will not be successful during Δt is given by

$$p_u = (1 - C) \cdot r_t \cdot \Delta t.$$

If a test has failed to detect a component failure due to it's limited diagnostic coverage it is assumed that this test will not detect the failure even if it is repeated (deterministic test model). The Markov representation of this test process is shown in Figure 5.

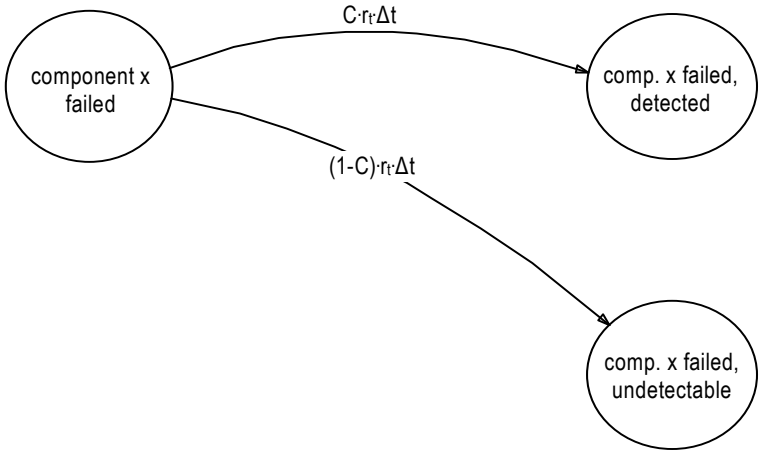


Figure 5: Online test of a component

The left circle in Figure 5 is depicting an intermediate state with the component x failed while the online test has not yet been carried out. Additional component failures may occur in all three states of Figure 5.

Detection of a component failure implies that there are still other components operational which can carry out an appropriate safety oriented action. Consequently each state must be checked carefully in order to determine which online test is executable actually.

2.5. Modelling demand

IEC 61508 distinguishes Safety Integrity Levels (SILs) for safety-related being employed in

- low demand mode of operation
- high demand mode of operation and
- continuous mode of operation.

In order to determine the SIL for the first two modes of operation the demand on the safety function has to be modelled. A demand will lead to a hazardous situation if the safety-related system is in a "dangerous" state which is the case whenever it is not able to fulfil it's intended safety function. This is taken account of in the model by introducing transition arcs for the demand leading from any dangerous state to a common "hazard state".

The circle on the left side of Figure 5 is representing an intermediate state where component x has failed but the online test has not yet been executed. If this state is "dangerous", it is contributing to the system's overall probability of dwelling in a dangerous state and, consequently, a "demand arc" must exit from the intermediate state. Then the probability of the intermediate state does not only depend on the failure rate of component x but also on the test rates and the demand rate. Therefore these two rates have an influence on the overall probability of the system to behave dangerous and on the SIL which is calculated from this probability (see chapter 3). Naturally test rate and demand rate are also affecting the number of hazardous events within the mission time of the safety system since a demand can hit the system in an intermediate state before an online test has taken place. These effects are clearly demonstrated in chapters 1.1 and 6.3.

By regarding the test rates as well as the demand rate this type of Markov model is able to simulate precisely the influence of both rates on the SIL and helps to answer the question which test rate is necessary.

The transition probability for a demand is given by

$$p_{demand} = r_d \cdot \Delta t \,.$$

For the continuous mode of operation there are continuous demands so that the potentially dangerous states are hazardous. The demand does not have to be modelled for these systems. Chapter 3 will describe how to achieve the SIL for the three different modes of operation.

2.6. Modelling repair

When a failure has been detected successfully the safety related system will carry out a predetermined action. Usually the same will happen as if the operational safety device would perform it's intended safety function: the process which is controlled by the device will be shut down to ensure a non-volatile safe behaviour.

Naturally, in this case shutdown is not a reaction due to an external hazardous situation but is used as an indicator to signalise the need of a repair. Furthermore, for machinery safety related systems it

is assumed that process operation will be prevented until the safety related device has been repaired or replaced. We also postulate no online repair capability to be provided so far.

Assuming an average repair time T_r, the (transition) probability that a repair will take place during the time interval Δt is given by

$$p_r = \frac{\Delta t}{T_r} = r_r \cdot \Delta t \,, \qquad \text{where} \qquad r_r = \frac{1}{T_r} \qquad \text{is referred to as the } \textit{repair rate}.$$

After repair (or replacement) system and process operation will be continued. Figure 6 presents the corresponding Markov diagram.

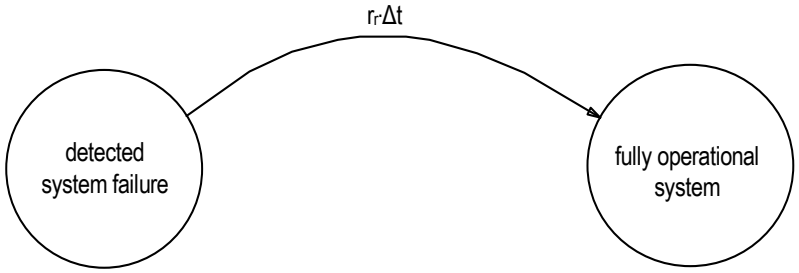


Figure 6: Repair of the system

Usually the assumption is made that a repaired system is as good as a new one. Actually the safety device has only been renewed in parts. Nevertheless this is a reasonable simplification as long as none of the system's components is drawing up to it's wear-out area during the residual mission time of the system.

2.7. Evaluation of a Markov model

The original method for evaluation of a given Markov model consists in deriving a complete set of differential equations from the model and solving for the desired state probabilities as continuous functions of time. This is a difficult and time-consuming job since the number of differential equations is equal to the number of model states. Thus this method is suitable only for small models with a few states.

Fortunately a numerical solution can also be obtained if a time discrete solution is accepted. This method requires the entire set of transition probabilities to be arranged into the template of a *transition matrix*. Since either of the transition probabilities in the matrix is related to the same time interval Δt, the transition matrix P itself is related to that interval as well.

In general the transition matrix P for a Markov model comprising n states consists of n rows and n columns. It is given by

$$P = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & & \vdots \\ p_{n1} & \cdots & p_{nn} \end{pmatrix},$$

with p_{ij} being the transition probability of a transition from state *i* to state *j* during the time interval Δt. If no transition from state *i* to state *j* is possible (i.e. if there is no transition arc), the corresponding transition probability p_{ij} in the *P*-matrix is set to zero.

The matrix elements of the diagonal represent the probabilities that there will be a transition from a particular state to that state itself, i.e. p_{ii} is the probability that the system will not leave state *i* during the time interval Δt.

The transition probabilities of each row in the matrix must sum to one, because it is sure that any transition will take place during. Δt, the "transitions" from states to themselves included. Thus the matrix elements of the diagonal can be calculated:

$$p_{ii} = 1 - \left(\sum_{j=1}^{i-1} p_{ij} + \sum_{j=i+1}^{n} p_{ij} \right)$$ (*n* is the number of model states.)

At any time the complete set of all state probabilities can be compiled by forming the *state probability row matrix S*, which is defined by

$S = (s_1 \; \cdots \; s_n)$, where s_i is the state probability of state *i*.

The elements of *S* must also sum to one, for it is secured that at any time the system must be in either of the states.

If S_t is the state probability row matrix at the point of time t, the state probability row matrix for $t+\Delta t$ can be calculated by using the transition matrix *P* related to the time interval Δt:

$$S_{t+\Delta t} = S_t \cdot P$$

By using this formula *n* times recursively, the state probability matrix $S_{t+n\cdot\Delta t}$ for the point of time $t+n\cdot\Delta t$ is obtained. Every single multiplication of the state probability matrix by the transition matrix P causes the state probabilities to proceed by a time step of Δt. Therefore a time step of $n\cdot\Delta t$ can directly be done by using the transition matrix that is raised to the power of *n*:

$$S_{t+n\cdot\Delta t} = S_t \cdot P^n$$

Making use of one or both of these two equations it is possible to calculate any state probability desired at any time which is equal to a multiple time step of Δt.

Usually the procedure is started with a state probability row matrix that has the form

$S_0 = (1 \; 0 \; \cdots \; 0)$.

This implies the assumption that at the beginning (time zero) the system's probability of being in state No. 1 is 100% whereas the probability to be in any of the other states is equal to zero. For instance, state 1 could represent a completely operational safety related system. All the other states symbolise system conditions where one or more components have failed.

After having executed the desired number of matrix multiplications there will be found a new distribution of probabilities related to the time step that has been made. Some components will have failed during the this time step. This results in a probability of state 1 which is smaller than 1 (or 100%) while the other probabilities have increased.

Some of the states represent a dangerous failure of the entire system. The probabilities of the latter states must be added to obtain the total probability of dangerous failure of the system for the pertinent point of time.

Usually the calculations are automated by computer software, either regular spreadsheet programs, specific Markov model software or universal mathematical software. BIA makes use of the windows-based programs MS Excel (the well-known spreadsheet program) and Carms [8] (a specific Markov modelling program). It has been testet by spot-checks that both programs deliver the same results.

2.8. Techniques for reducing the number of Markov states needed

In principle the Markov method requires every possible combination of component failures to be taken account of by a state of it's own. This is due to the fact that random failures will occur in an accidental chronological order. For instance, a system comprising only 10 components will show $2^{10} = 1024$ different failure combinations if each component is either operational or defective. Such a great number of states is hard to handle. Fortunately there are some techniques which can be applied in order to reduce the number of states needed:

1. Combining all "dangerous" states where *definitively* no online test will be effective any longer. It must be taken notice of the fact that there might exist some states with no effective online test but a test will become active after the occurrence of additional component failures. A state of this kind must not be put into the collection.

2. Symmetric architectures providing homogenous redundancy allow to unite model states which show the same system behaviour *as a consequence of the symmetric arrangement of the failed components*. Generally, different states must not be united only because they lead to uniform system behaviour.

3. The model development can normally be terminated if all combinations with a certain number of failures have been covered. For example, if every possible combination of four component failures has been regarded by particular states, it may be adequate to unite all states with five or more failures. Reason: the more failures are needed for arriving at a definite state the less will be the probability of that state. Executing the calculation once with the collective state assumed to be "dangerous" and once with the assumption that the system is operational in that state will show whether the accuracy of the simplified model is sufficient.

All three techniques have been applied to the Markov model of the homogenous triple channel system described in chapter 8. It consists of 9 components with 512 potential failure combinations, but the number of model states has been cut down to 91, including additional states for proper handling of the online tests.

3. Determination of the Safety Integrity Level according to IEC 61508 for the different modes of operation

IEC 61508-1 [1] defines in its tables 2 and 3 two target failure measures for a safety function as Safety Integrity Levels (SILs): Table 2 is allocated to an E/E/PE safety-related system operating in low demand mode of operation whilst table 3 is related to an E/E/PE safety-related system operating in high demand or continuous mode of operation. The target failure measure for low demand mode is given by the average probability of failure to perform its designed function on demand (PFD) whereas the measure for high demand or continuous mode is given by the (average)

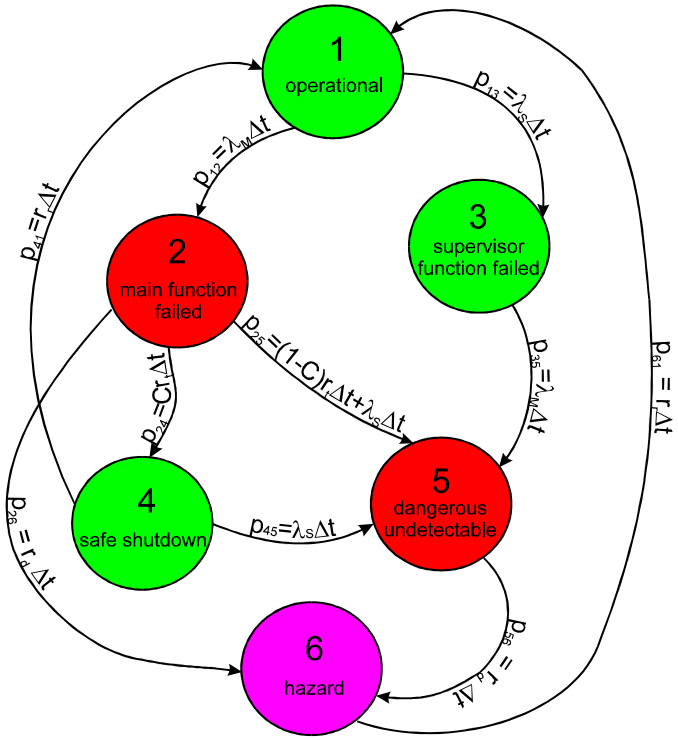
probability of a dangerous failure per hour (PDF). These definitions imply the demand on the safety function to be taken into account when the SIL of a particular system shall be ascertained. As a consequence the state “hazard” needs to be introduced into the Markov model. The term “hazard” must carefully be distinguished from the term “accident”, because in this context “hazard” means the coincidence of a dangerous system failure and a demand on the safety function, which will not necessarily lead to an accident. In the following it will be shown by using a simple example how to determine the SIL for the three different modes of operation: low demand mode, high demand mode and continuous mode of operation.

Figure 7 shows the Markov model of a safety system with a single channel for the main safety function and an additional supervision device. The supervisor function can detect a certain part of the failures in the main system and can shut down the machine (EUC) to a safe state (state 4). All undetectable failures will lead to a dangerous undetectable state (state 5). There is a probability that the supervision device has failed first and consecutively the main system fails also. This will lead to state 5 too. When the main function has failed (state 2) a demand will lead to the hazard state as long as this failure is not detected. The same is the case if there is a demand in state 5. If only the supervisor has failed (state 3) the system can still perform its designed safety function.

For low and high demand mode of operation the same Markov model is applicable, but the SIL is determined in two different ways: The PFD (probability of failure on demand) which delivers the value for the SIL table for low demand mode of operation (table 2 of IEC 61508-1) is calculated by:

$$PFD = 1/T_M \int_0^{T_M} [p_2(t) + p_5(t)]dt$$

As said before states 2 and 5 together present the probabilities of a hazard in case of the occurrence of a demand. The SIL is obtained from the average probability. Therefore the sum of these two probabilities must be integrated over and subsequently divided by the mission time T_M.



λ_M: Failure rate main system

λ_S: Failure rate supervision device

r_t: Test rate

r_d: Demand rate

r_r: Repair rate

C: Diagnostic coverage

Δt: Markov time step

Figure 7: Markov model for determining the SIL

The PDF (probability of a dangerous failure per hour) which is needed for the SIL in case of high demand mode of operation (table 3 of IEC 61508-1) is calculated by:

$$PDF = r_d / T_M \int_0^{T_M} [p_2(t) + p_5(t)]dt$$

As said before states 2 and 5 give the probabilities for a hazard in case that a demand occurs. To get the average probability of a dangerous failure per hour we have to calculate the average flow from states 2 and 5 to state 6. This is the average probability of the two states multiplied by the demand rate.

For continuous demand mode systems states 2 and 5 are directly hazardous because the demand is present continuously. State 6 and all arcs connected with state 6 must be removed from the model. Two new repair arcs must be added. The first one points from state 2 to state 1 and the second one from state 5 to state 1. In this simple example the safe shutdown (state 4) can only be reached after the occurrence of a hazard. This means that in practice, this simple system architecture is not suitable for continuous mode of operation. However the principle of model evaluation for continuous mode can be demonstrated.

Calculating the SIL in this case requires to determine the average flow into these hazardous states 2 and 5:

$$PDF = \lambda_M / T_M \int_0^{T_M} [p_1(t) + p_3(t)]dt$$

Again, the obtained value is used for table 3 of IEC 61508-1.

During the calculations it could be shown, that the same hardware is achieving the same SIL, independently from its use in high or low demand mode of operation. It could also be shown that the PDF for continuous mode of operation equals the PDF for high demand mode operations with a very high demand rate. Both results are plausible.

4. Single channel system without fault detection in accordance with category B or 1 of EN 954-1

4.1. Description

The categories B or 1 according to EN 954-1 [2] imply that the system does not provide any capability of detecting internal faults. For category 1 not only basic but well-tried safety principles and components must be used, which means that a higher reliability is achieved and therefore the probability of a system failure is lower than in category B (see EN 954-1, 6.22).

If we assume the system comprising a sensor (S), a programmable electronic device (PED) with integrated power supply for signal evaluation and a drive (D) that is controlled by the PED it can be represented in a block diagram by a simple series system. This is shown in Figure 8.

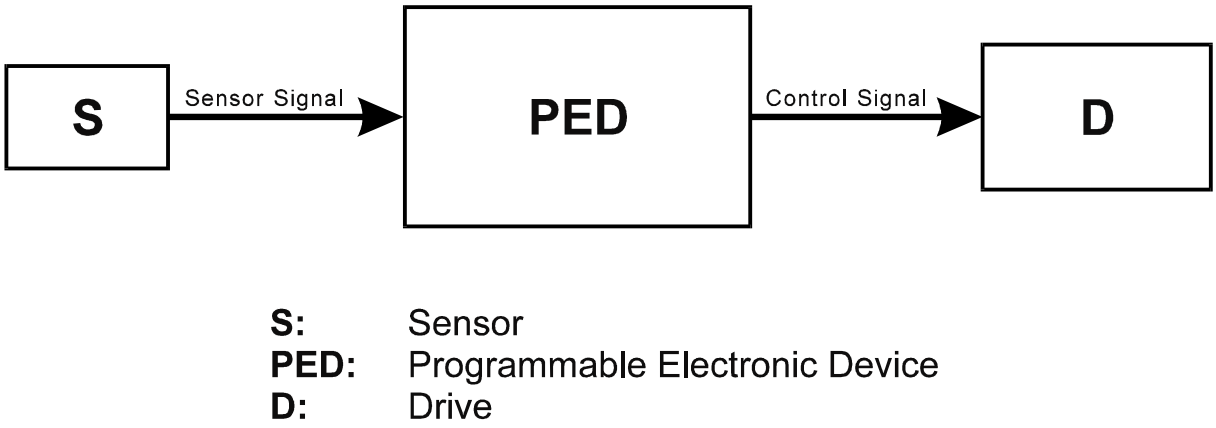


Figure 8: Block diagram of a single channel system without fault detection

Normally a single electronic device is not regarded to be a well-tried component. Thus, it is not possible to realise a category 1 single channel safety system using a PED.

Three assumptions have been made in order to determine the SIL:

1. Switching off the drive is the appropriate action to generate a safe state of the equipment under control (EUC) the drive is belonging to.

2. The safety system is not able to induce a hazardous situation by itself. The worst case which can occur is a dangerous failure, i.e. the system cannot perform it's intended safety function.

3. Failures are only revealed by a demand on the safety function. This leads to a hazardous situation which will be followed by a repair.

4.2. Markov model and assumptions

Since all three components are series-connected either of them must be operational for the safety system to be operational. Therefore a total failure rate for the system can be obtained by simply adding the failure rates oft the components:

$$\lambda_{SCS} = \lambda_S + \lambda_{PE} + \lambda_D$$

Assuming constant failure rates for the components the system failure is also constant. As mentioned formerly only dangerous failures are regarded. The Markov model regarding system failure, demand on the safety function and repair is shown in Figure 9.

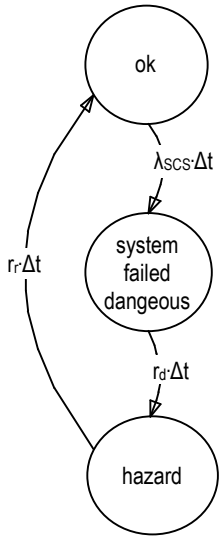


Figure 9: Markov model of the single channel system (SCS) without fault detection

4.3. Result of evaluation

Because of the elementary nature of this specific model no special matrix technique is needed (although such techniques could be applied successfully). The result can be obtained by solving a system of three differential equations describing the inputs and outputs of each state. Involving the initial conditions

$$p_{ok}(t=0) = 1, \qquad p_{syst.\,failed\,dang.}(t=0) = p_{hazard}(t=0) = 0,$$

and using the abbreviations

$$Q = \frac{1}{2} \cdot \left(\lambda_{scs} + r_d + r_r\right) \qquad \text{and} \qquad R = \frac{1}{2} \cdot \sqrt{\left(\lambda_{scs} - r_d - r_r\right)^2 - 4 \cdot r_d \cdot r_r}$$

the average probability of a dangerous failure on demand for the mission time T_M is given by

$$PFD = \frac{\lambda_{scs} \cdot r_r}{Q^2 - R^2} + \frac{\lambda_{scs}}{T_M} \cdot \left[\frac{r_r - Q - R}{2R(Q+R)^2} \left(1 - e^{-(Q+R)T_M}\right) - \frac{r_r - Q + R}{2R(Q-R)^2} \left(1 - e^{-(Q-R)T_M}\right) \right].$$

Thus the average probability of a dangerous failure per hour can be calculated by

$$PDF = \frac{\lambda_{scs} \cdot r_d \cdot r_r}{Q^2 - R^2} + \frac{\lambda_{scs} \cdot r_d}{T_M} \cdot \left[\frac{r_r - Q - R}{2R(Q+R)^2} \left(1 - e^{-(Q+R)T_M}\right) - \frac{r_r - Q + R}{2R(Q-R)^2} \left(1 - e^{-(Q-R)T_M}\right) \right].$$

These equations have been evaluated for a mission time T_M of 10 years and 1 year and a ("dangerous") mean time to failure of 15, 150 and 1500 years each component. The result is shown in the diagram of Figure 10.

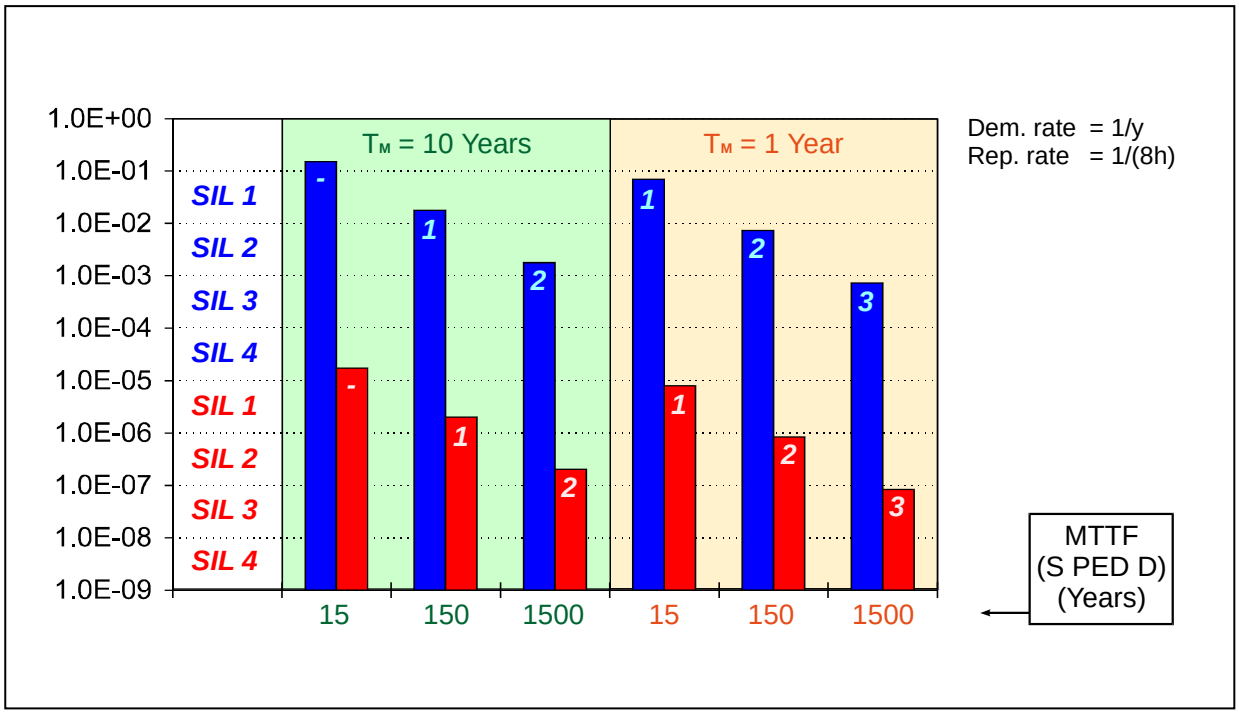


Figure 10: Average probabilities (PFD, PDF) versus MTTF for the single channel system without fault detection

According to the diagram, for a mission time of 10 years each unit of Figure 8 needs an MTTF of 150 years to achieve SIL 1. So the safety-related system has a total MTTF of 50 years.

Systematic failures are not included because they are assumed to be avoided by the qualitative measures and requirements of IEC 61508. If systematic failures are included, the MTTF of the hardware must be even better than 50 years.

The calculations assuming a mission time of 10 years and no proof test shows that SIL 1 cannot be achieved by complex electronics according to category B.

As defined in IEC 61508 a proof test requires each component of the safety-related system to be tested, so that after the proof test the system can be restored to an "as new" condition. We believe that proof tests are not possible for complex electronics but only for non complex electromechanics. A proof test may therefore be possible for category 1 systems.

Figure 10 also shows that SIL 1 is possible with a MTTF of 15 years per unit if the mission time is cut down to one year. This is equivalent to performing a perfect proof test once a year thus starting a "new" mission time in order to prolong the actual period of use. For electromechanical devices a

MTTF of 150 years may be possible so that SIL 2 may be achievable with a proof test interval of one year. Higher SILs are not realistic even for category 1 architectures.

The single channel system without fault detection establishes a "reference system" which the systems introduced in the next chapters will be compared with. Hence, the effects of measures like hardware redundancy or online tests will be made obvious.

5. Single channel system with implemented tests in accordance with category 2 of EN 954-1

5.1. Description

Category 2 of EN 954-1 [2] requires self checks to be executed by the safety related system "at suitable intervals". The tests may be initiated either manually or automatically. If a fault is detected an output signal shall be generated in order to initiate an "appropriate control action". Whenever possible a safe state shall be induced.

These requirements imply "that the occurrence of a fault can lead to the loss of the safety function between the checking intervals". Additionally it must be remarked that many of the typical testing techniques do not provide a diagnostic coverage of 100%. Therefore there may exist faults within the safety device which cannot be detected by the checks.

A representative system architecture for category 2 is presented by the block diagram of Figure 11 [9].

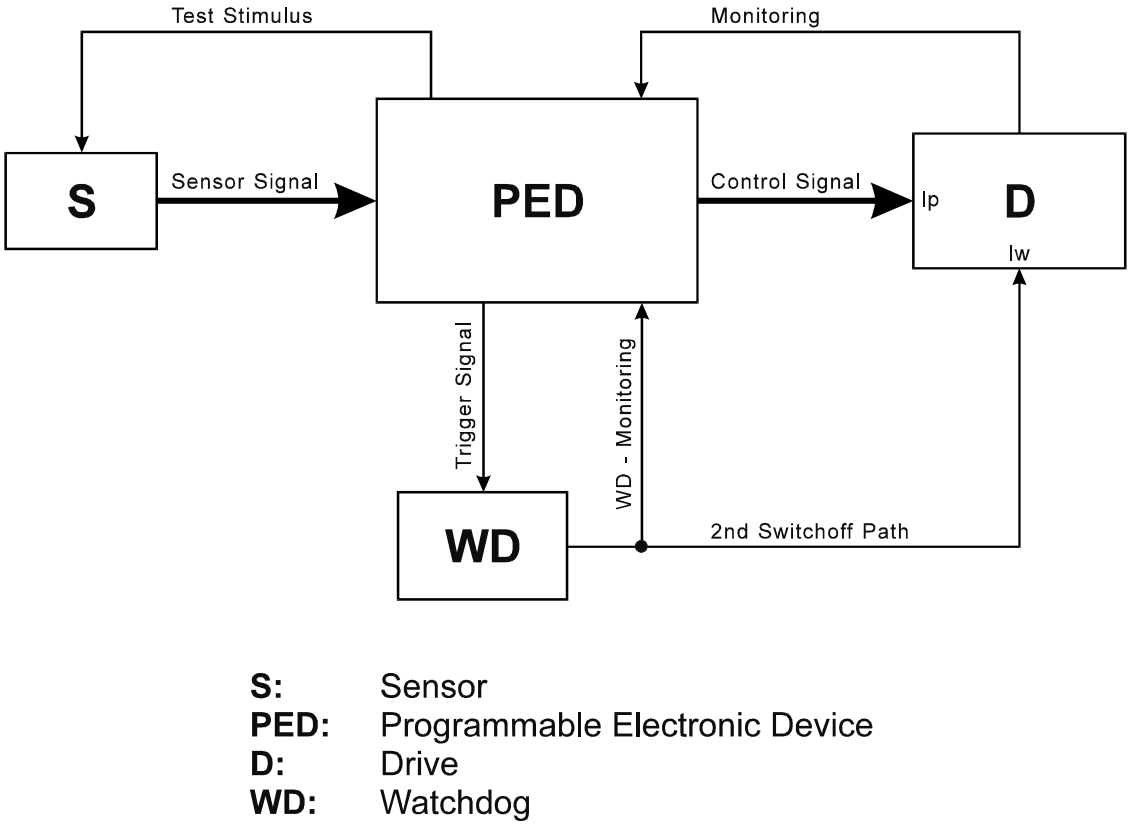


Figure 11: Block diagram of a single channel system with implemented tests

Compared with the simple system of Figure 8 a watchdog (WD) has been added in order to monitor the operation of the programmable electronic device (PED) which is thought to be represented by a microcontroller system. In the PED a power supply is integrated. The drive (D) has two separate inputs, the first (Ip) - as usual - for the PED and a second one (Iw) for the watchdog, each providing full switch-off capability. The system is also performing periodic tests of the sensor, the switch-off path(s) of the drive and the watchdog.

Several assumptions have been made in order to ease the creation of a suitable Markov model:

1. Switching off the drive is the appropriate action to generate a safe state of the equipment under control (EUC) the drive is belonging to.
2. The safety system is not able to induce a hazardous situation by itself. The worst case which can occur is a dangerous failure, i.e. the system cannot perform it's intended safety function.
3. The programmable electronic device (PED) is periodically performing a self test. Detection of a dangerous failure of the PED simply consists in staying away of the retrigger pulses which are normally sent repeatedly to the watchdog (WD). This online test is characterised by the test rate r_{tp} and the diagnostic coverage C_{pe} which is assigned a value between zero and one. C_{pe} is the conditional probability that a dangerous failure of PED will be detected, given that it has occurred. In this case the PED is no longer able to cut off the drive via input Ip although this might be necessary. If the fault is detectable the drive will be cut off by the watchdog via input Iw (presumed that WD and Iw both are operational).
4. The sensor and the drive-internal switch-off path beginning with input I_P of the drive are tested periodically by the PED. The corresponding test rates are named r_{ts} and r_{tip} respectively. The diagnostic coverages are assumed to be equal to one as long as the tests are carried out. The test rates can be set to zero in order to model the case that no such tests are implemented.
5. The watchdog is also tested by the PED. The corresponding test rate is called r_{tw} and the diagnostic coverage is supposed to be equal to one. If there is no watchdog test, the rate r_{tw} can be set to zero. There are two ways to monitor the operation of the watchdog. It's output signal can either be directly reread by the PED or the drive-internal switch-off path beginning with input Iw of the drive can be included in the test loop. In the latter case said switch-off path is also covered by the test. This can be expressed by the diagnostic coverage C_{iw} which is set either to zero or to one.
6 Any failure which has been detected successfully will drive the system to a non-volatile safe state with the drive cut off. The system is assumed to be disconnected from the power manually until it has been repaired or replaced by a new one.
7. If the PED has failed it will no longer perform any tests of PED-external components, i.e. S, Ip, WD and Iw are not tested in case of a failure of PED.
8. In order to describe the drive by a single dangerous failure rate a factor k out of the interval (0...1) has been introduced. Thereby the dangerous failure rates of the drive-internal switch-off paths beginning with inputs Ip and Iw respectively can be derived from the drive's total dangerous failure rate:

$$\lambda_{IP} = k \cdot \lambda_D \qquad \lambda_{IW} = (1-k) \cdot \lambda_D$$

5.2. Markov model and assumptions

Based on the assumptions listed in chapter 5.1 Markov model SCST (Single channel system with implemented tests) has been developed. It is plotted in Figure 12.

The state at the top is depicting the fully operational system. The ellipse-shaped state “undet dang” on the right represents a collection of dangerous states with no fault detection possible. Thus a demand from this state leads to the hazardous state at the bottom. All the other states are intermediate states where some components have failed and a detection is possible or has already happened (state “fail det” on the left). Every dangerous state of the model is labelled by the remark "dang". Any of the circle-shaped states is also labelled by names of the components that have failed. After a hazard has occurred the machine is disconnected from power and repaired. The same is valid when a failure is detected by online tests.

The Markov model is a little complicated because we wanted to simulate the time-related behaviour of the system. This is the reason why, for instance, the intermediate states “S dang”, “PED dang” and “IP dang” appear in the second row of Figure 12: some time is needed to detect the failures and during this span of time a demand on the safety function could lead to a hazard or a second unit could fail. Rows 3 and 4 show states where a second and third unit fails before the failure is detected and a demand occurs. With this complete Markov model the effect of the demand rate, the test rate and the diagnostic coverage can be studied. This is not possible with an often used simplified approach where a failure is immediately detected or not. After studying the time effects in detail we will decide whether a simplification is allowed or even fault tree analysis will be sufficient.

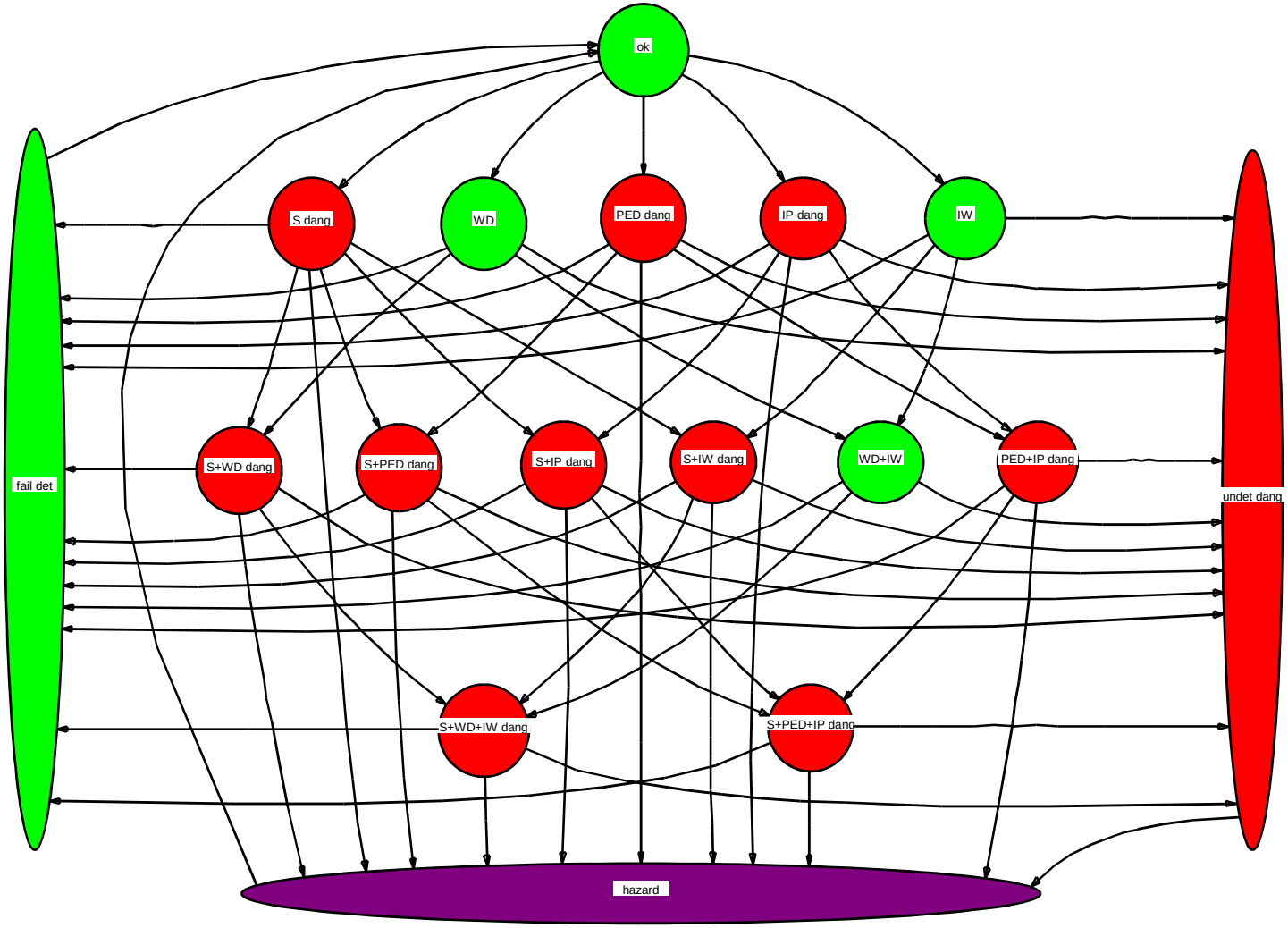


Figure 12: Markov model SCST of a single channel system with implemented tests

5.3. Result of evaluation

Model SCST was evaluated by using the spreadsheet program MS Excel. As a reference configuration we chose a MTTF of 15 years per unit. Drive D and sensor S can be tested with 100% coverage by the PED. The self test of the PED is executed in connection with the watchdog WD. According to [10] 80% coverage can be assumed for a tested WD. 100% diagnostic coverage is possible for a digital sensor giving an on or off signal. These signals are usual for sensors which are monitoring the position of a guard, for a safety mat or a light curtain in front of a machine. In order to test the drive it has to be checked whether the motor is moving or not. This can also be done by a sensor giving a digital output, thus we supposed 100% diagnostic coverage. Test and repair rate both were chosen one per 8 hours. The demand rate was set to 1 per year assuming the system to be operated in low demand mode. An overview of the reference input parameter set is given by he following table.

MTTF of the programmable logic device (PED)	$MTTF_d\ ped$	15 years
MTTF of watchdog (WD)	$MTTF_d\ wd$	100 years
MTTF of the sensor (S)	$MTTF_d\ s$	15 years
MTTF of the drive (D), k=0.5	$MTTF_d\ d$	15 years
Diagnostic coverage of the sensor	C_s	1
Diagnostic coverage of the PED	C_p	0.8
Diagnostic coverage of the drive's switch-off input for PED	C_{ip}	1
Diagnostic coverage of the drive's switch-off input for WD	C_{iw}	1
Test rate of the sensor	r_{ts}	1/(8 hours)
Test rate of the PED	r_{tp}	1/(8 hours)
Test rate of the drive's switch-off input for PED	r_{tip}	1/(8 hours)
Test rate of the watchdog and the drive's switch-off input for it	r_{tw}	1/(8 hours)
Repair rate after failure detection	r_r	1/(8 hours)
Demand rate of the safety function	r_d	1/year
Repair rate after hazardous event	r_{rh}	1/(8 hours)
Mission time (life time)	T_M	10 years

Figure 13 compiles the results, i.e. the probability of failure on demand (PFD) for the reference configuration and various parameter alterations. This will be discussed in the following.

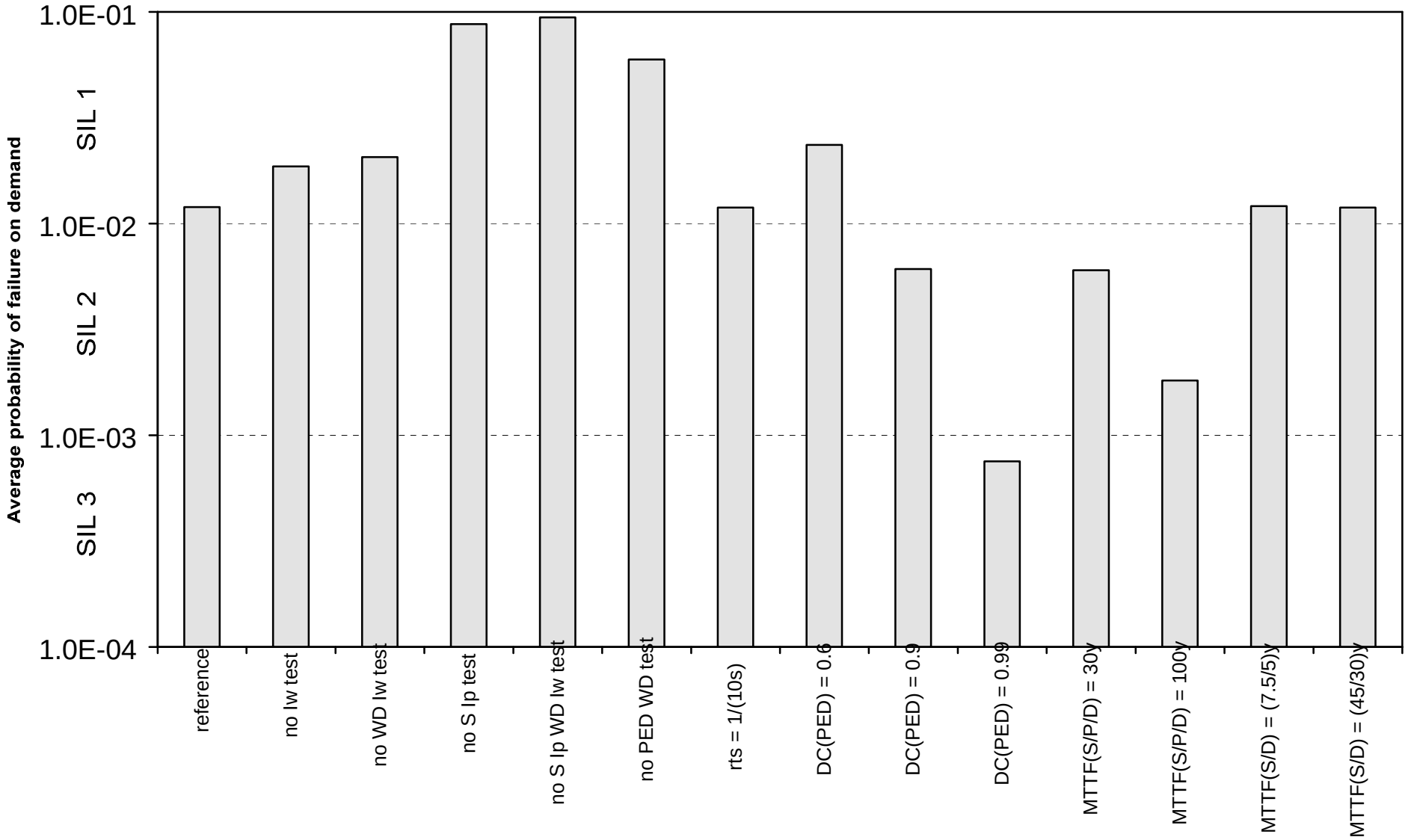


Figure 13: PFD of a single channel system with implemented tests in accordance with category 2

Failure rate of the subsystems

The last four bars in Figure 13 show the results with modified MTTFs. One can see that a change of the MTTF of all subsystems has a direct and proportional effect on the PFD. For a complex safety-related system an MTTF of 30 years may be achievable but 100 years are normally unrealistic. The changes of the MTTFs of sensor and drive exclusively have no remarkable influence on the PFD. This can easily be explained by the fact that we have assumed 100 % diagnostic coverage for sensors and drive. This justifies to assume equal MTTFs for the different components in the other parameter combinations. As a result we can say that a category 2 architecture is able to fulfil SIL 1 and with reliable components may in some cases achieve SIL 2.

Diagnostic coverage of the subsystems

Bars 2 to 6 show the effect of switch-off path testing and watchdog testing. In machinery applications normally it will be possible to test the switch off path when the machine is stopped. In this case the machine sometimes can be stopped by the 2nd switch off path and the reaction of the motor can be monitored. The second bar shows the effect of the omission of this test. It is also possible to test the effect of the WD. This can only be done by using the 2nd switch off path. If this test is omitted the result shown by bar 3 is attained. On the other hand the sensor S and the normal switch-off path can be tested by the PED. If these tests of the periphery are not executed a dramatic effect results as shown by bar 4. If no tests are carried out except the selftest of the PED we loose nearly 2/3 of a SIL step (bar 5). Bar 6 shows that the use of a standard controller (e.g. PLC) without diagnostic tests results in a similar worsening like omitting the peripheral tests. Bars 8, 9 and 10 demonstrate the major influence of the diagnostic coverage of the PED which is similar to the influence of the failure rates. Nearly one SIL step can be gained by improving the diagnostic coverage from 90% to 99%. A processor-watchdog-combination will not be able to achieve a diagnostic coverage of 99%. 90% may be possible by sophisticated means. Processor tests are very effective but they have to be combined with tests of the peripheral subsystems.

Repetition rates of the diagnostic tests

The seventh bar of Figure 13 shows what happens if the diagnostic tests are executed every 10 seconds instead of every 8 hours. Actually there is nearly no effect. Our investigations proved that a single channel system will show an effect if the test rate is not much higher than the demand rate. This is demonstrated in Figure 14. The bars indicate the number of hazardous situations per system within a mission time of 10 years. A hazard, in this sense, occurs at any time when a system which has failed dangerously is confronted with a demand on the safety function. Each bar of Figure 14 is labelled with the corresponding time T_t between consecutive online tests (the reciprocal value of the test rate r_t) and the mean time between demands ("*MTBD*", the reciprocal value of the demand rate r_d). For these calculations the assumption was made that no repair is carried out after a hazardous event but the system is decommissioned in this case. As shown in Figure 14, for maximum test effect the test rate must be at least a factor of 100 greater than the demand rate. A factor very much greater than 100 will offer no additional benefit. If the test rate has the same order of magnitude as the demand rate this results in an increase of the number of hazardous events by a factor of about 6 or 7.

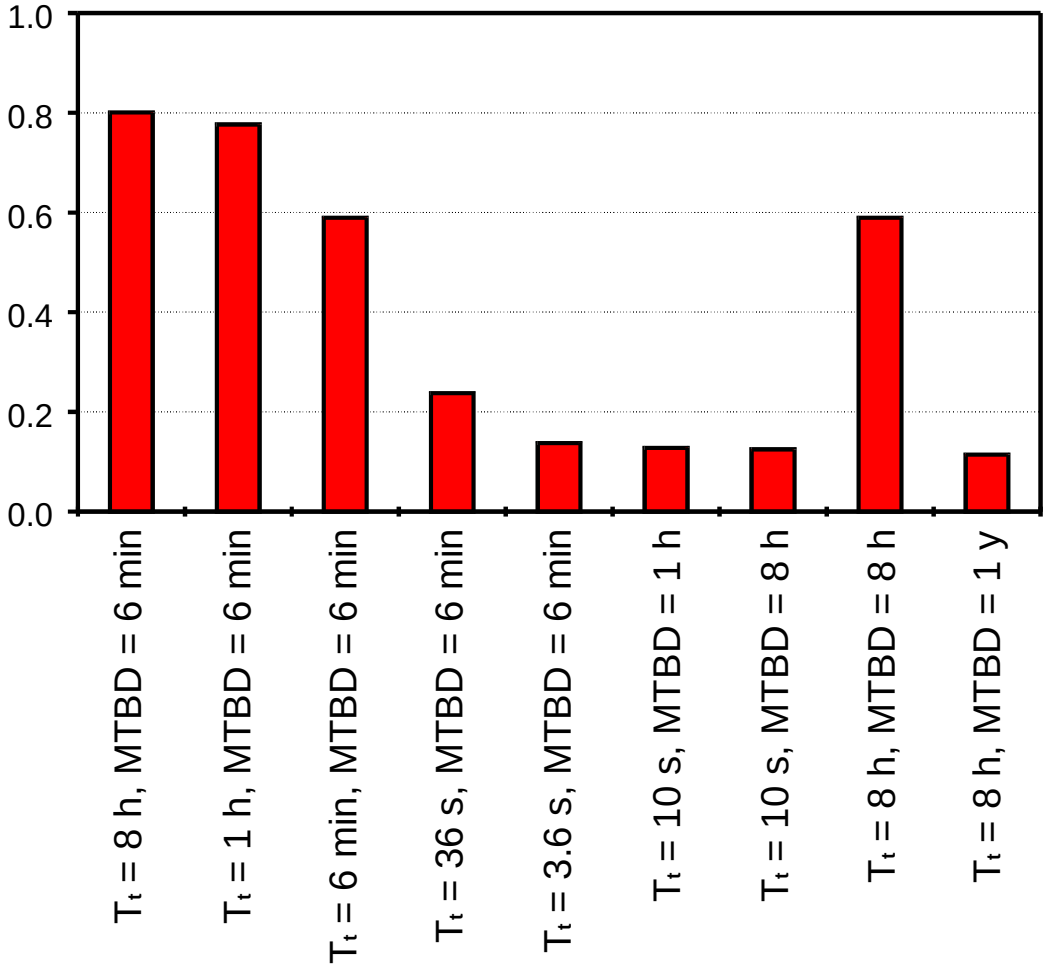


Figure 14: Single channel system with testing:
Number of hazardous events per system during a mission time of 10 years

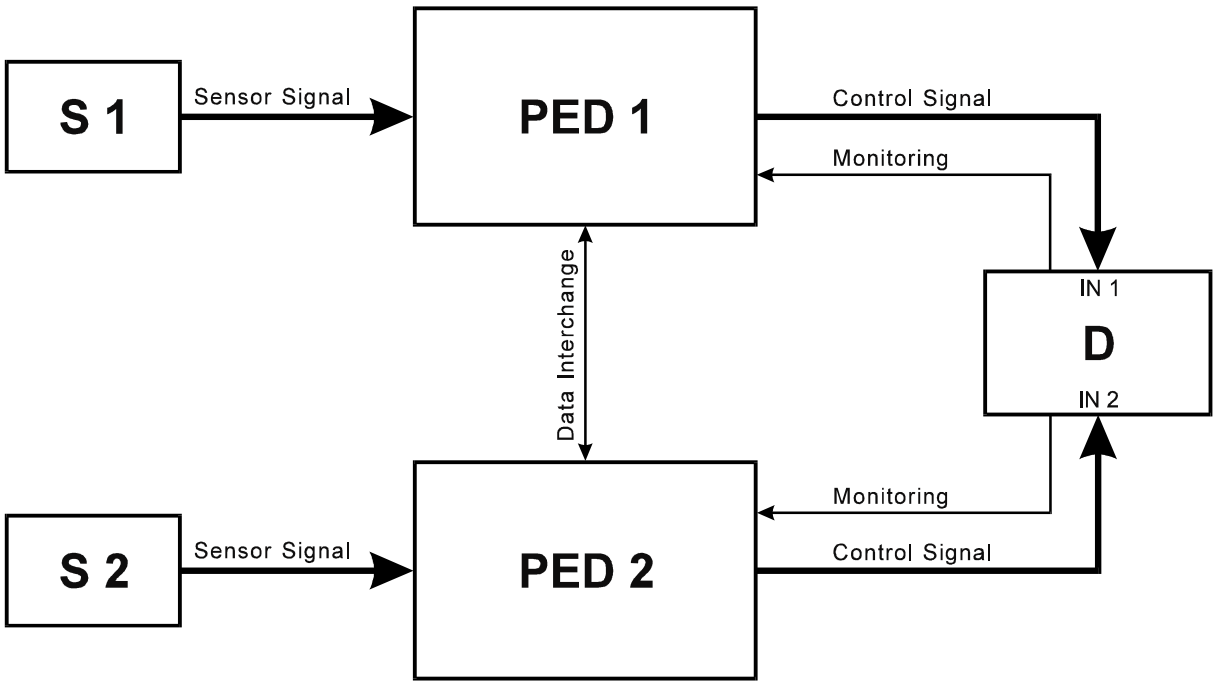
6. Dual channel system with comparison in accordance with category 3 or 4 of EN 954-1

6.1. Description

EN 954-1 [2] requires a category 3 device to remain operational if a single fault is present in any part of the system. Besides, "whenever reasonably practicable the single fault shall be detected at or before the next demand upon the safety function." This includes that not all faults must be detected and that "the accumulation of undetected faults may lead to an unintended output and a hazardous situation at the machine." Common mode failures shall be taken into account.

In addition to above-mentioned demands there are more rigid requirements to be fulfilled by a system that claims for category 4: The single fault shall be detected "whenever possible" and, "if this detection is not possible, then an accumulation of faults shall not lead to a loss of safety functions."

The problem of providing the safety functions after the occurrence of a fault is often solved by the implementation of redundancy. A typical example for homogeneous redundancy is given by the dual channel system depicted by Figure 15 [9]. Whether category 3 or 4 can be met depends on the extent to which faults can be detected or tolerated.



S 1, S 2: Sensor
PED 1, PED 2: Programmable Electronic Device
D: Drive

Figure 15: Block diagram of a dual channel system with comparison

The system comprises two sensors (S1, S2) of same type and two programmable electronic devices (PED1, PED2) of identical type with integrated power supply in each PED combined with a single drive (D). Either of the PEDs is connected with an individual input (IN1, IN2) of the drive. In reality the PEDs will usually be given by microcontrollers. The cross link between them is intended for data interchange.

Again, there is a number of reasonable assumptions which have been made in order to derive a suitable Markov model:

1. Switching off the drive is the appropriate action to generate a safe state of the equipment under control (EUC) the drive is belonging to.
2. The safety system is not able to induce a hazardous situation by itself. The worst case which can occur is a dangerous failure, i.e. the system cannot perform it's intended safety function.
3. Periodic online tests are carried out by the two programmable electronic devices (PEDs). The complete set of tests includes:
   - a self-test of PED1 controlled and monitored by PED2,
   - a self-test of PED2 controlled and monitored by PED1,
   - a test of the drive-internal switch-off path beginning with input IN1 of the drive, performed by PED1,
   - a test of the drive-internal switch-off path beginning with input IN2 of the drive, performed by PED2,

- a comparison of the output signals of the two sensors (S1, S2), performed by PED1 and PED2 together.

Each of the tests is checking subfunctions which are performed by the different components. Performing all subfunctions properly is a pre-condition for the safety system to provide it's intended safety function(s).

4. The mutually contolled and monitored self-tests of the PEDs are characterised by a diagnostic coverage, which can be assigned a value between zero and one.
5. The diagnostic coverage related to the sensors is equal to one. In some cases the feature will be implemented, in others it won't. This can be expressed by the diagnostic coverage which is set either to zero or to one.[1]
6. The diagnostic coverage related to the drive-internal switch-off paths beginning with inputs IN1 and IN2 of the drive is equal to one. In some cases the feature will be implemented, in others it won't. This can be expressed by the diagnostic coverage which is set either to zero or to one.[1]
7. Any failure which has been detected successfully will lead the system to a non-volatile safe state with the drive cut off. The system is assumed to be disconnected from the power manually until it has been repaired or replaced by a new one.
8. If one PED has failed dangerous it will no longer perform the test of it's related drive input. The comparison of the output signals of the sensors is also inhibited.
9. A dangerous failure of both sensors at the same time is not detectable because they deliver identical (wrong) output signals. This can not be revealed by a comparison.
10. The failure rate of each input channel of the drive is given by: $\lambda_I = 0.5 \cdot \lambda_D$
11. Common cause effects do not hit complete channels but the two sensors, the two PEDs and the two switch-off inputs of the drive separately.

6.2. Markov model and assumptions

Based on the assumptions listed in chapter 6.1 Markov model DCSC (Dual channel system with comparison) has been developed. This dual channel system is put up completely symmetric. Therefore not only the first but also the second of the techniques mentioned in chapter 2.8 could have been applied in order to reduce the number of states needed. For example it doesn't make any difference whether S2 and PED1 have failed or S1 and PED2. Uniting every pair of such "mirror combinations" to a single state in the Markov model cuts down the number of states necessary by nearly one half.

The resulting Markov model is plotted in Figure 16. All circle-shaped states are labelled with the components which have failed respectively. Dangerous states (red-coloured) have additionally been marked by the label "dang". State 17 was created using the first technique of chapter 2.8. It collects all dangerous states where

- the inherent faults can not be detected without having a real demand because there is no appropriate test left running and
- no additional failure of a component will lead to a condition where a test could be successful.

[1] For machinery normally only a few digital sensors like switches are used. Monitoring of the drive is also done by digital signals. Thus a 100% diagnostic coverage is possible.

Common cause effects have been taken account of by using the β model technique described in chapter 2.3 (Figure 2). For this the presumption was made that all components of same type can be hit by common cause failure. Therefore individual β factors were introduced for the sensors (β_d), the PEDs (β_p) and the switch-off inputs (β_i) of the drive.

Regarding the common cause effect results in 7 more transition arcs in the model. Furthermore the transition probability of many existing arcs has to be adapted. For better clearness in Figure 16 the additional arcs due to common cause effects have been drawn orange-coloured.

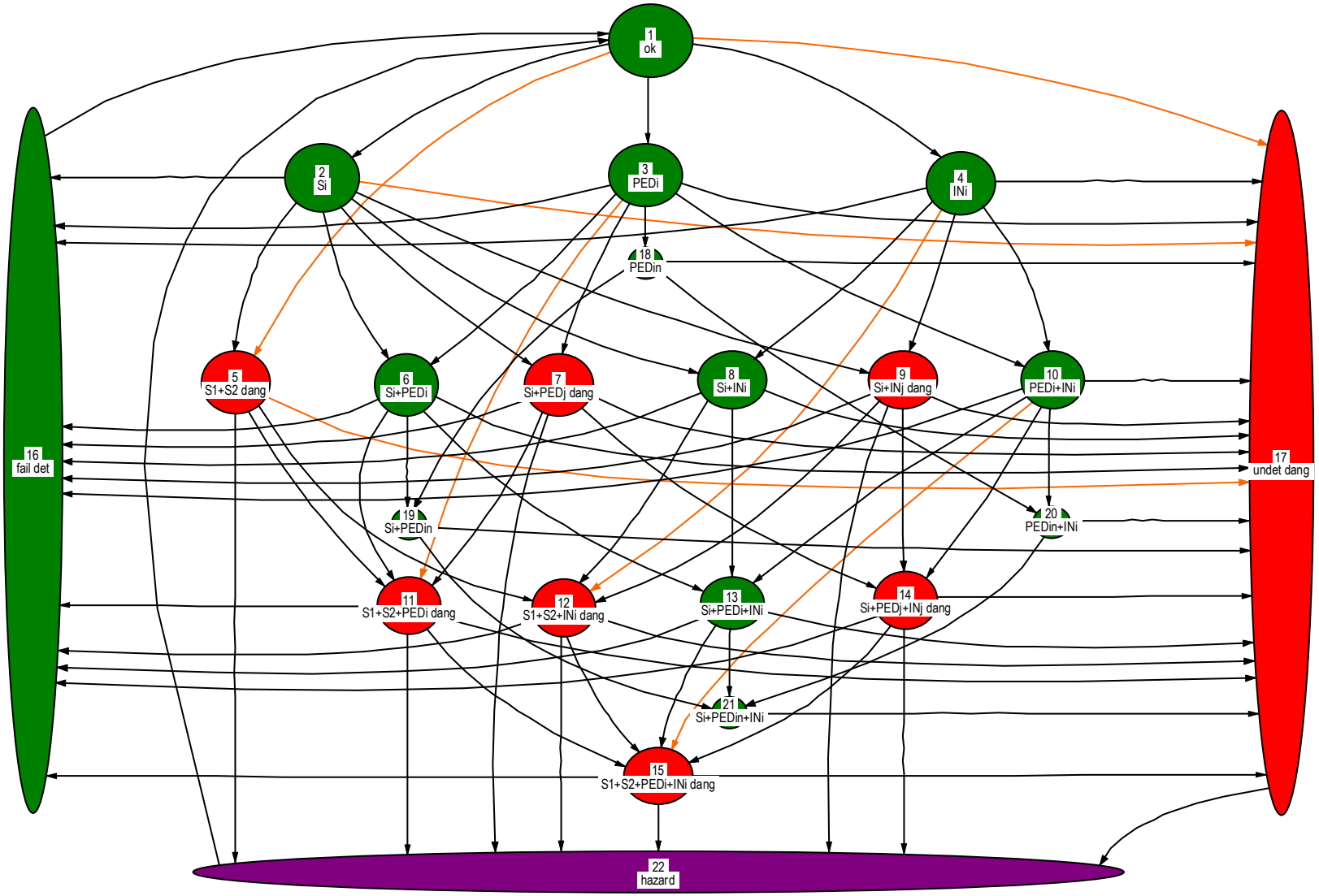


Figure 16: Markov model DCSC of the symmetric dual channel system

6.3. Result of evaluation

Markov model DCSC of Figure 16 has been evaluated as a high demand system with a demand rate of 10 demands on the safety function per hour. All calculations are based on an mission time of ten years. The following set of input parameters has been chosen as reference set:

MTTF of the sensors (S)	$MTTF_d\ s$	15 years
MTTF of the programmable logic devices (PED)	$MTTF_d\ p$	15 years
MTTF of the drive (D)	$MTTF_d\ d$	15 years
Diagnostic coverage of the sensor comparison	C_s	1
Diagnostic coverage of the PED self tests	C_p	0.9
Diagnostic coverage of the switch-off inputs of the drive	C_i	1
Test rate of all online test	r_t	1/(10 s)
Repair rate after failure detection	r_r	1/(8 hours)
Demand rate on the safety function	r_d	10/hour
Repair rate after hazardous event	r_{rh}	1/(8 hours)
Mission time (life time)	T_M	10 years

In the following paragraphs the influence of the different parameters on the probability of a dangerous failure per hour will be discussed. The complete compilation of all results is shown in the bar diagram of Figure 17. It should be noticed that in this diagram the probability is depicted in a logarithmic scale. The three β factors for the sensors, the PEDs and the switch-off inputs of the drive have been assigned the same value which is simply called β. Each parameter combination has been evaluated for the β values 0, 1%, 5% and 10%. In Figure 17 the β factor is indicated by the colour of the bars.

Implementation of diagnostic tests

A comparison of the results obtained by run 1, run 2, run 7 and run 8 reveals the immense impact of diagnostic coverage on the probability of a dangerous failure. Only the coverage for the PED has been altered. The step from 90% to 99% results in an improvement of about one order of magnitude (β=0) but a β factor of only 0.01 will reduce the gain to half an order of magnitude (or half a SIL step). The step from 60% to 90% only provides a smaller progress. Figure 17 shows that at least 90% diagnostic coverage is necessary to achieve SIL 2 with reasonable MTTFs (β=0.01). Comparing run 1, run 2, run 3 and run 4 gives an answer to the question whether internal online tests for PEDs are necessary. In run 4 no diagnostics were assumed while in run 3 100% diagnostics for sensors and drive and in run 7 additionally 60% diagnostics for the PED were chosen. Run 7 may be a good example for using two standard programmable logic controllers, implementing 100% diagnostics for the peripheral components and using these systems for safety functions. Figure 17 shows that this version is not much better than doing no diagnostics at all and too bad for SIL 2. Only the higher diagnostics in the PED (see run 1) brings the necessary jump into SIL 2 but a β factor of 0.05 or 0.1 will reduce the result to SIL 1.

Test rate

All tests in the system are assumed to be executed once within the same cycle. Thus, they all are related to the same test rate (or test interval). Comparing run 1 and run 5 the test rate is reduced from one test every ten seconds to one test per hour. In run 6 the test rate is only one test per eight hours. The result of the evaluation clearly shows that there is very low influence of the test rate on the probability of a dangerous failure per hour.

Figure 18 shows the influence of the test rate on dual channel systems. The mean time between demands ("MTBD") has been kept constant but the test interval T_t has been altered. As demonstrated by the diagram there is no significant increase in the number of hazardous events as long as the test interval is much smaller than the MTTF of a single channel. This is a fundamental difference to the single channel system where the test rate has to be 100 times larger than the demand rate in order to avoid a substantial increase in the number of accidents. An explanation of this is that in the dual channel system there is still an operational channel left if the first channel has failed. The failure of the first channel plays the role of a "demand" for the remaining "single channel system". Therefore the dominant factor here is not the ratio of test rate and demand rate but the MTTF of the a single channel.

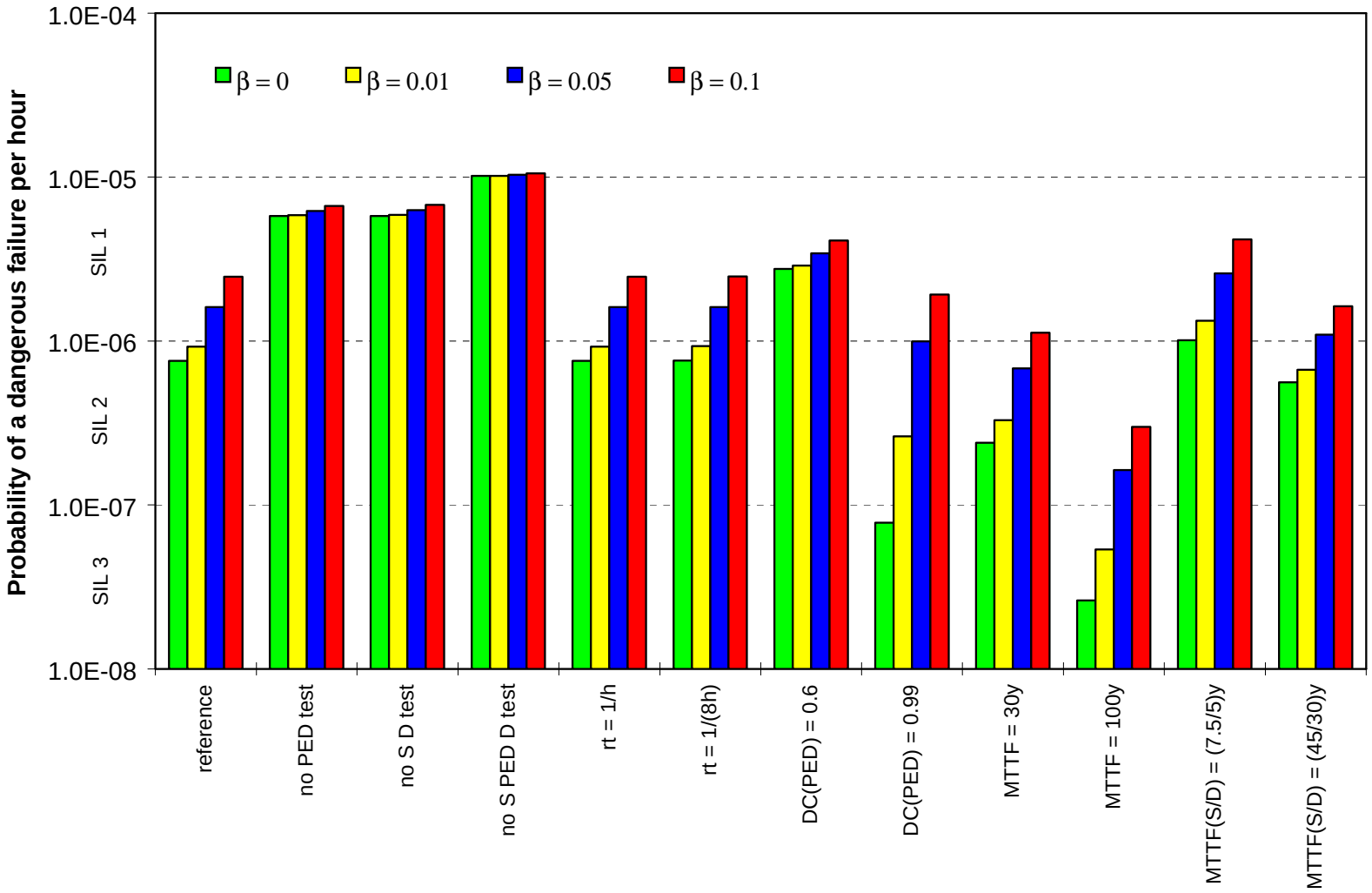


Figure 17: PDF of a dual channel system with comparison (Markov model DCSC)

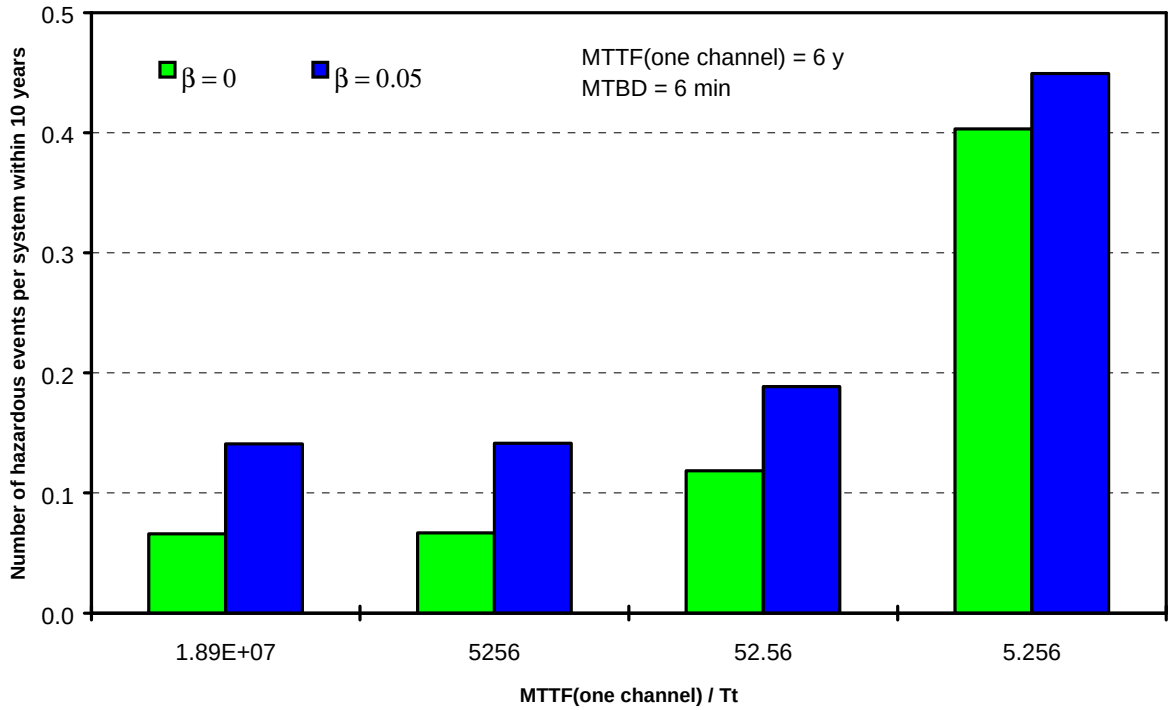


Figure 18: Dual channel system with comparison: Influence of the ratio of MTTF and test interval T_t

Failure rate of the subsystems

Considering Figure 17, the impact of the subsystem failure rate can be studied by a comparison of run 1 (15 years MTTF) , run 9 (30 years MTTF) and run 10 (100 years MTTF). The failure rates of all three types of components are altered in the same manner. It should be noticed that there is a non-linear relationship between the failure rate and the probability of a dangerous failure per hour but that the failure rate has also a big influence on the SIL.

Comparing run 1, run 11 and run 12 reveals what happens if only the failure rates of the sensors and the drive are altered. A lower or higher MTTF for sensors and drive than for the PED have a small effect on the SIL. This can be explained by the 100% diagnostic coverage for the sensors and the drive. This result justifies to take the same MTTF for all three subsystems in our simulations.

Influence of Common cause

The bar diagram of Figure 17 clearly depicts the impact of the β factor for each parameter combination. The reference combination looses about 2/3 of a SIL step due to a common cause factor of 10%. A general principle is recognisable: the lower the failure probability achieved by a system the higher the negative influence of common cause effects, no matter by which measures the low failure probability originally had been achieved. For instance, there is a loss of about 1.5 SIL steps if the system with 99% diagnostic coverage of the PEDs is confronted with a β factor of 10%. A comparison with the reference parameter set (90% coverage) shows that nearly the whole benefit of the very high coverage is lost due to common cause failures (β=10% for both cases). This demonstrates the immense importance of regarding common cause effects during design, development and operation.

According to part 6 of IEC 61508 a β factor of 2% can be looked upon as an achievable value for the machinery sector.

7. Dual channel system in mixed technology in accordance with category 3 of EN 954-1

7.1. Description

In many applications a mixed technology is used in order to implement a safety function. A first channel is given by a standard programmable logic controller (PLC) with integrated power supply and no specific online tests, while the second channel is formed by electromechanical means. Online tests are carried out by the PLC to check the elements of the electromechanical signal path.

As an example the simplified schematic of Figure 19 depicts the implementation of an emergency stop function employing a PLC and a relay circuit.

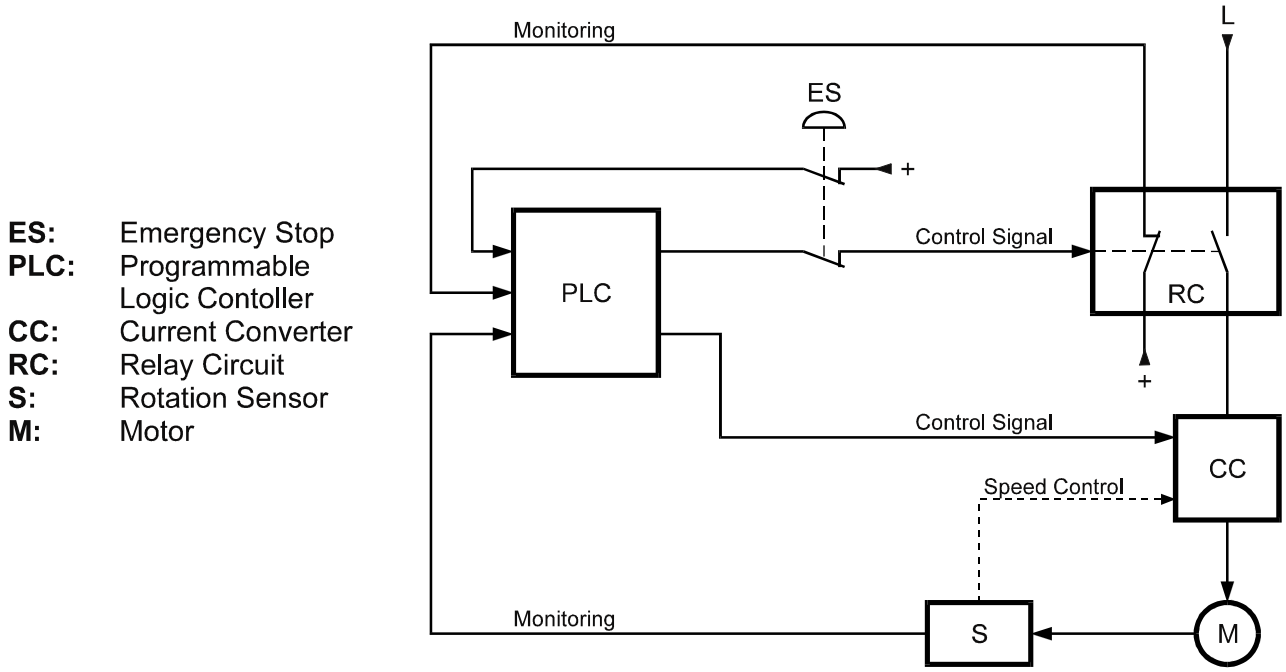


Figure 19: Implementation of an emergency stop function using mixed technology

We assume a machine where a current converter (CC) is controlled by a standard PLC. The rotation sensor (S) is part of the speed or position control of the current converter and can be used by the PLC to monitor the motor movements.

The safety function to be implemented is the emergency stop of the dangerous movement as soon as the emergency stop device (ES) is actuated. The actuator contains two mechanically forced contacts, either of them providing a separate output signal. One of which is processed by the PLC while the other is led to a relay circuit (RC) consisting of 2 relays (or contactors respectively) with forced contacts. The emergency stop function is executed by both the PLC via the current converter and the relay circuit. A failure of the opening of the contacts of the emergency stop actuator device is excluded. Independent random failures are supposed to happen to the PLC, the current converter, the relay circuit and the sensor while the emergency stop actuator ES is imputed not to fail to open it's contacts if the button is pressed.

The PLC software is designed so that the opening of the contact of ES immediately leads to a stop signal for the current converter. Four online tests can be modelled by our Markov model. If one of the tests is not implemented in reality the pertinent test rate may be set to zero.

Description of the online tests:

- PLC diagnostic test:

  As said before a standard PLC is used. Therefore we assume only simple online tests like a watchdog and parity bit test of the memory which are common today also for standard electronics. This will result in a low diagnostic coverage C_p of perhaps 30%. The test rate is r_{tp}. We assume that the PLC after failure detection permanently switches off the outputs connected with CC and RC.

- CC diagnostic test:

  In suitable time intervals e.g. once per day or during maintenance the PLC switches off the motor movement using the current converter CC. In parallel the PLC monitors the output signal of the rotation sensor S so that it can detect the reaction of CC. If the movement is not stopped by CC the PLC permanently stops the motor via the relay circuit RC. The diagnostic coverage of this test is named C_c and the test rate is called r_{tc}.

- Rotation sensor diagnostic test:

  The diagnostic test of CC can only be effective if the rotation sensor S is able to detect the motion of the motor. To check this the PLC is reading the sensor signal after switching on the motor. If the motion is not detected the PLC permanently stops the motor using the relays circuit RC. Diagnostic coverage of this test: C_s, test rate: r_{ts}.

- Relay circuit diagnostic test:

  After a normal stop of the motor using CC and after executing the CC diagnostic test the PLC switches off the control signal for RC. Simultaneously the PLC monitors the corresponding contact(s) of the relay circuit RC. If RC does not react properly the PLC permanently stops the motor via the current converter CC. Because of the test's simplicity the diagnostic coverage C_r can reach 100%. The test rate is titled r_{tr}.

7.2. Markov model and assumptions

The four subsystems PLC, CC, S and RC are assumed to be hit by random failures. Because of the total different structure of the two channels we did not presume common cause failures. The Markov model has to model the failure of all subsystems in all possible sequences and in all combinations. We assume that the system after a permanent stopping of the motor in case of failure detection is disconnected from power. In this situation we do not have to assume further random failure occurring during repair. The repair rate is called $r_{r.}$

With these assumptions we get the Markov model shown in Figure 21. All states depicted by circles are labelled with the subsystems which have failed dangerously (exception is state 1 where all is ok). The letter n after a subsystems name indicates that the failure of this subsystem is not detectable. State 24 shows the permanent stopping of the motor after failure detection.

For the evaluation of the model it is necessary to know which of the states are dangerous. As a useful tool a *fault tree* may be used identify them. The fault tree of our system is depicted in Figure 20. This tree could also form the first step of a quantitative *fault tree analysis* (FTA) which is able to deliver probability values [6], [7], but in this case it is used as qualitative tool only.

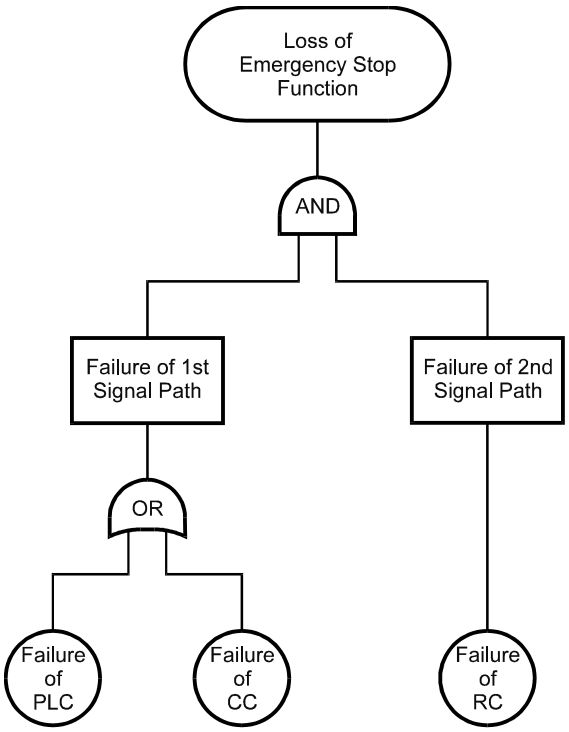


Figure 20: Fault tree of the dual channel system in mixed technology

According to the fault tree states 14, 23 and 25 are dangerous states which means the loss of the emergency stop function. State 25 summarises all dangerous states where no test is effective. In Figure 21 all dangerous states are additionally labelled by the appendix “dang”.

The single failure fault tolerance of this redundant architecture can be perceived in the Markov model by the fact, that no state with one subsystem faulty (states 2 to 9) is dangerous. State 26 represents the hazardous state which will be reached if an emergency stop has to be executed while the system is in a dangerous state. In the labelling of the transition arcs *dt* is used instead of Δt and *lp*, *lc*, *ls* and *lr* instead of λ_p, λ_c, λ_s and λ_r.

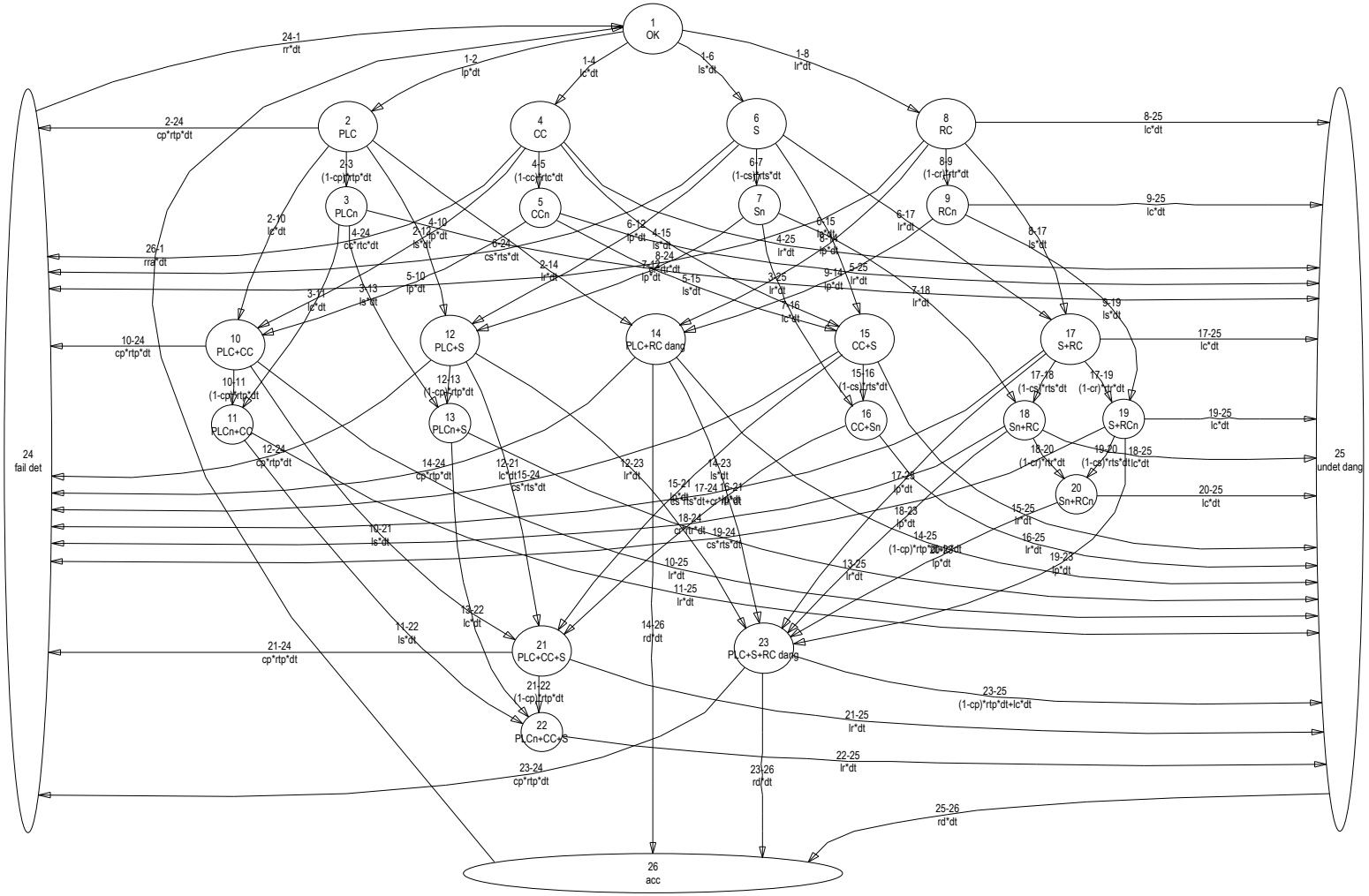


Figure 21: Markov model DCSMT of the dual channel system in mixed technology

7.3. Result of evaluation

A reference input parameter combination was chosen which is shown in the following table. With a demand rate of 1/year the appliance was evaluated as a low demand system.

MTTF of the programmable logic controller (PLC)	$MTTF_d\ plc$	15 years
MTTF of current converter (CC)	$MTTF_d\ cc$	15 years
MTTF of rotation sensor (S)	$MTTF_d\ s$	15 years
MTTF of relay circuit (RC)	$MTTF_d\ rc$	15 years
Coverage of the PLC diagnostic test	C_p	0.3
Coverage of the CC diagnostic test	C_c	0.9
Coverage of the rotation sensor diagnostic test	C_s	0.9
Coverage of the relay circuit diagnostic test	C_r	1.0
Test rate of PLC diagnostic tests	r_{tp}	1/hour
Test rate of the current converter diagnostic test	r_{tc}	1/(24 hours)
Test rate of the rotation sensor diagnostic test	r_{ts}	1/(24 hours)
Test rate of the relay circuit diagnostic test	r_{tr}	1/(24 hours)
Repair rate after failure detection	r_r	1/(8 hours)
Demand rate of the emergency stop function	r_d	1/year
Repair rate after hazardous event	r_{rh}	1/(8 hours)
Mission time (life time)	T_M	10 years

Based on this reference data a number of simulations runs with different parameter deviations were performed. The result is shown in Figure 22. One can see that SIL 2 will hardly be achieved by the reference configuration.

Investigations revealed that a demand rate lower than 1/year results in an increase of the probability of a dangerous failure on demand. The deterioration reaches about 2/3 of a SIL step if the demand rate is assumed to be zero. This effect is independent from the other input parameters and it is due to the fact that a demand hitting a defective system will not only lead to a hazardous event but will also reveal that the system has failed dangerously. Consequently a very low demand rate will raise the fraction of systems dwelling in dangerous undetectable states. Therefore it is sensible to check the emergency stop function manually once a year.

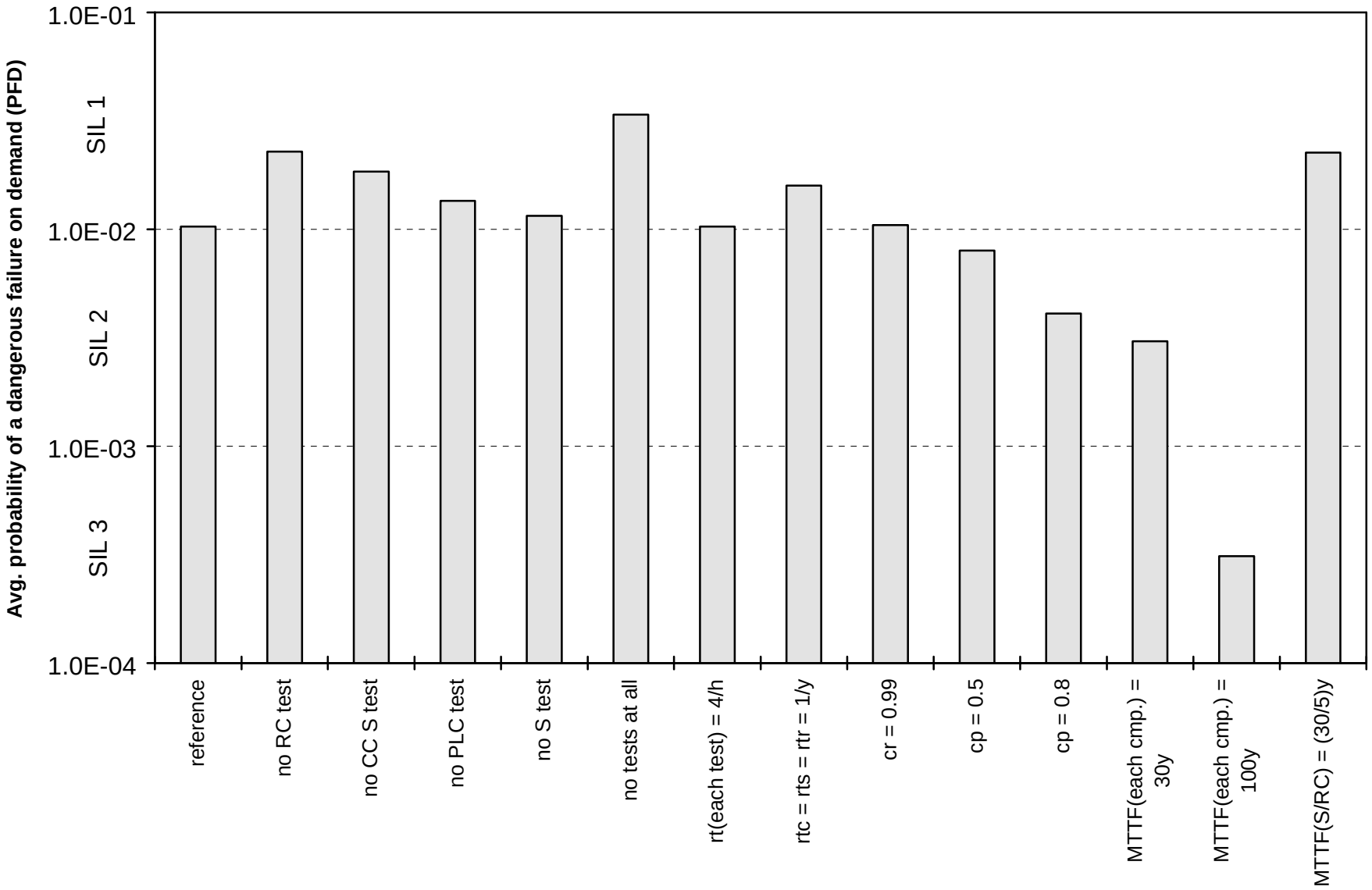
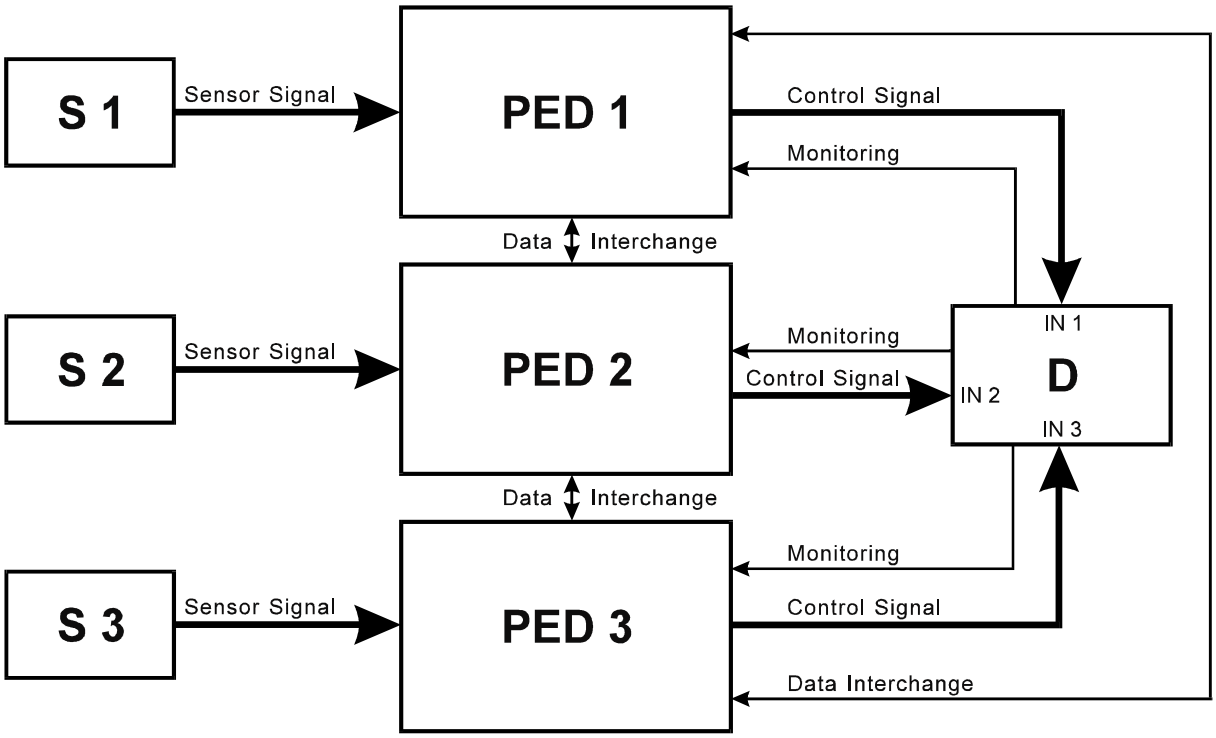


Figure 22: Evaluation result of Markov model DCSMT

8. Triple channel system with comparison in accordance with category 4 of EN 954-1

8.1. Description

In seldom cases the problem of providing the safety functions after the occurrence of a fault is solved by the implementation of triple redundancy. A typical example for homogeneous redundancy is given by the tiple channel system depicted by Figure 23. Whether category 3 or 4 can be met depends on the extent to which faults can be detected or tolerated.



S 1, S 2, S 3: Sensor
PED 1, PED 2, PED 3: Programmable Electronic Device
D: Drive

Figure 23: Block diagram of a triple channel system with comparison

The system comprises three sensors (S1, S2 and S3) of same type and three programmable electronic devices (PED1, PED2 and PED3) of identical type (with integrated power supply) in connection with a single drive (D). Each PED is connected to an individual input (IN1, IN2 and IN3) of the drive. In reality the PEDs will usually be given by microcontrollers. The three cross links between them are intended for data interchange.

8.2. Markov model and assumptions

More or less the same or equivalent assumptions are made as for the dual channel architecture in chapter 6.1 in order to derive a Markov model which can deliver comparable results.

The system contains 9 individual components: three sensors, three PEDs and three switch-off paths ("inputs") of the drive. Supposing each component to be either operational or defective will result in $2^9 = 512$ different failure combinations. Therefore all three techniques of chapter 2.8 have been applied in order to reduce the number of states needed:

- Combining all "dangerous" states where *definitively* no online test will be effective any longer,
- Making use of the architectures' symmetry and
- Termination of further model development after the fourth failure in sequence.

Failures due to common cause effects have been taken account of by the simple β model implementing the modelling principle demonstrated in Figure 4 of chapter 2.3.

The result was a Markov model consisting of 91 states and a very large number of transition arcs. Due to it's complexity no drawing of it is shown in this report.

8.3. Result of evaluation

The Markov model has been evaluated as a high demand system with a demand rate of 10 demands on the safety function per hour. All calculations are based on a mission time of ten years. The input parameters for the reference set is nearly identical with the table in chapter 6.3. Again, the MTTF of each switch-off path of the drive D is set to 30 years; all other components have a MTTF of 15 years. Deviating from the symmetric dual channel system the three test rates for sensor comparison, PED self test and switch-off path test are set to one per day (instead of one every 10 seconds). The complete reference parameter set is presented in the following table.

MTTF of the sensors (S)	$MTTF_d\ s$	15 years
MTTF of the programmable logic devices (PED)	$MTTF_d\ p$	15 years
MTTF of the drive (D)	$MTTF_d\ d$	10 years
Diagnostic coverage of the sensor comparison	C_s	1
Diagnostic coverage of the PED self tests	C_p	0.9
Diagnostic coverage of the switch-off inputs of the drive	C_i	1
Test rate of all online test	r_t	1/(24 hours)
Repair rate after failure detection	r_r	1/(8 hours)
Demand rate on the safety function	r_d	10/hour
Repair rate after hazardous event	r_{rh}	1/(8 hours)
Mission time (life time)	T_M	10 years

In the following paragraphs the influence of the different parameters on the probability of a dangerous failure per hour will be discussed. The complete compilation of all results is shown in the bar diagram of Figure 24. It should be noticed that in this diagram the probability is depicted in a logarithmic scale. The three β factors for the sensors, the PEDs and the switch-off inputs of the drive have been assigned the same value which is simply called β. Each parameter combination has been evaluated for the β values 0.1%, 5% and 10%. In Figure 24 the β factor is indicated by the colour of the bars.

Implementation of diagnostic tests

A comparison of the results obtained by run 1, run 2, run 7 and run 8 reveals the immense impact of diagnostic coverage on the probability of a dangerous failure. Only the coverage for the PED has been altered. The step from 90% to 99% results in an improvement of about two orders of magnitude (β=0) but a β factor of only 1% will bring all efforts to nothing. The step from 60% to 90% only provides a small progress also for a β of 1% or 5%. Figure 24 shows that at least 90% diagnostic coverage is necessary to achieve SIL 2 with reasonable MTTFs (β=1%). Comparing run 1, run 2, run 3 and run 4 gives an answer to the question whether internal online tests for PEDs are necessary. In run 4 no diagnostics were assumed while in run 3 100% diagnostics for sensors and drive and in run 7 additionally 60% diagnostics for the PED were chosen. Run 7 may be a good example for using three standard programmable logic controllers, implementing 100% diagnostics for the peripheral components and using this systems for safety functions. Figure 24 shows that this version leads to SIL 2 with a β of 1%. As a result we can state that we do not gain much in a triple redundant system using high diagnostic coverage for the PEDs because of the tremendous influence of the common cause factor.

Test rate

All tests in the system are assumed to be executed once within the same cycle. Thus, they all are related to the same test rate (or test interval). Comparing run 1 and run 5 the test rate is reduced from one test per day to one test per week. In run 6 the test rate is one test in 10 seconds. The result of the evaluation clearly shows that there is very low influence of the test rate on the probability of a dangerous failure per hour. The effects are even smaller than those at a dual channel system (see Figure 17).

Failure rate of the subsystems

Considering Figure 24, the impact of the subsystem's failure rates can be studied by a comparison of run 1 (15 years MTTF) , run 9 (30 years MTTF) and run 10 (100 years MTTF). The failure rates of all three types of components are altered in the same manner. It should be noticed that there is a non-linear relationship between the failure rate and the probability of a dangerous failure per hour but that the failure rate has also a big bearing on the SIL.

Comparing run 1, run 11 and run 12 reveals what happens if only the failure rates of the sensors and the drive are altered. A lower or higher MTTF for sensors and drive than for the PED have a small effect on the SIL. This can be explained by the 100% diagnostic coverage for the sensors and the drive. This result justifies to take the same MTTF for all three subsystems in our simulations.

Influence of common cause

The bar diagram of Figure 24 clearly depicts the tremendous impact of the β factor for each parameter combination. The reference combination looses nearly 2 SIL steps due to a common cause factor of 10%. As stated before a β factor of even less than 5% destroys the gain obtained by high diagnostic coverage. Also the gain by better subsystems is strongly limited by the β factor. Due to common cause effects it seems to be hard to achieve SIL 3 with complex electronic systems. It should be noticed that, according to IEC 61508-6, a β factor of 1% may me achievable with diverse redundancy only.

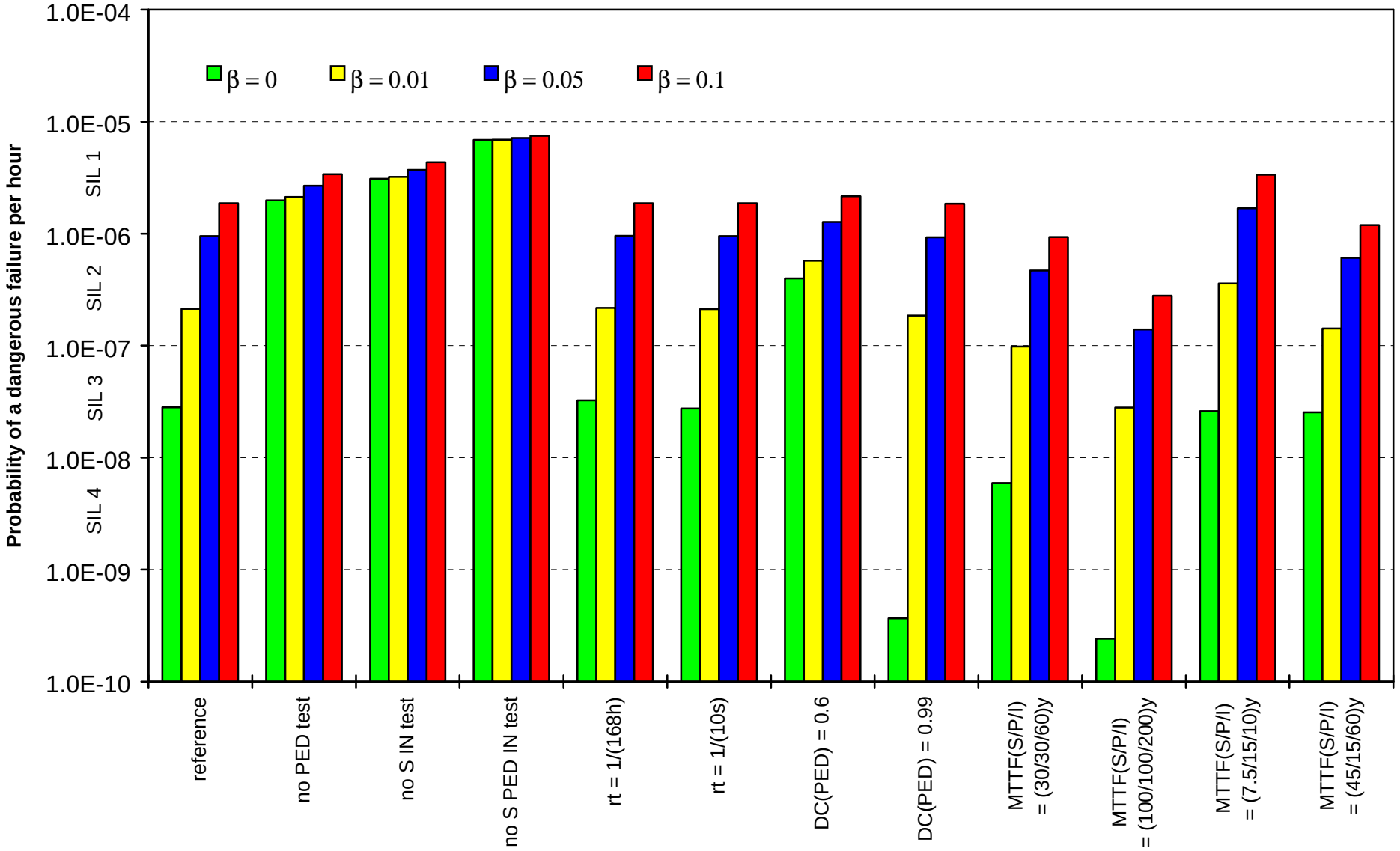


Figure 24: Evaluation result of Markov model TCSC for the symmetric triple channel system

9. Designated architectures of CES for the machinery sector

It could be shown in this report that typical architectures used in machinery which fulfil the requirements of EN 954-1 can be linked to the SILs of IEC 61508. Figure 25 compiles some results obtained by the Markov models presented in the preceding chapters.

In order to make different architectures comparable the input parameters for identical or similar functional units have been set to the same values. In other cases reasonable values have been assumed. (Unifying the input parameters as far as possible will sometimes lead to results differing a little from those presented earlier.)

Unless otherwise noted, the following input data have been assumed:

MTTF of sensors, PEDs and PLCs:	15 years
MTTF of switch-off paths of the drive:	30 years
MTTF of a watchdog:	100 years
MTTF of a relay circuit (two contactors):	50 years
Repair rate (after failure detection or hazardous event):	1/(8 hours)
All test rates of single channel systems:	1/(15 min)
All test rates of dual or triple channel systems:	1/(10 s)
All demand rates of single channel systems:	1/(24 hours)
All demand rates of dual or triple channel systems:	10/hour
Mission time (life time)	10 years

All evaluations have been executed applying the high demand procedure. As shown in Figure 25, SILs 1 to 3 can be achieved by system architectures belonging to different categories. For category B no link to a SIL is possible. With category 2 and suitable tests running in a time interval which is about 100 times smaller than the mean time between demand SIL 1 is achievable. Redundancy without any diagnostic tests running is comparable to category B systems and cannot be used even for SIL 1. Redundancy in mixed technology may achieve SIL 2 if online testing of the periphery is implemented. To achieve SIL 3 a redundant system needs to have 99% diagnostic coverage or a much better MTTF of the subsystems than we presumed for our reference systems. Given appropriate conditions SIL 3 is possible with a triple redundant system.

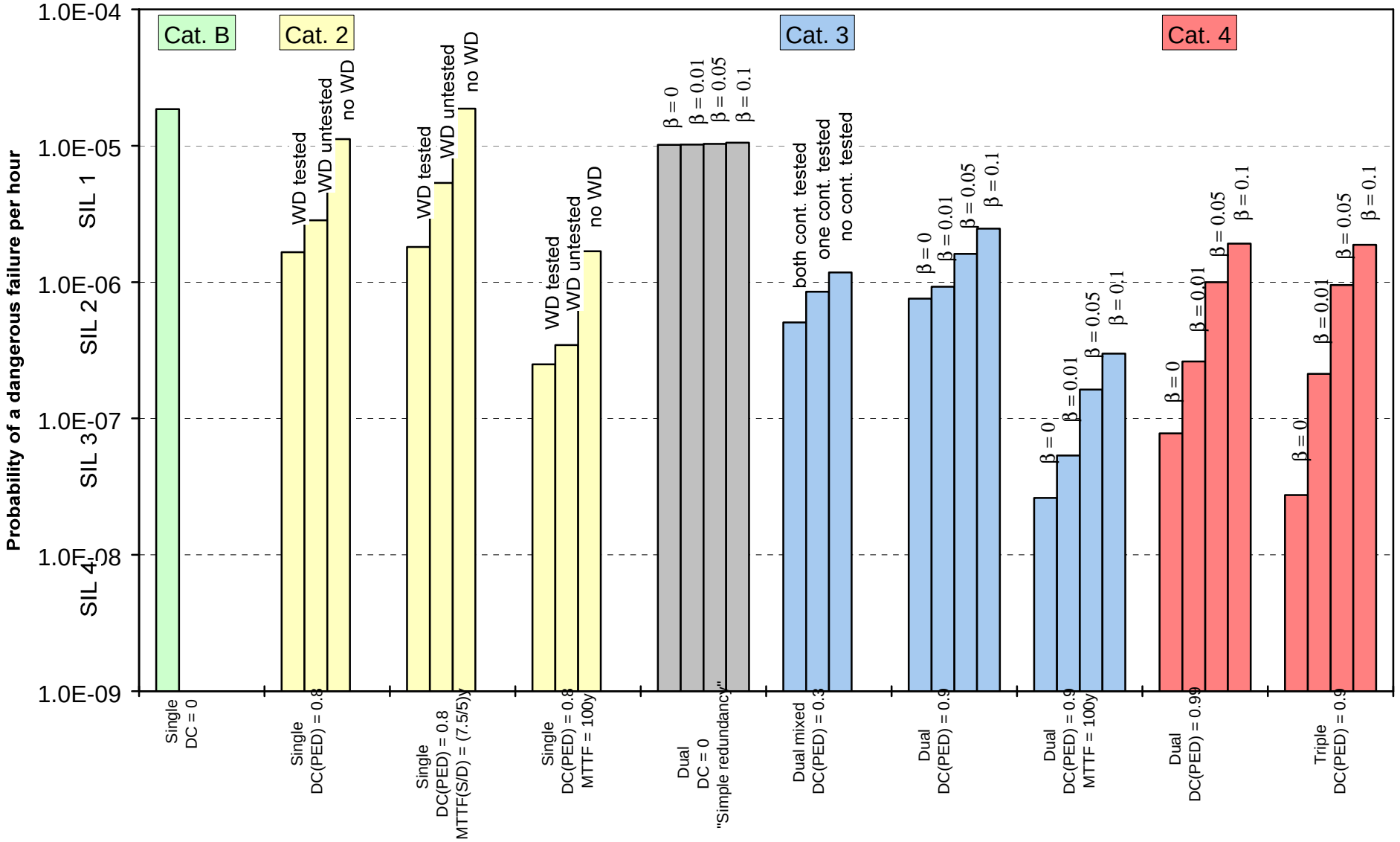


Figure 25: Comparison of different architectures used in machinery

Figure 25 demonstrates that simple doubling of signal processing paths and implementing no online tests ("simple redundancy") does not provide a significant gain if the mission time has a similar order of magnitude as the MTTF of a single channel. Other investigations we did have shown that "simple redundancy" can only have a positive effect if the mission time is one order of magnitude smaller than the MTTF. For simple systems (e.g. contactors or valves) which can be proof tested once a year (i.e. 100% diagnostic coverage for all subsystems) simple doubling of the hardware may be useful. For complex subsystems like ASICS or PEDs simple doubling is only useful if the MTTF is one order of magnitude bigger (possible e.g. for some ASICS) than the mission time (life time) of the safety system. In all other cases online diagnostics are essential also in redundant safety-related systems.

These results compiled in Figure 25 could be helpful for standardisation. A link may be drawn between SILs and the categories for so called designated architectures. The architectures introduced in this chapter are proposed to be considered as designated architectures for the machinery sector. A manufacturer who can prove that his architecture is equivalent to one of the designated architectures only has to determine the $MTTF_{dangerous}$ of his the subsystems, to determine the diagnostic coverage of the online tests and, in case of redundant systems, estimate the common cause factor. Then he may derive the SIL out of a table. As an example, a table of this kind is presented in the following. This table is the compilation of results achieved by choosing particular input data. New Markov modelling will be necessary only if system architectures and/or parameters for the subsystems are used, which are not listed in the table.

There are several data banks which can be employed to determine the MTTF of hardware components, for example [11], [12], [13]. Standardisation e.g. could demand for the use of one of these appropriate data sources in order to attain comparable results. The diagnostic coverage can be determined using the failure model in annex A of part 2 of IEC 61508 [1]. Part 6 of IEC 61508 may be helpful to estimate the common cause factor β. Standardisation could specify one methodology for estimating the CCF. With this proposal a link between the two standards IEC 61508 and EN 954-1 is possible. It is not a fixed link between categories and SILs but it is applicable without individual quantification of control systems.

Table: Possible designated architectures for machinery

SIL	System Architecture	Mean Time to dangerous Failure $MTTF_d$ (years)	CCF β (%)	Diagnostic Coverage (each Channel) (%)	Cat.
		In/Processing/Out		In/Processing/Out	
-	Single PE, Single I/O	15/15/30	-	0/0/0	**B**
	Single PE, Single I, Ext. WD(u/t)	15/15/30	-	0/60/0	**B**
	Dual PE, Dual I/O, 1oo2	15/15/30	5	0/0/0	**?**
1	Single PE, Single I, Ext. WD(u/t)	15/15/30	-	100/60/100	**2**
	Single PE, Single I, Ext. WD(u/t)	7.5/15/10	-	100/60/100	**2**
	Dual PE, IPC, Dual I/O, 1oo2	15/15/30	5	100/60/100	**3**
	Dual PE, IPC, Dual I/O, 1oo2	15/15/30	10	100/90/100	**3**
	Dual PE, IPC, Dual I/O, 1oo2	45/15/60	10	100/90/100	**3**
	Triple PE, IPC, Triple I/O, 1oo3	15/15/30	5	100/60/100	**3**
	Triple PE, IPC, Triple I/O, 1oo3	15/15/30	10	100/90/100	**4**
2	Single PE, Single I, Ext. WD(t)	15/15/30	-	100/90*/100	**2**
	Dual PE, IPC, Dual I/O, 1oo2	15/15/30	1	100/90/100	**3**
	Dual PE, IPC, Dual I/O, 1oo2	30/30/60	5	100/90/100	**3**
	Dual PE, IPC, Dual I/O, 1oo2	7.5/15/10	1	100/99/100	**4**
	Mixed Dual Processing, Dual O, 1oo2	∞/(15/100)/(15/100)	-	0/(30/100)/(100/100)	**3**
	Triple PE, IPC, Triple I/O, 1oo3	15/15/30	1	100/60/100	**3**
	Triple PE, IPC, Triple I/O, 1oo3	100/100/200	10	100/90/100	**4**
3	Single PE, Single I, Ext. WD(t)	30/30/60	-	100/99*/100	**2**
	Dual PE, IPC, Dual I/O, 1oo2	45/45/90	1	100/99/100	**4**
	Triple PE, IPC, Triple I/O, 1oo3	100/100/200	1	100/90/100	**4**

Conditions for single channel systems:

All test rates: 1/(15 min)
Demand rate: 1/(24 h)
Repair rate: 1/(8h)
Mission time (life time): 10 years

$MTTF_d$ of watchdog: 100 years
$MTTF_d$ of switch-off path for watchdog: equal to normal switch-off path
WD(u/t): Watchdog and pertinent switch-off path untested or tested
WD(t): Watchdog and pertinent switch-off path tested

(* not achievable by simple watchdog)

Conditions for dual or triple channel systems:

All test rates: 1/(24h)
Demand rate: 10/h
Repair rate: 1/(8h)
Mission time (life time): 10 years

$MTTF_d$ of output sensor of mixed system: 15 years (output sensor not tested)

IPC: Inter-processor communication

10. Conclusions

During the STSARCES research project WP 2.1 wanted to execute systematic investigations on the effect of the test time interval on the Safety Integrity Level (SIL). In addition the concept of a proof test making the control system “as good as new” is a theoretical model which is not suitable for validation of complex electronic systems (CES) in the machinery sector. Therefore we determined the average probability of a dangerous failure per hour or the average probability of a failure on demand during the typical lifetime of a control system i.e. 10 years. (In the report the life time is referred to as the “mission time”.) It could be shown that without doing proof tests the demand had to be introduced into our Markov model so that one of the states is the hazard state in case of a demand arising at a point of time where the safety function cannot be performed by the control system due to an internal failure. With this model we could determine the SIL for the three modes of operation according to IEC 61508. The results are comparable and the SIL of a CES does not depend on the mode of operation. To determine the influence of the test time interval in our Markov models intermediate states had to be introduced where faults are present but online tests did not detect them because they have not yet been executed. With this models we could show that the test time interval is connected to the mean time to demand in a single channel system and to the mean time to dangerous failure (MTTF) of the individual channels for a multi channel system. These results can be generalised for all CESs. The generalisation justifies a dramatic simplification of Markov modelling which is necessary to handle existing CES in the machinery sector.

This report also demonstrated that a link between the categories (CAT) of EN 954-1 and the SILs of IEC 61508 cannot be made by a fixed relation. If we interpret a category as an architecture with a specific diagnostic coverage, a SIL can be determined using several assumptions which are common in the machinery sector and giving the MTTFdangerous as an input parameter. For realistic input data the fixed relation of the past can be derived but this is only one possibility. It can be shown that SIL 3 is hard to achieve for a mission time of 10 years with dual redundancy only.

The concept of designated architectures was developed on the base of modelling of the different typical architectures for the machinery sector. This concept which had been proposed to IEC 61508 several years ago was rejected there because the standard is generic and it was impossible to find generic architectures for all application sectors. However, this concept seems to be usable in a sector specific standard as IEC 62061 [14]. This is the reason why the authors propose this concept as an link between CATs and SILs and as an input to IEC 62061. The concept seems to be realistic to be accepted by machine manufacturers because it strongly simplifies the quantification of CES in the machinery sector.

It should be noticed that this report can only be useful in connection with the other reports of the STSARCES project. “Quantification of the hardware” is only one small step in the design and validation of safety related systems. The report of WP 2.2 [3] will give the basis to determine the diagnostic coverage for each subsystem. The aspect of systematic failures cannot fully be covered by the β factor model. The outputs of WP 1 “Software” is essential to cover the aspect of systematic failures in CES [15]. A validation of CES can only be done in a combination of different techniques as described in the reports of WP 3 [16].

11. References

[1] IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems 7 Parts: CEI/IEC 61508-1: 1998; CEI/IEC 61508 3: 1998; CEI/IEC 61508-4: 1998; CEI/IEC 61508-5: 1998; IEC 65A/294/FDIS and IEC 65A/295/FDIS.

[2] EN 954-1: 1996 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design. Brussels, December 1996.

[3] Jan Jacobson; Jacques Hérard: Methods for fault detection. STSARCES WP 2.2. Borás, September 1999.

[4] William M. Goble: Evaluating Control Systems Reliability. Instrument Society of America (ISA), Research Triangle Park, North Carolina 1992.

[5] Alessandro Birolini: Qualität und Zuverlässigkeit technischer Systeme. Springer, Berlin 1991.

[6] INRS, Dept. Ingénierie des Equipementes de Travail, Lab. Sûreté des systèmes Electroniques: STSARCES WP 1.2 Software Quality and Safety Requirements, Tools for Software Fault Avoidance. Vandoeuvre, December 1999.

[7] Reliability Analysis Center (RAC): Fault Tree Analysis Application Guide. Rome, NY 1990.

[8] CARMS (Computer Aided Rate Modeling and Simulation). DAINA, Columbia Heights, MN 1994.

[9] Werner Kleinbreuer; Franz Kreuzkampf; Karlheinz Meffert; Dietmar Reinert: Categories for safety-related control systems according to EN 954-1. BIA-Report 6/97e. Sankt Augustin, September 1999.

[10] Heinz Gall; Klaus Kemp: Einsatz und Wirksamkeit von Programmlaufüberwachungen. In: atp40(1998) Oldenbourg. p. 40 – 48.

[11] FARADIP.THREE (Failure Rate and Failure Mode Data Bank and Failure Mode and Effect Analysis Package). Technis, Tonbridge, Kent UK 1997.

[12] Reliability Analysis Center (RAC): Automated Databook (Electronic Parts Reliability Data, Nonelectronic Parts Reliability Data). Rome, NY 1994 - 1997.

[13] SN 29500 Failure Rates of Components, Part 1 – 7, Part 9 – 10. Siemens AG, ZT TN Corporate Functions Technical Regulation and Standardization, Munich and Erlangen 1982 – 1999.

[14] IEC 62061 Functional safety of electrical, electronic and programmable electronic control systems for machinery: Working group document 1999.

[15] INRS, Dept. Ingénierie des Equipementes de Travail, Lab. Sûreté des systèmes Electroniques STSARCES WP 1: Software Quality and Safety Requirements Vandoeuvre, December 1999.

[16] Timo Malm; Maarit Kivipuro: Safety Validation of Complex Components – Validation by Analysis. STSARCES WP 3.1. Tampere, September 1999.