Reliability Analysis of Safety Systems Subject to Multiple Testing Levels

Siegfried Eisinger
DNV GL, Norway

Luiz Fernando S. de Oliveira, Joaquim Domingues do Amaral Netto,
Luciana M. Chame and Raphael Fernandes
DNV GL, Brazil

Abstract

Currently some components of complex safety systems may be subject to multiple testing levels. That is the case of BOPs of which some key components may be subject to up to a four-level functional and integrity testing scheme, in addition to online diagnostics. Such multiple-testing-level (MTL) schemes impose additional requirements with their associated computational difficulties on the assessment of the SIS PFDs. In this paper we investigate possible solution methods for the calculation of PFD of safety systems subject to MTL, assess the differences in results of PFD obtained with various methods (analytical equations, FT, numerical and simulation) and analyze to which degree they give conservative or optimistic results.

1. INTRODUCTION

It is well known among safety practitioners that the reliability of safety critical systems subject to low number of demands is strongly dependent on a rigorous testing scheme of such systems. The introduction of IEC-61508 [1] in 1998 introduced formal requirements for the performance of such tests for the so-called safety instrumented systems (SIS) and proposed several methods for the evaluation of the PFD (Probability of Failure on Demand) of SIS as a function of their testing schemes.

Currently, most typical SIS found in industrial installations are subject to two levels of testing: online diagnostics and periodic tests. Online diagnostics conducted by fault detection systems are performed on a quasi-continuous basis and are capable of identifying an important fraction of otherwise hidden failures that could, if not duly identified, lead to dangerous failures of the safety system, i.e., its failure to perform the assigned safety function when demanded by a plant hazardous event. By its turn, periodic tests are typically manually performed at periodic times according to a pre-determined scheme.

More recently the so-called partial stroke testing (PST) [2, 3] has been introduced to allow periodic testing of safety block valves to be done without interfering with the continuity of the plant operation. Nevertheless, such PSTs are inherently incomplete, in the sense that only a fraction of the valves failure modes can be tested without actually blocking the process flow. Therefore, there remains a need to perform “complete tests” on a periodic basis, but because of the PSTs, the period can then be extended while maintaining a low value for the SIS PFD. Therefore, the introduction of PST implies a third testing level for the SIS: the first is “online diagnostic”, the second is PST, and the third is the complete test.

In many cases one cannot guarantee that the complete tests are really perfect, that is, that they are capable of detecting all failure modes such as rendering the SIS to a perfectly good state after the test (and repair, if some failure is detected by the test). In many cases, the complete test is imperfect, meaning that some residual failure remains undetected (hidden)

even after the complete test. In these cases, the full failure detection will only be achieved upon occurrence of a true demand event. Therefore, in terms of PFD assessment, the consideration of test imperfection implies that during the period between true demands of the SIS there will be a residual hidden failure rate that will give a small contribution to the average PFD of the SIS. This introduces a fourth testing level, which is that of the true demand event.

Some more complex safety systems may be subject to even more than the above levels of testing. That is the case of Blowout Preventers (BOPs) currently in operation in various parts of the world, of which some key components may be subject up to a five-level testing scheme, such as:

1. Online diagnostics,
2. Weekly testing,
3. Bimonthly testing,
4. Semi-annually testing, and
5. Overall revision (typically at five-year periods).

Such multiple-testing-level schemes impose additional requirements (with their associated computational difficulties) on the assessment of the SIS PFDs. They are addressed in this paper.

The meanings of the abbreviations used in this paper are summarized in Table 1.

Table 1 - Abbreviations

Abbreviation	Meaning
BOP	Blowout Preventer
CCF	Common-Cause Failure
DC	Diagnostic Coverage
FT	Fault Tree
KooN	K-out-of-N configuration
MTL	Multiple Testing Levels
MTTR	Mean Time to Repair
PFD	Probability of Failure on Demand
PST	Partial Stroke Testing
RBD	Reliability Block Diagram
SIL	Safety Integrity Level
SIS	Safety Instrumented System

2. OBJECTIVES OF THE WORK

In this paper we investigate possible solution methods for the calculation of PFD of safety systems subject to multiple testing levels (MTL), develop approximate analytical equations for the evaluation of the PFD of safety systems subject to MTL based on simplified RBDs, assess the differences in results of PFD values obtained with various methods (analytical equations, FT, numerical integration and Monte-Carlo simulation) and analyze to which degree they give conservative or optimistic results. It is shown that with proper modelling all methods give acceptable results, that is, within acceptable differences between them. We also introduce a discussion (without exhausting it in anyway) on the meaning of common-cause failures for safety systems subject to the conditions stated in this paper.

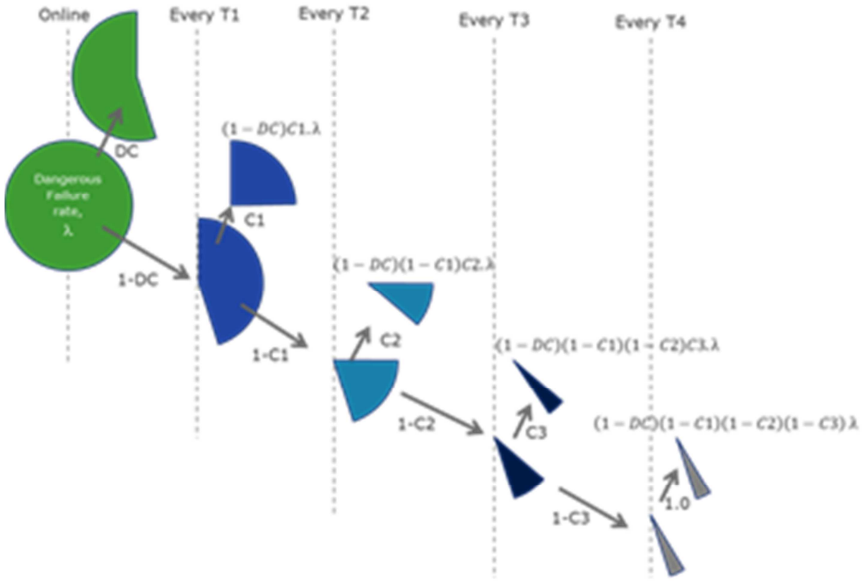


Figure 1 - Failure rate splitting at each testing level

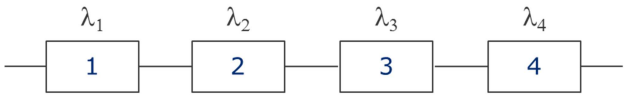
3. EVALUATION OF THE PFD OF A SIS SUBJECT TO MULTIPLE TESTING LEVELS

3.1 Basic Assumptions

Three basic assumptions are used in this paper for the evaluation of the PFD of a SIS subject to MTL.

First assumption: each testing level has a coverage factor that implies the detection of a certain fraction of the failure modes included in the total failure rate of a component (the coverage factor of the last testing level is always equal to one). Therefore, the total dangerous failure rate is decomposed in several failure rates as indicated in Figure 1. Each component can be thought as a series of subcomponents as indicated in the RBD of Figure 2.

Second assumption: when a failure of a component is detected (by the online diagnostics system or by a periodic test), the operating system is immediately stopped and remains out of operation during the repair of the failed protection component. Therefore there is no contribution of the detected failure modes to the PFD of the protection system. Most systems are not operated this way, but this is generally true for drilling operations with BOPs. This assumption can be easily relaxed but the corresponding analytical expressions become too large.



$\lambda_1 = \lambda \times C_1$
$\lambda_2 = \lambda \times (1 - C_1) \times C_2$
$\lambda_3 = \lambda \times (1 - C_1) \times (1 - C_2) \times C_3$
$\lambda_4 = \lambda \times (1 - C_1) \times (1 - C_2) \times (1 - C_3)$

Figure 2 - RBD representation of a component subject to four testing levels

Third assumption: the higher order testing levels are multiple of the time between tests of the first test level. This is expected in practice as it minimizes the overall number of tests and of possible process interruptions for testing. This assumption is drawn uniquely for the development of the approximate analytical equations.

3.2 Models for PFD Evaluation of Systems Subject to MTL

The definition of the SIL levels in IEC 61508 [1] uses the average PFD of the system, which is the same as the average value of the instantaneous unavailability function over a certain test period. The instantaneous unavailability at time t, or the value of PFD(t), is by definition the probability that the system is unavailable at time t. As indicated by Apostolakis and Chu [4] a long time ago, the average unavailability of a periodically tested safety system is not really a probability. Therefore strictly speaking, the Theory of Probability does apply to instantaneous unavailabilities but not to average unavailabilities (In most cases, this "error" does not introduce very important differences in the numerical results). The latter used to be usually done in most PFD calculations, but this has started to change in recent years.

As indicated in IEC 61508 [1] there are several methods that can be used to evaluate the PFD of a SIS. In this paper we work with the following methods:

1. Numerical integration of time-dependent equations, PFD(t), obtained from SIS RBD modelling;
2. Approximate analytical equations derived from SIS RBD modelling;
3. Fault tree analysis and
4. Monte Carlo simulation.

3.3 Some Comments on the Above Methods

The numerical method is not explicitly mentioned in the standards but it has been known from a long time, its first ever implementation having been that of the FRANTIC code [5]. It is based on the numerical integration and averaging of the time-dependent system PFD(t) which is obtained by the logic combination (probability rules) of the time-dependent unavailability functions of the components.

The approximate analytical equations for protection systems subject to MTLs derived in this paper are obtained from approximations using RBD representations expressing the logic arrangements of the components. The MTLs of each component are expressed by the series RBD as exemplified in Figure 2 for a four-testing level case. They are extensions of previously derived equations for KooN configurations by Oliveira and Abramovitch [6]. Several other analytical equations for KooN configurations are publicly available (the most recent ones being those of Jahanian [7] and Innal et al [8] although not for systems subject to MTL.

Fault tree analysis has been around since the 60´s and was extensively used in the Reactor Safety Study [9]. Until quite recently most fault tree programs were based on the average values of unavailability of each component which were combined using the probabilistic rules for the various logic configurations of the components. In fact the vast majority had algorithms for the determination of the minimal cut sets, which were then combined by some upper-bound method to give the PFD of the system. The more modern FT programs use binary decision diagrams for the logic part and numerical integration and averaging of the

corresponding time-dependent unavailability functions. The GRIF-Tree program [10] used in this paper is one of the best examples of the modern FT programs.

There exists a variety of good Monte Carlo simulation methods and programs that can be used for determining the PFD of safety systems. Their biggest advantage is their flexibility to model the vast majority of the situations found in practice. Their main disadvantage is the computational time needed to obtain precise results for the extremely reliable safety system configurations (PFDs of the order of 10^{-6} or less). In this paper we used a Harel State formulation [11] implemented in the Extendsim software [12].

3.4 Using the Numerical Method

We hereby demonstrate the use of numerical method by starting from the development of a model for a single component subjected to four testing levels. Then extend it to the case of 1oo2 and 2oo3 configurations. The generalization to KooN is then explained.

3.4.1 *Application of the Numerical Method: One Component Subject to Four Testing Levels*

The general representation of the time-dependent unavailability, PFD(t), of a single component subject to periodical tests (a single testing level) is indicated in Figure 3. The function in Figure 3 can be analytically expressed by the following equations:

$$\begin{aligned} PFD(t) &= 1-\exp(-\lambda.t) && 0 < t < T \\ PFD(t) &= 1-\exp[-\lambda.(t-T)] && T < t < 2T \\ PFD(t) &= 1-\exp[-\lambda.(t-2T)] && 2T < t < 3T \\ &\ldots \\ PFD(t) &= 1-\exp\{-\lambda.[t-(n-1)T]\} && (n-1).T < t < n.T \end{aligned} \quad (1)$$

A more compact analytical representation is given by:

$$PFD(t) = 1-\exp[-\lambda.Mod(t,T)] \qquad 0 < t \leq n.T \quad (2)$$

where

$$Mod(t,T) = t - Int(t/T).T] \quad (3)$$

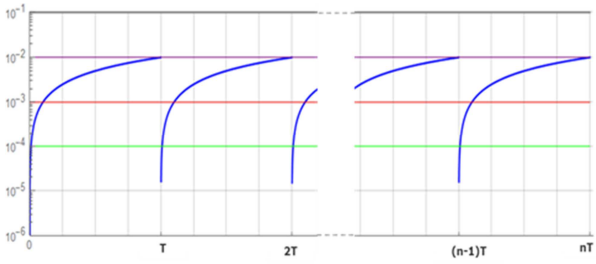


Figure 3 – Graphical representation of PFD(t) of one component under periodical testing (single testing level)

As indicated in Section 2.1, the logical representation of the four testing levels is that of an RBD with each of the four testing levels considered as an independent component of a series system, as presented in Figure 2. Hence to obtain the PFD(t) of the component subject

to four testing levels, one must use the probabilistic expression of the union of the unavailabilities of the four testing levels:

$$PFD_{comp4TL}(t) = 1-[1-PFD_1(t)]\times[1-PFD_2(t)]\times[1-PFD_3(t)]\times[1-PFD_4(t)] \quad (4)$$

To simplify the graphical representation and better explain the numerical method, let us show an example where T1=1000h, T2=4000h, T3=8000h and T4=16000h. The specific values of the failure rate and of the coverage coefficients for the various testing levels are not important at this point. For this case, the PFD(t) for each of the four testing levels are presented in Figure 4.

Applying Eq.(4) by numerically combining the functions in Figure 4, one obtains the PFD(t) of the component subject to the four testing levels, resulting in the function shown in Figure 5. To obtain the average value of PFD_{1avg} for this component all we have to do is to perform a numerical integration of the function in Figure 5 from 0 to 16000h. This above numerical procedure gives the most accurate possible value for this average (the accuracy being governed by the numerical integration method).

3.4.2 *Application of the Numerical Method to Systems with Components Subject to Four Testing Levels*

The general representation of the time-dependent unavailability for one component, $PFD_1(t)$, subject to MTL is shown in Figure 5. Now suppose we would like to obtain the PFD(t) for a 1oo2 system and then obtain its average value. The logical function in this case is the intercession of the failures of the two components, and the corresponding probabilistic rule is the product of the PFD(t) of the two components. Thus by numerically multiplying $PFD_1(t)$ by itself (assuming the two components are identical), one obtains the $PFD_{1oo2}(t)$ as the function shown in Figure 6. The average value $PFD_{1oo2avg}$ is simply obtained by performing the numerical integration of the function in Figure 6 from 0 to 16000h. Again, this procedure gives the most accurate possible value of PFD1oo2avg.

To generalize it to a KooN system, one must perform the numerical application of the known formula for the PFDKooN(t) given in Eq.(5) below, where PFD1(t) is the function for the component subject to the four specified testing levels given in Figure 5.

$$PFD_{KooN}(t) = \sum_{i=N-K+1}^{N} C_i^N \left[PFD_1(t)\right]^i \left[1-PFD_1(t)\right]^{N-i} \quad (5)$$

The numerical method presented above can be used to any situation where the PFD(t) of the components can be expressed numerically. The example above was presented for two identical components because this is the usual case of KooN systems, but it is by no means limited to that situation. We have implemented the numerical method in Excel VBA and Wolfram Mathematica, and both gave identical results to a very high level of accuracy.

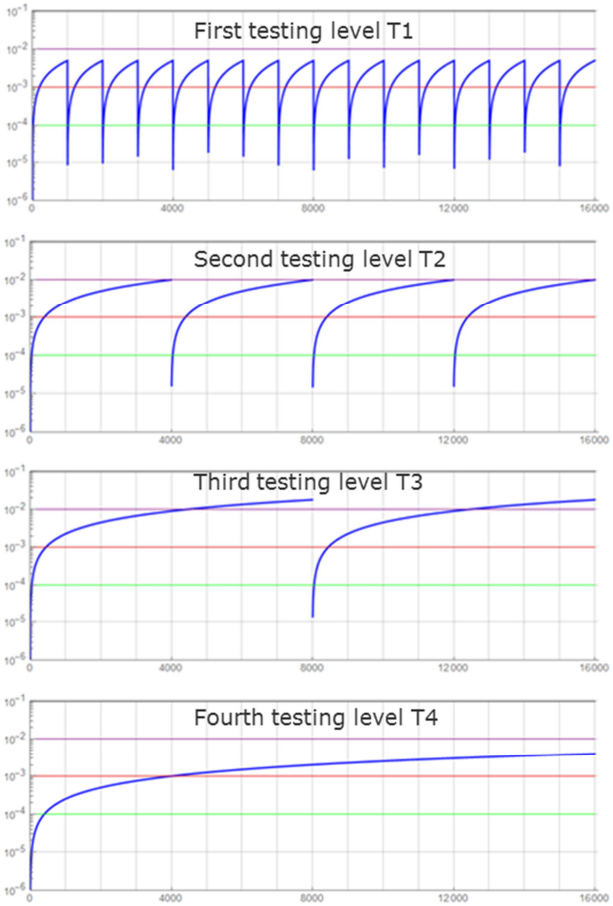


Figure 4 – PFD(t) functions for one component for each of the four testing levels T1 to T4

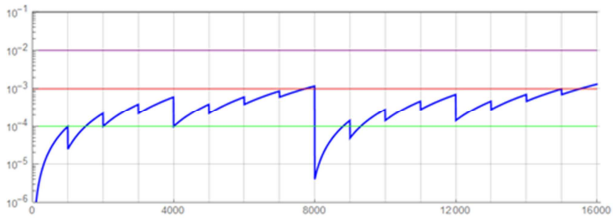


Figure 5 – PFD1(t) for one component subject to the specified four testing levels

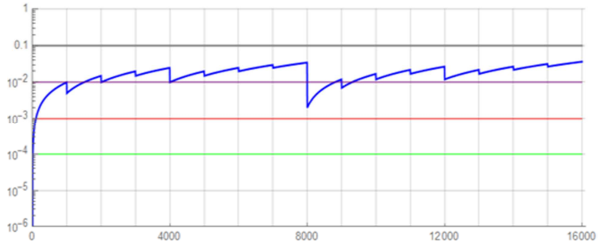


Figure 6 – PFD1oo2(t) for a 1oo2 system whose components are subject to the specified four testing levels

3.5 *Approximate analytical equations for systems with components subject to MTL*

We have developed a general approximate equation for the evaluation of the PFD of a KooN system with components subject to up to five testing levels. Since the general equation is too lengthy to show in this paper we will only present here its application to the case of a 1oo2 and 1oo3 systems with three testing levels. They are given below:

$$PFD_{1oo2} = \lambda_1^2 \frac{T_1^2}{3} + \lambda_2^2 \frac{T_2^2}{3} + \lambda_3^2 \frac{T_3^2}{3} + \\ + \frac{1}{2}\lambda_1 T_1 * \lambda_2 T_2 + \frac{1}{2}\lambda_1 T_1 * \lambda_3 T_3 + \frac{1}{2}\lambda_2 T_2 * \lambda_3 T_3$$

$$PFD_{1oo3} = \lambda_1^3 \frac{T_1^3}{4} + \lambda_2^3 \frac{T_2^3}{4} + \lambda_3^3 \frac{T_3^3}{4} + \\ + \lambda_1 \lambda_2^2 \frac{T_1 T_2^2}{2} + \lambda_1^2 \lambda_2 \frac{T_1^2 T_2}{2} + \lambda_1 \lambda_3^2 \frac{T_1 T_3^2}{2} + \\ + \lambda_1^2 \lambda_3 \frac{T_1^2 T_3}{2} + \lambda_2 \lambda_3^2 \frac{T_2 T_3^2}{2} + \lambda_2^2 \lambda_3 \frac{T_2^2 T_3}{2} \\ + 3\lambda_1 \lambda_2 \lambda_3 \frac{T_1 T_2 T_3}{4}$$

The formation law for the development of such equations can be easily explained. From the 1oo2 case, it can be seen that the first three terms correspond to average values of the combination of two failures of the same testing level (T1 to T3). The other three terms correspond to two by two combinations of the products of the average unavailability values due to different testing levels. The latter three terms contain the approximations because the integration of the time-dependent piecewise functions cannot be analytically expressed. Similar explanation can be given for the 1oo3 case except that now there are more combinations to be considered as you need three failures to make the system unavailable.

The general KooN equation is developed along the same line, namely, by combining the failures of each testing level to form the N-K+1 failures needed to make the system unavailable.

Common-mode failures can be easily introduced by using the beta-factor model. The general assumption here is that only dependent failures among the failures due to the same testing levels are considered (first three terms of the equations), and not a more generic common-cause failure which could also occur between the combinations of failures of different testing levels. This assumption is, of course, debatable.

3.6 *Applying Fault Trees to the Modelling of Systems with Components Subject to MTL*

Most existing FT software programs contain a KooN type gate where the user specifies the values of K and N and the program constructs the proper logic of the specified KooN configuration using the user specified basic events. In the case of application to components subject to MTL, each input to the KooN is formed by an OR gate with the failures at each testing level as its input. An example of FT for a 1oo2 system with four testing levels is shown in Figure 7.

The way the different FT programs actually quantifies the PFDavg of the KooN system varies among the existing programs. As indicated before, in this work we used GRIF-

Tree [12] to solve the FTs for all configurations, which is undoubtedly one of the most advanced FT programs available in the market. It is not clear from the User Manual how GRIF-Tree performs the calculations, but it indicated that the Albizia computational engine is used to solve the fault tree. A recent book just published by Aubry & Brinzei [13] explains in details the algorithm used in Albizia which is based on the application of binary decision diagrams (BDD). Since in GRIF-Tree the results are also presented in time-dependent format it can be inferred that it uses some kind of numerical solution similar to the numerical method shown in Section 2.4.

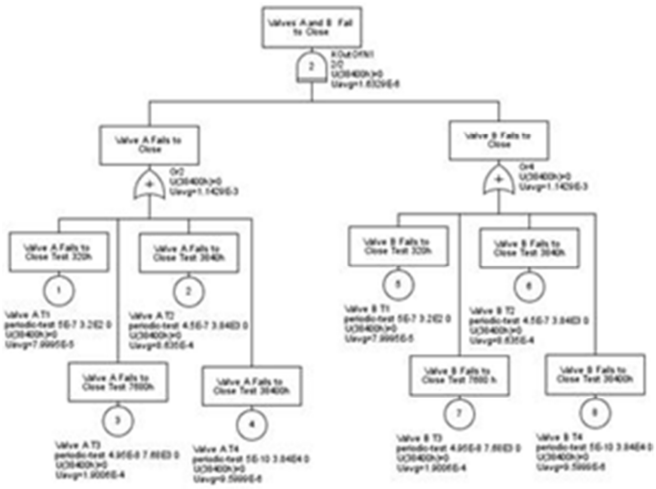


Figure 7 – Example of FT for a 1oo2 System with components subject to four testing levels

3.7 *Application of the Simulation Method to Systems with Component subject to MTL*

The simulation model can be readily constructed using a general finite-state model. State models can become rather involved and hard to maintain. Therefore the components have been modelled as Harel State charts [11]. The State chart modelling paradigm has previously been implemented in our custom library of the general simulator ExtendSim [12]. Special features of hierarchical state modelling which are used here are hierarchical variable handling, where the scope of variables is only within its own hierarchy. In this way, the periodic test times Ti, and the actual time when the last test was performed are variables global to the whole model, while the failure rates λi and the diagnostic coverage factors Ci of each testing level are local to each component (though they are all equal in our simplified case). Figure 8 shows the state chart sub-model of a component with three testing levels in addition to the online diagnostics. As indicated by Assumption #2 in Section 2.1, component repair is not considered here; therefore there are no repair states in the model.

In the initial state the component is working. The type of failure is randomly chosen according to the failure rate λ and the coverage factors Ci , deciding which state transition U0, ..U3 is chosen. The component stays in state Ui until the next test of level i occurs, when it is immediately transferred to the working state and starts the next loop. As a component state the working state is used which is informed to the super-model as ‘WorkingOut =True/False’. Components are then combined into systems according to the logic of the system configuration. Figure 9 shows the system level model (the super-model with respect to the components) with up to four components (Comp1 to Comp4) of the type shown in Figure 8 and the possibility of Common Cause Failures (CCF). The system can be configured using the parameters k and N and by excluding/including CCF (besides changing the

component parameters). Statistics on system failures are collected in the block ‘System’, while detailed component statistics are available in the component sub-models.

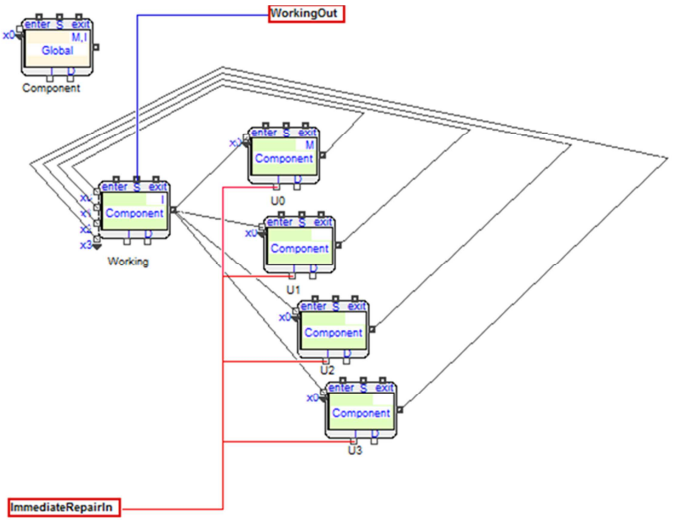


Figure 8 - State-based simulation sub-model of a component with 3 testing levels

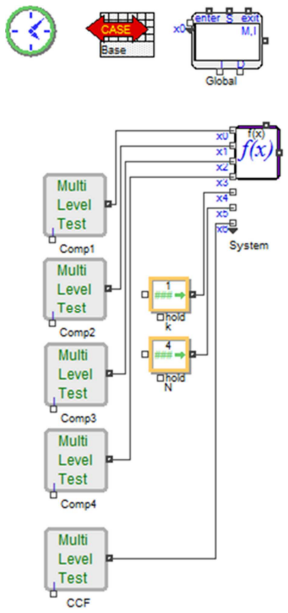


Figure 9 - System model of up to four components in KooN configuration and the possibility of CC Failures

3.8 *The Consideration of CCF*

As indicated in Figure 3, a component subject to MTL is here represented as a series system of “independent components” each one detectable at a given test level. They can also be thought as different failure modes of the same component, which seems to be a better idea. The latter is commonly used in the construction of fault trees where the failure of a component is represented by an OR gate with its different independent failure modes listed as

basic events of the gate. By adopting this representation we introduce CCF contributions for the failure modes at each testing level. Hence, using the Beta-Factor Model for CCF, Eqs. (6) and (7) must be modified by multiplying each failure rate by (1-β), and by adding the following CCF term to both equations (actually this CCF term would be the same for any KooN configuration with three testing levels)

$$CCF_{KooN\_3}(t) = \beta\lambda_1 \frac{T_1}{2} + \beta\lambda_2 \frac{T_2}{2} + \beta\lambda_3 \frac{T_3}{2} \qquad (8)$$

In Eq.(8) we have considered the same value of beta for all three testing level, but of course, they could be different for each testing level. One could also apply a different CCF model or use different beta factors for different redundancy levels.

4. COMPARISON OF RESULTS

4.1 *Results Obtained without CCF*

Results obtained with the different methods for systems with components subject to MTL are presented in this section. The value of 1.0E-6/h was used for the dangerous undetected failure rate (λ_{DU}) for all components. Values of the test periods and the corresponding coverage factors are given in **Table 2**.

Table 2 – Data used for comparison of results

Test Levels	Test Period Parameter	Test Period (hours)	Coverage Coefficient
One Test Level	T1	38400	1
Two Test Levels	T1	320	0.5
	T2	38400	1
Three Test Levels	T1	320	0.5
	T2	3840	0.9
	T3	38400	1
Four Test Levels	T1	320	0.5
	T2	3840	0.9
	T3	7680	0.99
	T4	38400	1

A comparison of the results obtained with the different methods for various cases of KooN configurations from 1oo1 to 3oo4 and for the number of testing levels varying up to 4 are shown in **Table 3**.

Table 3 – Comparison of results obtained with different methods for various systems configurations and various testing levels

Case	MTL Appr. Eq.	Nmerical	GRIF-FT	Extend	Ratio MTL/ Num.	Ratio MTL/FT	Ratio MTL /Extend
1oo2_1	4,92E-04	4,78E-04	4,78E-04	4,79E-04	2,9%	3,0%	2,6%
1oo2_2	1,24E-04	1,23E-04	1,23E-04	1,23E-04	0,8%	1,1%	0,8%
1oo2_3	4,18E-06	4,24E-06	4,24E-06	3,98E-06	-1,4%	-1,3%	4,8%
1oo2_4	1,57E-06	1,63E-06	1,63E-06	1,67E-06	-3,7%	-3,9%	-6,4%
1oo3_1	1,42E-05	1,35E-05	1,35E-05	1,41E-05	5,2%	5,0%	0,7%
1oo3_2	1,80E-06	1,76E-06	1,76E-06	1,81E-06	2,3%	2,4%	-0,6%
1oo3_3	1,01E-08	1,04E-08	1,04E-08	8,71E-09	-2,9%	-3,0%	13,8%

Case	MTL Appr. Eq.	Nmerical	GRIF-FT	Extend	Ratio MTL/ Num.	Ratio MTL/FT	Ratio MTL /Extend
1oo3_4	2,40E-09	2,60E-09	2,61E-09	2,68E-09	-7,7%	-8,1%	-11,7%
2oo3_1	1,48E-03	1,41E-03	1,41E-03	1,40E-03	5,0%	5,3%	5,4%
2oo3_2	3,73E-04	3,65E-04	3,64E-04	3,66E-04	2,2%	2,4%	1,9%
2oo3_3	1,26E-05	1,27E-05	1,27E-05	1,23E-05	-0,8%	-0,7%	2,4%
2oo3_4	4,71E-06	4,88E-06	4,89E-06	4,83E-06	-3,5%	-3,7%	-2,5%
1oo4_1	4,35E-07	4,08E-07	4,08E-07	4,30E-07	6,6%	6,6%	1,1%
1oo4_2	2,78E-08	2,69E-08	2,69E-08	2,77E-08	3,3%	3,4%	0,4%
1oo4_3	2,60E-11	2,74E-11	2,75E-11	***	-5,1%	-5,3%	-
1oo4_4	3,91E-12	4,43E-12	4,47E-12	***	-11,7%	-12,6%	-
2oo4_1	5,66E-05	5,29E-05	5,29E-05	5,41E-05	7,0%	7,1%	4,4%
2oo4_2	7,20E-06	6,95E-06	6,95E-06	7,18E-06	3,6%	3,6%	0,3%
2oo4_3	4,04E-08	4,16E-08	4,16E-08	3,83E-08	-2,9%	-2,8%	5,2%
2oo4_4	9,59E-09	1,04E-08	1,04E-08	1,06E-08	-7,8%	-8,1%	-10,5%
3oo4_1	2,95E-03	2,76E-03	2,76E-03	2,75E-03	6,9%	6,9%	6,8%
3oo4_2	7,47E-04	7,22E-04	7,22E-04	7,22E-04	3,5%	3,5%	3,3%
3oo4_3	2,51E-05	2,53E-05	2,53E-05	2,55E-05	-0,8%	-1,0%	-1,6%
3oo4_4	9,43E-06	9,75E-06	9,78E-06	9,74E-06	-3,3%	-3,5%	-3,3%

* These two values were not calculated with the simulation model because they are too small and would need too much computational time to be obtained.

As can be seen from Table 3, all four methods give very similar results. The largest differences between the results of the approximate analytical equations with respect to the other three methods is of the order of 10%, indicating that the derived equations can be used without introducing any significant deviations from the results. It is always important to indicate that because of the linearization approximation, the results of the analytical equations should not be used for values of λT greater than 0.1 (a restriction that is not very often attained in practice).

It is also interesting to note that the results obtained with the numerical method and those from GRIF-Tree differ by less than 1% in all cases, indicating than the latter must use a numerical integration model to obtain the time-averaged value of the system PFD.

We have performed several other comparisons by varying the computational parameters, namely, the failure rates, the testing period and the coverage coefficients. In Figure 10 we show the comparison of results obtained for the four testing level case by varying the third coverage coefficient (C3) from 0.1 to 0.9. This corresponds to an increase of the part of the failure rate that is left to be detected at the last (fourth in this case) testing level. As can be seen, the results continue to be very close between all methods.

4.2 *Results Obtained with CCF*

By using the same CCF method (Beta-Factor model in this case) the inclusion of CCF has the effect of making the results even more equal between the various computational methods. The reason is simply because the CCF model is the same for all methods and it tends to be the dominant term specially for the higher redundancy configurations.

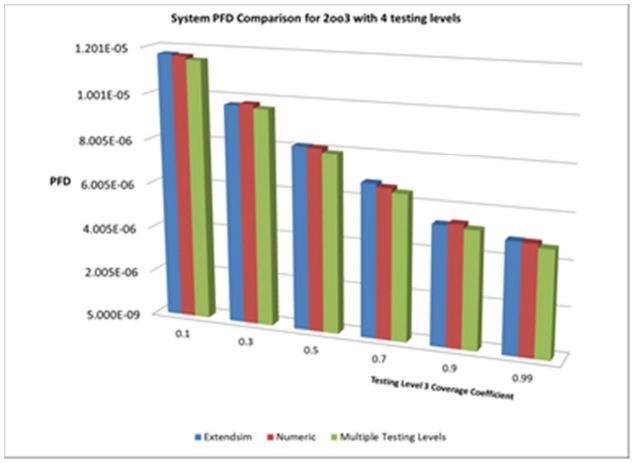


Figure 10 - Comparison of PFD results for a 2oo3 system varying the Level 3 diagnostic coverage coefficient

5 APPLICATION TO THE CASE OF A BOP

The fact that some components of a BOP are subject to many testing levels (up to five in some cases) was the main motivation for the development of this work.

A BOP is a much more complex system than just a KooN configuration and therefore the approximate analytical equations presented in this paper cannot be directly applied to it. Nevertheless there are many instances of such configurations inside the BOP structure and the equations could still be applied to them.

For lack of space, here we will not go into the details of the application to BOP. We only would like to mention that the other three methods (numerical, FT and simulation) could be equally applied to the case of a BOP. The application of the numerical method as indicated here would require some method to develop the logical structure of the BOP (a reliability structure function). This could in the form of a minimal cut sets, for example. In this case, the application of the numerical method would be the same as the application of a fault tree program that performs the quantitative evaluation of the PFDavg of the system by numerical integration of the time-dependent, PFD(t), of the system.

6 FINAL COMMENTS

Most safety systems currently in use may be subject to more than the usual two testing levels: online diagnostics and periodic testing. Some more complex safety systems, such as Blowout Preventers (BOPs) currently in operation in various parts of the world, have some of their key components subject to multiple testing levels (up five levels in some cases).

In this paper we investigate possible solution methods for the calculation of PFD of safety systems subject to multiple testing levels (MTL), develop an approximate analytical equation for the evaluation of the PFD of safety systems subject to MTL based on simplified RBDs, assess the differences in results of PFD values obtained with various methods: approximate analytical equations, numerical integration, fault tree analysis, and Monte-Carlo simulation. It is shown that with proper modelling all methods give acceptable results, that is, within acceptable differences between them.

5. REFERENCES

[1] International Electrotechnical Commission, “Functional Safety of Electrical/-Electronic-/Programmable Electronic Safety-Related Systems”, IEC 61508, 2nd edition, 2010.

[2] Knegtering, B., “Safety-PLC´s Striking Role for Partial Valve Stroke Testing”, ISA 2004 Houston Technical Conference, 2004.

[3] McCrea-Steele, R., “Partial Stroke Testing: Implementing for the Right Reasons”, ISA Expo 2005, Chicago, IL, 2005.

[4] Apostolakis, G. and Chu, L.,“The Unavailability of Systems under Periodic Test and Maintenance”, Nuc. Technology 59, Mid-Aug 1980.

[5] Vesely, W.E. and Goldberg, F.F., “FRANTIC – A Computer Code for Time-Dependent Unavailability Analysis”, USNRC NUREG 75/015 (1975).

[6] Oliveira, L.F. & Abramovitch, R., “Extension of ISA TR84.00.02 PFD equations to KooN architectures,” Reliability Engineering & System Safety, vol. 95(7), p. 707-715, 2010.

[7] Jahanian, H. , “Formulas of IEC 61508 for KooN Configurations”, ISA Transactions Nov. 2014.

[8] Innal, F., Dutuit, Y., and Chebila, M., “Safety and operational integrity evaluation and design optimisation of safety instrumented systems”, Reliab. Eng. Syst. Saf. 134, Feb 2015, Pages 32–50 (2015).

[9] Rasmussen, N. et al., “U.S. Reactor Safety Study”: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants”, US NRC Report NUREG-75/014 (WASH-1400) 1975.

[10] TOTAL (2014), “Software GRIF- Tree (“Graphiques Interactifs pour la Fiabilité”, developed by TOTAL, grif-workshop.com/grif/tree-module/.

[11] Harel, D. (1987), “Statecharts: A Visual Formalism for Complex Systems”, Science of Computer Programming 8 (1987)

[12] ImagineThat, Extendsim, Inc. www.extendsim.com (2008).

[13] Aubry, J.F., and Brinsei, N., “System Dependability Assessment: Modelling with Finite State Automata”, Wiley 2015.