Performance evaluation of Safety Instrumented Systems using Markovian approach

A. Mkhida [#1], B. Zouhri [#2], A. Ejjedoui [#3]

#1 #2 #3, ENSAM (Ecole Nationale Supérieure d'Arts et Métiers), Meknes BP 4024, Marjane II, Morocco. Moulay Ismaïl University. MTICS (Modeling, Information Processing and Control Systems).

ABSTRACT

This article deals with the performance evaluation of dependability of Safety Instrumented Systems using markovian approach. The Formulas of average of probability of failures in demand (PFDavg) are given without justification in the safety related standards. The work presented in this article deals with modeling in order to evaluate the performances relating to the dependability for different architectures in conformity with the international standards (IEC 61508 & IEC 61511). In the modeling of the system, the functional and dysfunctional aspects coexist and the dynamic approach using the markovian approach is proposed to overcome the difficulties mentioned above. Numerical results are used to assess the dependability parameters (probability of failure in demand) in compliance with safety standards related to SIS (IEC 61508 & IEC 61511).

Key words: IEC 61508, IEC 61511, Safety Instrumented Systems, Markovian Approach, Probability of Failure on Demand, Modeling, Performance evaluation.

Corresponding Author: Abdelhak MKHIDA

1. INTRODUCTION

The process industry is technically more complex and the potential danger increases accordingly if risk flows are not adequately controlled. So when industrial facilities pose potential risks to people, property or the environment, various safety devices are to be implemented. These contribute to the prevention or minimizing the likelihood of risk or protection to limit the consequences of a malfunction.

SIS aim to make the process of failsafe position when changing to a channel with a real risk (explosion, fire, etc..), That is to say, a steady state with no risk for people, the environment or property. SIS to define, identify and assess the risks against which we must protect. The main norms and standards in terms of safety IEC 61508 [1] and IEC 61511 [2] can be used for design. Methods that offer these standards are based on an estimate of the necessary risk reduction should achieve the SIS.

Standards IEC 61508 and IEC 61511 (oriented process industries) define levels of safety integrity level (SIL Safety Integrity Levels) that fix the level of risk reduction to be achieved by the SIS. There are four possible levels, denoted SIL1 to SIL4. Each depends on the severity and frequency of occurrence of the risk. It is obvious that if a risk is very important, it requires very efficient parades. It will automatically assign a SIL level (3 or even 4). Both standards define an important criterion to characterize the SIS: the average probability of failure on demand (PFDavg: Average Probability of Failure on Demand) for SIS low loads

(less than one solicitation per year) and the probability of failure per hour (PFH: Probability of Failure per Hour) for SIS heavily loaded or operating in continuous mode.

Implementation of the requirements of these two standards is not necessarily trivial where there is no real explanation or justification for formulas induced them to calculate PFDavg.

View that the standard has not given evidence concerning these formulas and to remove the doubt vitiates the relevance of these formulas have been used in the probabilistic method the most sensitive and accurate approach namely the graph Markov for comparison between PFDavg (that given by the standard) and PFD (calculated by the latter).

2. ARCHITECTURES OF SAFETY INSTRUMENTED SYSTEMS

Safety instrumented systems are used in many industrial processes to reduce the consequences of process demands on humans, the environment and material assets.

Different standards can be used to design safety instrumented systems for process industry like IEC 61508 and IEC 61511 (IEC61508 2000, IEC61511 2003, ISA84 1996). These standards have been developed to ensure that the SIS is designed, implemented and operated according to the specified needs.

Safety Instrumented Systems are used in many industrial processes to reduce the frequency and the severity of the consequences of process demands on humans, the environment and material assets. Different standards can be used to design safety instrumented systems for process industry like IEC 61508 and IEC 61511 (IEC 61511, 2004; IEC 61508, 2002). These standards have been developed to ensure that the SIS is designed, implemented, and operating according to the specified needs.

2.1. Objectives of Safety Instrumented Systems

IEC 61511 defines a safety function as a: "function to be implemented by a SIS, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the process with respect to a specific hazardous event". The Safety Instrumented Function (SIF) is used to describe the safety functions implemented by instrumented technology. The SIS is the physical system implementing one or more SIFs.

The objectives of SIS is to reduce the frequency at which hazard may occur to an acceptable level (Weiegerinck, 2002). The safety function only reduces the risk (multiplication: probability x consequences) and never completely eliminates the risk. Some safety functions do not reduce the probability of the consequences but they reduce the severity.

All combined instrumentation, devices, and equipment that are fulfilling an intended safety function are considered to be part of the safety instrumented systems. The SIS could be composed of a set of safety-related sensing elements, safety-related logic solver and safety-related final elements.

It is interesting to notice that there exists a clear distinction between the Basic Process Control System (BPCS) and the safety instrumented systems as part of the Prevention and Mitigation layers. The primary objective of a BPCS is to optimize the process conditions in order to maximize the production capacity and quality. Safety-instrumented systems are primarily applied to prevent hazardous events from occurring (Prevention layer), and mitigation of the consequences of hazardous event (Mitigation layer). The reason for this distinction is due to the fact that a BPCS does not necessarily have to contribute to the risk reduction and sometimes might even pose a potential risk itself.

2.2. Architectures of Safety Instrumented Systems

1oo1 architecture

This architecture includes a single channel, where any dangerous failure leads to a failure of the safety function when a demand arises [3] and it consists of a single hardware path so that a signal can travel in the chain of processing an application. Generally, for a MooN architecture, the first number is the number of elements that must be in working order for the system to ensure the safety function and the second digit indicates the level of redundancy [1].

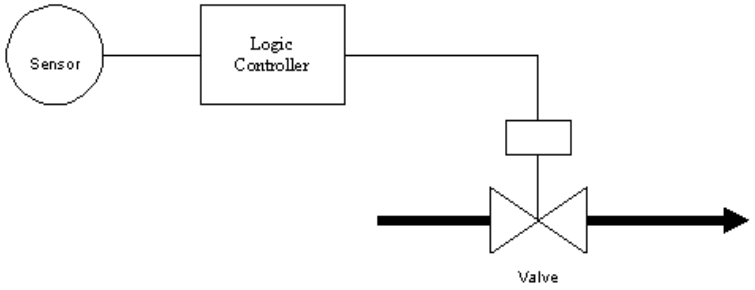

Fig. 1 : Safety Instrumented Systems (1oo1 Architecture)

1oo2 architecture

This architecture consists of two channels connected in parallel [3], so that either channel can process the safety function. Thus there would have to be a dangerous failure in both channels before a safety function failed on demand. It is assumed that any diagnostic test would only report the faults found and would not change any output states or change the output voting. Fig. 2 contains the relevant block diagram. Note that common cause failure has to be considered because there are two identical channels. β denotes the fraction of undetected failures that have a common cause, while β_D is of those failures that are detected by the diagnostic tests, the fraction that have a common cause.

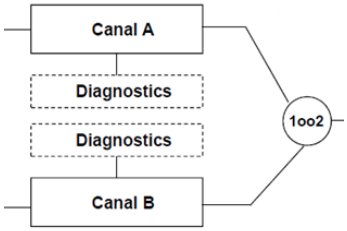

Fig.2 : Safety Instrumented Systems (1oo2 Architecture)

2oo2 architecture

The second architecture has two channels operating in active redundancy. It will take the case of a dangerous failure in the two channels for a valid alarm signal is not treated properly. Both channels need to demand the safety function before it can take place [3].

2oo3 architecture

This architecture consists of three channels connected in parallel with a majority voting arrangement for the output signals [3], so that the output state is not changed if only one channel gives a different result, which disagrees with the other two channels.

3. MARKOVIAN APPROACH

Modeling by Markov chains is one approach quoted in IEC61511 [2]. It is a holistic approach often used in dependability studies when one wishes to model a reparable system with components at constant failure and restoration rates [4], [5]. In this work, the transition probabilities of the Markov chain are considered independent of time (homogeneous process). So, the failures rates are considered constants. This assumption is consistent when working in the useful life period (maturity phase) of components. When using Markov chains, it is also possible to take into account some dependencies and to make a dynamic analysis of the system [6].

The solving equations, when one knows the initial distribution Qi (0), can be done by including explicit resolution methods using the Laplace transformation, discretization or calculation of the eigenvalues of the matrix A (and using matrix exponential).

Mention just a few features of these methods:

- The resolution of a linear system of differential equations of the first order is standard in numerical analysis and many computer programs are available.
- The resolution of equations of state for calculating the eigenvalues of the matrix leads to a solution of the system of differential equations known explicitly using a matrix exponential.

Q (t) = Q (0) * exp (At)

This method poses a problem for highly reliable systems. In fact, the largest eigenvalue is much smaller than the other in absolute value and accuracy may be poor when the number of states is large enough. This is even more annoying is that this eigenvalue which determines the behavior of the system when t is large enough. That is why this method is generally not used.

We recall the numbering convention states of a system:

The system state equations are defined by:

$$\left[\frac{dP_1(t)}{dt} \quad \frac{dP_2(t)}{dt} \quad \dots \quad \frac{dP_n(t)}{dt}\right]^T = \left[P_1(t) \quad P_2(t) \quad \dots \quad P_n(t)\right] \cdot \mathrm{Q}$$

The transition matrix is the matrix Q such that we have previously defined

sum of lines = 0 so : $|Q| = 0$

$$\mathrm{Q} = \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,l} & a_{1,l+1} & \dots & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & & \vdots & \vdots & & & \vdots \\ \vdots & & Q_l & \vdots & \vdots & & & \vdots \\ a_{l,1} & a_{l,2} & \dots & a_{l,l} & a_{l,l+1} & \dots & \dots & a_{l,n} \\ a_{l+1,1} & & & a_{l+1,l} & a_{l+1,l+1} & a_{l+1,l+2} & & a_{l+1,n} \\ \vdots & & & \vdots & \vdots & & & \vdots \\ \vdots & & & \vdots & & Q_p & & \vdots \\ a_{n,1} & \dots & \dots & a_{n,l} & a_{n,l+1} & \dots & \dots & a_{n,n} \end{bmatrix}$$

Working States

Availability

Failed States

In our case we are interested in determining the availability of end deduct the downtime is the PFD.

Asymptotic availability is calculated by the sum of the probabilities of asymptotic reside in different operating states of the system:

So we need to calculate Pj (t) in steady state (ie when t tends to infinity).

Mathematical properties of the system of differential equations we have to solve to determine simple formulas for calculating the asymptotic values for the different variables of the system.

By the properties of the matrix Q, we use the following determinant:

$$\Delta = \begin{vmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,l} & a_{1,l+1} & \dots & a_{n,n-1} & 1 \\ a_{2,1} & a_{2,2} & & \vdots & \vdots & & & \vdots \\ \vdots & & & \vdots & \vdots & & & \vdots \\ a_{l,1} & a_{l,2} & \dots & a_{l,l} & a_{l,l+1} & \dots & \dots & 1 \\ a_{l+1,1} & & & a_{l+1,l} & a_{l+1,l+1} & a_{l+1,l+2} & & 1 \\ \vdots & & & \vdots & \vdots & & & \vdots \\ \vdots & & & \vdots & \vdots & & & \vdots \\ a_{n,1} & \dots & \dots & a_{n,l} & a_{n,l+1} & \dots & a_{n,n-1} & 1 \end{vmatrix}$$

This matrix is constructed by replacing the last column of the matrix by a column of Q 1.

This matrix is constructed by replacing the last column of the matrix Q by a column of 1.

To calculate the asymptotic availability we have to calculate the following determinants [7]:

$$A(\infty) = \sum_{j=1}^{l} P_j(\infty) = \frac{Q^*}{\Delta}$$

Q* determination :

$$Q^* = \begin{vmatrix} a_{1,1} & \dots & \dots & a_{n,n-1} & 1 \\ \vdots & & & & \vdots \\ a_{l,1} & \dots & \dots & a_{l,n-1} & 1 \\ a_{l+1,1} & & & a_{l+1,n-1} & 0 \\ \vdots & & & & \vdots \\ a_{n,1} & \dots & \dots & a_{n,n-1} & 0 \end{vmatrix}$$

Working State

Failed State

To calculate the asymptotic availability so we have to calculate the following determinants:

$$A(\infty) = \sum_{j=1}^{l} P_j(\infty) = \frac{\begin{vmatrix} a_{1,1} & \dots & \dots & a_{n,n-1} & 1 \\ \vdots & & & & \vdots \\ a_{l,1} & \dots & \dots & a_{l,n-1} & 1 \\ a_{l+1,1} & & & a_{l+1,n-1} & 0 \\ \vdots & & & & \vdots \\ a_{n,1} & \dots & \dots & a_{n,n-1} & 0 \end{vmatrix}}{\begin{vmatrix} a_{1,1} & \dots & a_{n,n-1} & 1 \\ & & & \vdots \\ & & & \vdots \\ a_{n,1} & \dots & a_{n,n-1} & 1 \end{vmatrix}}$$

Issue 3, Vol.2 (May 2013)
ISSN 2249-6149

We can calculate the unavailability by two methods:
The first :

$$\overline{A}(\infty) = 1 - A(\infty)$$

The second :

$$\overline{A}(\infty) = \frac{\begin{vmatrix} a_{1,1} & \cdots & \cdots & a_{n,n-1} & 0 \\ \vdots & & & & \vdots \\ a_{l,1} & \cdots & \cdots & a_{l,n-1} & 0 \\ a_{l+1,1} & & & a_{l+1,n-1} & 1 \\ \vdots & & & & \vdots \\ a_{n,1} & \cdots & \cdots & a_{n,n-1} & 1 \end{vmatrix}}{\begin{vmatrix} a_{1,1} & \cdots & a_{n,n-1} & 1 \\ \vdots & & & \vdots \\ \vdots & & & \vdots \\ a_{n,1} & \cdots & a_{n,n-1} & 1 \end{vmatrix}}$$

Failure states

4. MODELING FRAMWORK

In the present approach, it is assumed that the failure distributions of individual components of a system are given, and the dependability measures of the stochastic system are sought. Furthermore, the system is assumed to be dynamic (its properties change with time) [8].
In the modeling of the system, the functional and dysfunctional aspects coexist; the failures are divided into safe failures and dangerous failures. A dangerous failure results in an absence of reaction of the safety function. A safe failure results by the setting in a safe position of the system or in an unexpected execution of the safety function. The detection of a safe or dangerous failure results in a setting into a safe position of the system or a forced execution of the safety function [8].
1oo1 architecture
Given the mode of this channel and assumptions made in the standard, a Markov model is suitable to represent the functional and dysfunctional behavior of this channel.

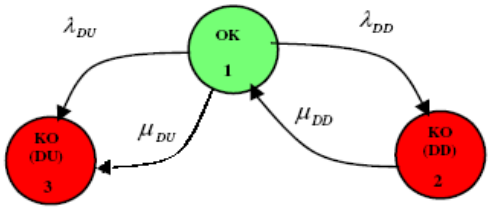

Fig. 3 : Markovien Model, 1oo1 architecture

Approximate expression of tDU:
Reminder limited development of $e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots , \ -\infty < x < \infty$
To order 2, we therefore $e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!}$
And tDU becomes equal to : tDU=T/2
Calculation of tC1: tC1=T-T/2 + MTTR
So: tC1=T/2 + MTTR

We deduce the repair rate is µDU:[9]

$$\mu_{DU} = \frac{1}{tc1} = \frac{1}{\frac{T}{2} + MTTR}$$

Architecture 1oo1D:

The detection of a dangerous failure led to a safe fallback position.

The coverage and frequency of diagnostic tests have an impact on the security of such architecture.

Dangerous fouls (resulting in loss of the safety function) are faults not detected by testing.

The formula of PFD(1oo1) following the standard [1] is :

$$PFD = \lambda_{DU} * \left(\frac{T}{2} + MTTR\right) + \lambda_{DD} * MTTR$$

By the method of PFD Markov architecture 1oo1:

According to the graph Figure 1, we have 3 states: The first one in which the system is in a running state, the second one in which the system is in a dangerous condition and detectable and the third state in which the system is in a dangerous state but not detectable.

Graph can be drawn from the following equations:

$$\begin{cases} p_1(t+dt) = p_1(t) * (2 - \lambda_{DD}dt - \lambda_{DU}dt) + p_2(t) * \left(\mu_{DD}dt + \mu_{DU}dt\right) \\ p_2(t+dt) = p_1(t) * (\lambda_{DD}dt) + p_2(t) * \left(1 - \mu_{DD}dt\right) \\ p_3(t+dt) = p_1(t) * (\lambda_{DU}dt) + p_3(t) * \left(1 - \mu_{DU}dt\right) \end{cases}$$

when $dt \to \infty$, we have :

$$\begin{cases} p_1'(t) = -(\lambda_{DD} + \lambda_{DU}) * p_1(t) + \left(\mu_{DD} * p_2(t) + \mu_{DU} * p_2(t)\right) \\ p_2'(t) = -\mu_{DD} * p_2(t) + \lambda_{DD} * p_1(t) \\ p_3'(t) = -\mu_{DU} * p_3(t) + \lambda_{DU} * p_1(t) \end{cases}$$

Solving these equations can lead us to the Markov matrix:

$$\left[p_1'(t)\ p_2'(t)\ p_3'(t)\right] = \left[p_1(t)\ p_2(t)\ p_3(t)\right] \begin{bmatrix} -(\lambda_{DD} + \lambda_{DU}) & \lambda_{DD} & \lambda_{DU} \\ \mu_{DD} & -\mu_{DD} & 0 \\ \mu_{DU} & 0 & -\mu_{DU} \end{bmatrix}$$

Markov matrix is:

$$Q = \begin{bmatrix} -(\lambda_{DD} + \lambda_{DU}) & \lambda_{DD} & \lambda_{DU} \\ \mu_{DD} & -\mu_{DD} & 0 \\ \mu_{DU} & 0 & -\mu_{DU} \end{bmatrix}$$

Solving these equations using the Laplace transform, leads us to:
- Calculate the determinant:

$$\Delta = \begin{vmatrix} -(\lambda_{DD}+\lambda_{DU}) & \lambda_{DD} & 1 \\ \mu_{DD} & -\mu_{DD} & 1 \\ \mu_{DU} & 0 & 1 \end{vmatrix}$$

Calculate the determinant of the first probability P1:
We'll put '1 'in the first line because it is the first state in the probability of walking

$$\Delta_1 = \begin{vmatrix} -(\lambda_{DD}+\lambda_{DU}) & \lambda_{DD} & 1 \\ \mu_{DD} & -\mu_{DD} & 0 \\ \mu_{DU} & 0 & 0 \end{vmatrix}$$

Which allows the deduction of P_1:

$$P_1 = \frac{\Delta_1}{\Delta} = \frac{\begin{vmatrix} -(\lambda_{DD}+\lambda_{DU}) & \lambda_{DD} & 1 \\ \mu_{DD} & -\mu_{DD} & 0 \\ \mu_{DU} & 0 & 0 \end{vmatrix}}{\begin{vmatrix} -(\lambda_{DD}+\lambda_{DU}) & \lambda_{DD} & 1 \\ \mu_{DD} & -\mu_{DD} & 1 \\ \mu_{DU} & 0 & 1 \end{vmatrix}}$$

P1 knowledge to deduce the asymptotic availability of the system:

$$A(\infty) = P_1$$

The asymptotic unavailability is obtained simply by exchanging the "0" with "1" in the last column of the determinant in the numerator:

$$PFD = \bar{A}(\infty) = 1 - A(\infty) = \frac{1}{\Delta} * \begin{vmatrix} -(\lambda_{DD}+\lambda_{DU}) & \lambda_{DD} & 0 \\ \mu_{DD} & -\mu_{DD} & 1 \\ \mu_{DU} & 0 & 1 \end{vmatrix}$$

Determining the rate µDU
We will determine the average tc1 unavailable due to an undetected fault line for the channel. It is defined without any justification in the standard by the following expression:

$$\text{tc1} = \frac{\text{T}}{2} + \text{MTTR}$$

This is going to demonstrate:

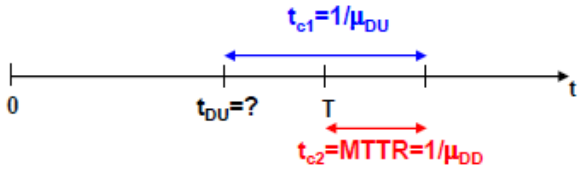

Fig. 4: Graphic representation of the average unavailability

t_{DU} is the moment which means a dangerous failure is likely to happen:

$$t_{DU} = \frac{\int_0^T tf(t)dt}{\int_0^T f(t)dt}$$

Dangerous failures follow an exponential distribution law, then:

$F(t) = 1 - e^{-\lambda_{DU} t}$ where $f(t) = \frac{dF(t)}{dt} = \lambda_{DU} e^{-\lambda_{DU} t}$

So we have : $t_{DU} = \frac{\int_0^T tf(t)dt}{\int_0^T f(t)dt} = \frac{\int_0^T t*\lambda_{DU} e^{-\lambda_{DU} t} dt}{\int_0^T \lambda_{DU} e^{-\lambda_{DU} t} dt} = \frac{\int_0^T t* e^{-\lambda_{DU} t} dt}{\int_0^T e^{-\lambda_{DU} t} dt} = \frac{\frac{1-e^{-\lambda_{DU} T}}{\lambda_{DU}} - Te^{-\lambda_{DU} T}}{1-e^{-\lambda_{DU} T}}$

1oo2 architecture

The second architecture has two channels operating in active redundancy. Each channel has three states; architecture has 9 = 32 possible states. Some states may be aggregated. The aggregation of states leads to a model with six states which must be added two additional states considering the common mode failures. The β_D failure rate common cause of failures is detected by a diagnostic test and β failure rate common cause failures is not detected by a diagnostic test.

The Markov graph is shown in the following figure 5:

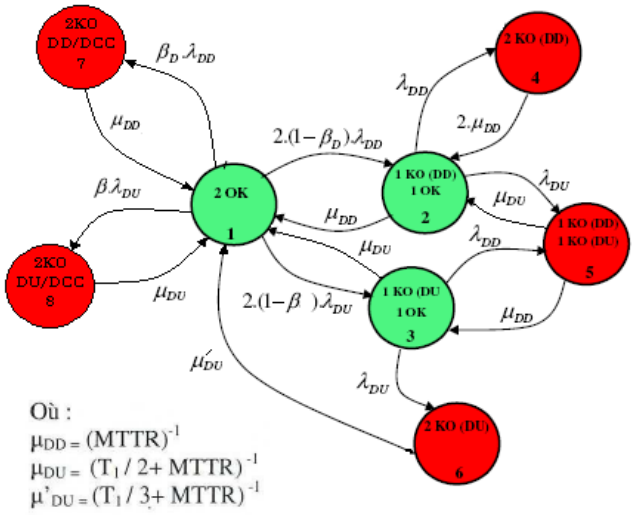

Fig. 5 : Markovian Model, 1oo2 architecture [9]

μ'_{DU} is different than μ_{DU} because it corresponds to the repair of two channels having been successively an undetected failure.

Determination of repair rate μ'_{DU}:

t_{c1} is the average downtime of the overall system due to undetected failures successive two channels occurred in the course of [0, T].

Either way t'_{DU} now on [0, T] the failure of the overall system.

Issue 3, Vol.2 (May 2013)
ISSN 2249-6149

$$t'DU = \frac{\int_0^T tf(t)dt}{\int_0^T f(t)dt}$$

F(t) =(1 - $e^{-\lambda_{DU}\,t}$)2 where $f(t) = \frac{dF(t)}{dt} = 2\lambda_{DU}\,e^{-\lambda_{DU}\,t} * (1 - \lambda_{DU}\,e^{-\lambda_{DU}\,t})$

So : $t'_{DU} = \frac{\int_0^T tf(t)dt}{\int_0^T f(t)dt} = \frac{\int_0^T t*2\lambda_{DU}\,e^{-\lambda_{DU}\,t}*(1-\lambda_{DU}\,e^{-\lambda_{DU}\,t})\,dt}{\int_0^T 2\lambda_{DU}\,e^{-\lambda_{DU}\,t}*(1-\lambda_{DU}\,e^{-\lambda_{DU}\,t}dt} = \frac{\int_0^T e^{-\lambda_{DU}\,t}*(1-\lambda_{DU}\,e^{-\lambda_{DU}\,t})dt}{\int_0^T e^{-\lambda_{DU}\,t}*(1-\lambda_{DU}\,e^{-\lambda_{DU}\,t})dt}$

After integration and approximation of exponential terms with their limited development, t'_{DU} becomes equal to:

$$t'_{DU} = \frac{2T}{3}$$

Calculation of t_{C1} : $tc1 = T - \frac{2T}{3} + MTTR$

so : $tc1 = \frac{T}{3} + MTTR$

we deduce the repair rate :

$$\mu'_{DU} = \frac{1}{tc1} = \frac{1}{\frac{T}{3} + MTTR}$$

The calculation of the PFD by the IEC 61508 standard:

$$PFD = \left\{(1-\beta) * \lambda_{DU} * \frac{T}{2} + [(1-\beta) * \lambda_{DU} + (1-\beta_D) * \lambda_{DD}] * MTTR\right\}^2 + \frac{T^2}{2} * (1-\beta)^2 * {\lambda_{DU}}^2 + \beta * \lambda_{DU}\left(\frac{T}{2} - MTTR\right) + \beta_D * \lambda_{DD} * MTTR$$

β (respectively β_D): factors common cause for undetected failures (detected)

The calculation of PFD by the method of MARKOV:

According to the graph in Figure 4, we deduce the following system:

$$[p'_1(t)\ \ p'_2(t)\ p'_3(t)\ ....\ \ p'_8(t)] = [p_1(t)\ \ p_2(t)\ \ p_3(t)\ \ p_4(t)\ ...\ \ p_8(t)\ ] * Q$$

The Markov transition matrix is written:

$$\begin{bmatrix}
2\lambda_{DD}*(1-\beta_D)+2\lambda_{DU}*(1-\beta)-\lambda_{DD}*\beta_D-\lambda_{DU}*\beta_U & -2\lambda_{DD}*(1-\beta_D) & -2\lambda_{DU}*(1-\beta) & 0 & 0 & 0 & \lambda_{DD}*\beta_D & \lambda_{DU}*\beta_U \\
\frac{1}{MTTR} & -\frac{1}{MTTR}-\lambda_{DU}-\lambda_{DD} & 0 & \lambda_{DD} & \lambda_{DU} & 0 & 0 & 0 \\
\frac{1}{\frac{T}{2}+MTTR} & 0 & -(\lambda_{DD}+\lambda_{DU}+\frac{1}{\frac{T}{2}+MTTR}) & 0 & \lambda_{DD} & \lambda_{DU} & 0 & 0 \\
0 & 2*\frac{1}{MTTR} & 0 & -2*\frac{1}{MTTR} & 0 & 0 & 0 & 0 \\
0 & \frac{1}{\frac{T}{2}+MTTR} & \frac{1}{MTTR} & 0 & -\left(\frac{1}{MTTR}+\frac{1}{\frac{T}{2}+MTTR}\right) & 0 & 0 & 0 \\
\frac{1}{\frac{T}{3}+MTTR} & 0 & 0 & 0 & 0 & -\frac{1}{\frac{T}{3}+MTTR} & 0 & 0 \\
\frac{1}{MTTR} & 0 & 0 & 0 & 0 & 0 & -\frac{1}{MTTR} & 0 \\
\frac{1}{\frac{T}{2}+MTTR} & 0 & 0 & 0 & 0 & 0 & 0 & -\frac{1}{\frac{T}{2}+MTTR}
\end{bmatrix}$$

We calculate the determinant Δ :

$$\begin{bmatrix}
2\lambda_{DD}*(1-\beta_D)+2\lambda_{DU}*(1-\beta)-\lambda_{DD}*\beta_D-\lambda_{DU}*\beta_U & -2\lambda_{DD}*(1-\beta_D) & -2\lambda_{DU}*(1-\beta) & 0 & 0 & 0 & \lambda_{DD}*\beta_D & 1 \\
\frac{1}{MTTR} & -\frac{1}{MTTR}-\lambda_{DU}-\lambda_{DD} & 0 & \lambda_{DD} & \lambda_{DU} & 0 & 0 & 1 \\
\frac{1}{\frac{T}{2}+MTTR} & 0 & -(\lambda_{DD}+\lambda_{DU}+\frac{1}{\frac{T}{2}+MTTR}) & 0 & \lambda_{DD} & \lambda_{DU} & 0 & 1 \\
0 & 2*\frac{1}{MTTR} & 0 & -2*\frac{1}{MTTR} & 0 & 0 & 0 & 1 \\
0 & \frac{1}{\frac{T}{2}+MTTR} & \frac{1}{MTTR} & 0 & -\left(\frac{1}{MTTR}+\frac{1}{\frac{T}{2}+MTTR}\right) & 0 & 0 & 1 \\
\frac{1}{\frac{T}{3}+MTTR} & 0 & 0 & 0 & 0 & -\frac{1}{\frac{T}{3}+MTTR} & 0 & 1 \\
\frac{1}{MTTR} & 0 & 0 & 0 & 0 & 0 & -\frac{1}{MTTR} & 1 \\
\frac{1}{\frac{T}{2}+MTTR} & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}$$

We compute the determinant in running condition which corresponds to the states P1, P2 and P3 because there will always be the system works (although there is a channel fails either state or non-detected which corresponds to the state 2et3) where Δ_{A_∞} :

$2\lambda_{DD} * (1-\beta_D) + 2\lambda_{DU} * (1-\beta) - \lambda_{DD} * \beta_D - \lambda_{DU} * \beta_U$	$-2\lambda_{DD} * (1-\beta_D)$	$-2\lambda_{DU} * (1-\beta)$	0	0	0	$\lambda_{DD} * \beta_D$	1
$\frac{1}{MTTR}$	$-\frac{1}{MTTR} - \lambda_{DU} - \lambda_{DD}$	0	λ_{DD}	λ_{DU}	0	0	1
$\frac{1}{\frac{T}{2}+MTTR}$	0	$-(\lambda_{DD}+\lambda_{DU}+\frac{1}{\frac{T}{2}+MTTR})$	0	λ_{DD}	λ_{DU}	0	1
0	$2*\frac{1}{MTTR}$	0	$-2*\frac{1}{MTTR}$	0	0	0	0
0	$\frac{1}{\frac{T}{2}+MTTR}$	$\frac{1}{MTTR}$	0	$-\left(\frac{1}{MTTR}+\frac{1}{\frac{T}{2}+MTTR}\right)$	0	0	0
$\frac{1}{\frac{T}{3}+MTTR}$	0	0	0	0	$-\frac{1}{\frac{T}{3}+MTTR}$	0	0
$\frac{1}{MTTR}$	0	0	0	0	0	$-\frac{1}{MTTR}$	0
$\frac{1}{\frac{T}{2}+MTTR}$	0	0	0	0	0	0	0

So the availability is :

$$A_{\infty} = \frac{\Delta_{A_{\infty}}}{\Delta}$$

Hence we can draw the unavailability:

$$\bar{A}(\infty) = 1 - A(\infty)$$

2oo3 Architecture

This architecture includes three parallel connected with a device for majority logic output signals, such that the output state is not changed channels when one channel gives a different result from the other two channels. It is assumed that all diagnostic tests that would indicate anomalies and alter or output neither states nor the majority logic.

The average probability of failure for the architecture is given by [1]:

$$PFD_G = 6\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right)$$

The 2oo3 architecture (two of three) corresponds to the redundancy of three channels 1oo1 type with a majority vote to passivate the failure of one of them, the 27 = 33 possible states of this architecture can aggregated by the following ten states:

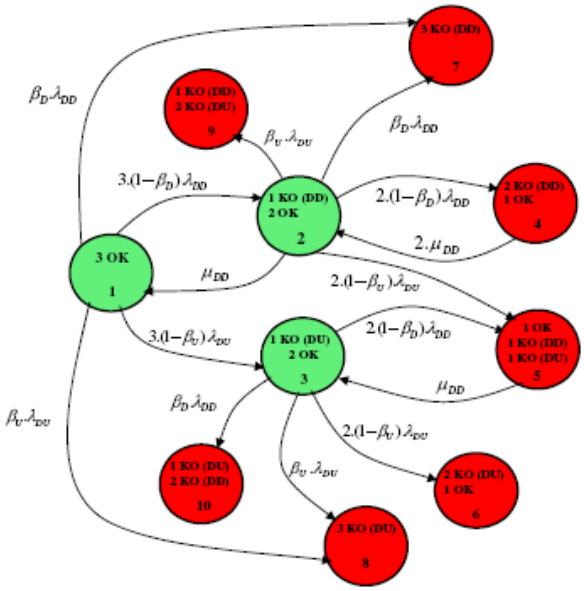

Figure 6: Markovian Model, 2oo3 architecture [6]

Determining repair rate µ"DU:
Tc1 is the average downtime of the overall system due to undetected failures successive three channels occurred in the course of [0, T].
THE" t be the time average over [0, T] the failure of the overall system.

$$t'DU = \frac{\int_0^T tf(t)dt}{\int_0^T f(t)dt}$$

F(t) =$(1 - e^{-\lambda_{DU}\, t})3$ where $f(t) = \frac{dF(t)}{dt} = 3\lambda_{DU} e^{-\lambda_{DU}\, t} * (1 - e^{-\lambda_{DU}\, t})2$

So we have: $t'_{DU} = \frac{\int_0^T tf(t)dt}{\int_0^T f(t)dt} = \frac{\int_0^T t*3\lambda_{DU}\, e^{-\lambda_{DU}\, t}*(1-e^{-\lambda_{DU}\, t})2\, dt}{\int_0^T 3\lambda_{DU}\, e^{-\lambda_{DU}\, t}*(1-e^{-\lambda_{DU}\, t})2dt} = \frac{\int_0^T e^{-\lambda_{DU}\, t}*(1-e^{-\lambda_{DU}\, t})2dt}{\int_0^T e^{-\lambda_{DU}\, t}*(1-e^{-\lambda_{DU}\, t})2dt}$

After integration and approximation of exponential terms with their limited development, t"DU

5. NUMERICAL RESULTS

1oo1 Architecture

The results are presented in Table 1:
For the 1oo1 architecture, the results are summarized in Table taking into account different values for the diagnostic coverage (DC) and taking the following values: for MTTR=8h, $\lambda_D = 2.5 * 10^{-5} h^{-1}, T = 4380h$
We see that the results of the calculation for PFD Markov method are roughly those obtained by the standard.

Table 1: Results of 1oo1 architecture

DC	PFD by Standard	PFD by MARKOV
0%	0.0553	0.0514
60%	0.0225	0.0209
90%	0.0061	0.0054

1oo2 Architecture

The comparison between the results of the method and the standard Markov is shown in the table 2:

$$\lambda_D = 2.5 * 10^{-5} h^{-1}, T = 4380h \; et \; \beta = \; 2\% \; et \; \beta_D = 20\% \; et \; \text{MTTR} = 8\text{h}$$

Table 2: Results for the 1oo2 architecture

DC	Standard	MARKOV	MARKOV without DCC
0%	0.0137	0.0128	0.0028
60%	0.0050	0.0047	4.9203e-004
90%	0.0012	0.0011	3.3391e-005

When we neglect the states of common mode, the results of the Markov graph are far from the results obtained by the standard. Hence we are interested in integrating common mode failures (DCC) in our system to estimate a good value for the PFD and therefore take different changes that can take our system.

We see that when we increase the coverage rates SIL levels are improving, which is normal. In comparing the values of Standard IEC 61508-6 and that of Markov, we find a slight difference between them; it shows that we were able to approach the formulas given by the IEC 61508-6 standard by the method of Markov.

2oo3 Architecture

The comparison between the unavailability of the standard to Markov method and comments:

For the values :

MTTR = 8h ; T1=4380h ; λ_D=2,5.10^{-5} h^{-1} ; μ_{DD}=1/MTTR ;

Tableau 5 : Results of the 2oo3 architecture

DC	Standard	Markov	Markov without CCF
60%	0.0019	0.0023	0.0010
90%	2.2050e-004	5.0317e-004	7.2764e-005

$$\lambda_D = 10^{-4} h^{-1}, \lambda_{DU} = 10^{-5} h^{-1}, T = 8760h \; et \; \beta = \; 2\% \; et \; \beta_D = 1\% \; et \; \text{MTTR} = 24\text{h}$$

Standard (DC=90%)	Markov	Markov without CCF
0.0081	0.0069	0.0043

From the table, we can conclude that the values of the standard are similar to those of the Markov approach taking into account the common cause failures (CCF).

6. CONCLUSION

Because the formulas of standard IEC61508 are not justified and that the mathematical method used to calculate the PFD remains mysterious. We used to use the Markovian approach to determining the PFD and the level of safety integrity on the safety instrumented by each architecture in accordance with IEC 61511 systems. We have been approached by the Markov models different type configurations k / n (at least k out of n) to give an understandable interpretation.

From the point of view of performance evaluation, the areas of dependability in the design phase seem to provide analysis and resolution techniques. This is not only due to the Markov framework in which we place ourselves. The results were indeed used in the field of dependability including the assessment of availability.Thus, the goal of our work is to propose a modeling approach and a model that can represent both the process on the structure and the process for functionality. In this sense, we have analyzed the safe system operation with a view to assess its performance. We have identified a number of concepts that have been the basis of our modeling approach.The objective of our work was to evaluate the dependability of safety instrumented systems as well as systems design phase. The use of security systems has been apprehended under the new standards for safety IEC 61508 and IEC 61511.

REFERENCES

[1] IEC61508. Functional safety of electrical/electronic/programmable electronic safety related systems. (2010).

[2] IEC61511. Functional safety: Safety instrumented systems for the process industry sector. (2000).

[3] H. Guo, X. Yang. A simple reliability block diagram method for safety integrity verification. Reliability Engineering and System Safety 92 (2007) pp, 1267–1273

[4] Y. Langeron, A. Barros, A. Grall, & C. Bérenguer. Combination of safety integrity levels (SILs): a study of IEC61508 merging rules. Journal of Loss Prevention in the Process Industries, (2008), 21(4), pp, 437-449.

[5] Y. Liu, & M. Rausand, Reliability assessment of safety instrumented systems subject to different demand modes. Journal of Loss Prevention in the Process Industries, (2011). 24(1), pp, 49-56.

[6] W. Mechri, C. Simon F. Bicking K. Ben Othman, Fuzzy multiphase Markov chains to handle uncertainties in safety systems performance assessment, Journal of Loss Prevention in the Process Industries (2013).

[7] A. Pagès & M. Gondran. Fiabilité des systems, edition Eyrolles, Paris, ISSN 0399-4198, 1980.

[8] A. Mkhida, J.M. Thiriet, J.F. Aubry. Integration of intelligent sensors in Safety Instrumented Systems (SIS). Process Safety and Environmental Protection, Volume , pp , janvier 2013.

[9] F. Innal, Y. Dutuit, M. Djebabra. Analyse critique des formules de base de données dans la norme internationale CEI 61508-6. 6ème congrès international pluridisciplinaire, Qualité et sûreté de fonctionnement. Bordeaux, France. Mars, 2005.