Uncertainty evaluation of Safety Instrumented Systems by using Markov chains

W. Mechri∗ Ch. Simon∗∗ K. Ben Othman∗ M. Benrejeb∗

∗ LARA Tunis, Ecole Nationale d’Ingénieurs de Tunis, BP37 Le Belvédère, 1002 Tunis, Tunisie
∗∗ CRAN Nancy Université CNRS UMR 7039, 2 Rue Jean Lamour, Vandoeuvre les Nancy, France

Abstract: In this article, the problem of imprecision in assessing the performance of Safety Instrumented Systems (SIS) using fuzzy Markov chains is addressed. The scalar elementary probabilities usually considered in Markov chains are replaced by fuzzy numbers. It allows experts to express their uncertainty concerning the basic parameters of systems (common cause factors, failure rate . . . ) and, to evaluate the impact of the uncertainty. We show how the imprecision induces significant changes on the Safety Integrity Level (SIL) of a SIS. The proposed method ensures the relevance of the results. It is affirmed by the comparison with results obtained by a Monte Carlo sampling approach.

Keywords: Common Cause Failure (CCF), Safety Instrumented Systems (SIS), Safety Integrity Level (SIL), Markov chains, uncertainty, Fuzzy probability.

1. INTRODUCTION

The application of IEC61508 (1998) and its sectoral variants, including IEC61511 (2000) for the process industry has radically changed the position of companies over the issue of safety. A major key point pointed out in these standards is the quantitative assessment of the performance of the safety system implemented and the classification of its performance level according to reference ranges of values. The performance must be proved by quantitative evaluations from referenced methods like fault trees, Markov chains, Petri nets . . . to classify it according to Safety Integrity Levels (SIL) defined in IEC61508 (1998). In this context, Markov chains are probably the most relevant model to take account the different events and the studied parameters.

In system unavailability studies, probabilities are often considered precise and perfectly known but real problems are not easily captured with a precise knowledge of the probabilities involved (Utkin and Coolen, 2007). This problem of imperfect knowledge about the probability values is known and handled in various ways. Interval valued probability is a simple and attractive representation of imprecision (Kozine and Utkin, 2002). The problem of imprecision is considered by other authors using imprecise probabilities (Utkin and Coolen, 2007), possibility distributions (Dubois, 2006) or belief functions (Simon and Weber, 2009). Fuzzy probabilities are an interesting representation of uncertainty in Markov chains (Buckley, 2005) because it corresponds to linguistic formulation of the expert knowledge and can be computed in a simple approach as interval valued probabilities.

In this work, we propose to use the work of Buckley (2005) within the framework of the performance evaluation of Safety Instrumented Systems (SIS) in low demand mode and periodically tested, by modelling the imprecision on the failure rates of components and other characteristic parameters such as the Common Cause Failure (CCF) factors. The second section is devoted to the study of the performance of periodically tested SIS in low demand mode. The third section sticks to the modelling of the imprecise knowledge of SIS parameters by fuzzy numbers and, the integration of the fuzzy parameters in multiphase Markov chains for the performance evaluation. The last section is devoted to the study of a practicable case relating to the process industry and the description of the conformity of our results with a purely random approach of uncertainty.

2. SIS PERFORMANCE EVALUATION

2.1 Safety Instrumented System

The goal of a SIS is to bring the system it supervises in a safe position i.e. a situation where it does not create a risk when the supervised process goes to a hazardous situation involving a real risk to people or the environment (blast, fire . . . ). The SIS is a system composed of sensors, logic solvers and final elements for the purpose of taking the supervised process to a safe state when predetermined conditions are violated.

A SIS is in low demand mode if the demand is less than or equal to 1 per year and also less or equal to two times the test period (IEC61508, 1998). It is in high demand mode if the demand is greater than 1 per year or greater than two times the periodical test frequency.
The IEC 61508 standard (IEC61508, 1998) establishes 4 classification levels based on the average Probability of Failure on Demand (PFDoD_{avg} in low demand mode) or the Probability of Failure per Hour (PFH in high demand mode) defined in Table 1.

<table>
<thead>
<tr>
<th>Demand mode</th>
<th>PFDoD_{avg}</th>
<th>PFH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>(10^{-6}, 10^{-4})</td>
<td>(10^{-6}, 10^{-3})</td>
</tr>
<tr>
<td>High</td>
<td>(10^{-4}, 10^{-3})</td>
<td>(10^{-7}, 10^{-6})</td>
</tr>
</tbody>
</table>

Table 1. SIL levels definition

As mentioned in the previous paragraph, SIS in low demand mode has the specificity to be periodically tested. The test objectives are to check the SIS reaches and preserves its SIL but also to detect latent failures.

### 2.2 Diagnosis Coverage rate model

IEC61508 (1998) defines the coverage rate for the diagnosis tests as being the ratio of the failure rate of the detected dangerous failure rate \(\lambda_{DD}\) (by a diagnosis test) on the total failure rate of the dangerous failure rate \(\lambda_D\) (detected and undetected).

\[
DC = \frac{\lambda_{DD}}{\lambda_D} = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} \quad (1)
\]

As the objective is to determine the probability of dangerous failure on demand, only the dangerous failure rates \(\lambda_D\) of the modules of the architectures components are taken into account. Considering the estimated coverage rate \(DC\) and the total dangerous failure rate \(\lambda_D\), the dangerous detected \(\lambda_{DD}\) and undetected \(\lambda_{DU}\) failure rates are then determined by:

\[
\lambda_{DD} = DC.\lambda_D \quad \text{and} \quad \lambda_{DU} = (1 - DC).\lambda_D \quad (2)
\]

The CCFs can be directly introduced into the failure probability evaluation. Given the difficulty of obtaining such data, parametric models have been developed. Several models have been considered in the literature as the model of factor \(\beta\) (Fleming, 1974), the PDS method (Hauge et al., 2006), the model of multiple Greek letters (MLG) (Barros et al., 2009). In this article, we preferred the model of factor \(\beta\) due to its reasonable complexity that makes it one of the most popular models.

### 2.3 CCF factor modelling

The main assumption in the model of factor \(\beta\) (Fleming, 1974), is that each component \(i\) \((i = 1, \ldots, N)\) can be down due to:

- events that have effects only on the concerned component. The corresponding failure rates, called independents, are noted \(\lambda_{i}^{(i)}\).
- events that induce simultaneous failures of the system or sub-system components. The corresponding failure rates, called common cause, are noted \(\lambda_{i}^{(ccf)}\).

Factor \(\beta\) is defined as the failure probability due to a common cause given the occurrence of a failure. The expression of \(\beta\) is given by:

\[
\beta = \frac{\lambda_{i}^{(ccf)}}{\lambda_{i}^{(ccf)} + \lambda_{i}^{(i)}} = \frac{\lambda_{i}^{(ccf)}}{\lambda_{i}} \quad (3)
\]

Usually experts give a scalar estimation of the value of \(\beta\) involved in the performance analysis of the SIS. The choice of \(\beta\) directly induces the values of \(\lambda_{i}^{(ccf)}\) and of \(\lambda_{i}^{(i)}\) as explained by the following relations:

\[
\lambda_{i}^{(i)} = (1 - \beta).\lambda_{i} \quad \text{and} \quad \lambda_{i}^{(ccf)} = \beta.\lambda_{i} \quad (4)
\]

According to 2 and 4, the various rates of the detected and undetected dangerous failures become:

\[
\begin{align*}
\lambda_{DD}^{(i)} &= (1 - \beta).\lambda_{DD} = (1 - \beta)DC.\lambda_D \\
\lambda_{DU}^{(i)} &= \beta.\lambda_{DU} = \beta(1 - DC).\lambda_D \\
\lambda_{DD}^{(ccf)} &= (1 - \beta).\lambda_{DD} = (1 - \beta)DC.\lambda_D \\
\lambda_{DU}^{(ccf)} &= \beta.\lambda_{DU} = \beta(1 - DC).\lambda_D
\end{align*}
\]

\(\beta_D\) and \(\beta\) respectively represent the proportion of detected and undetected common cause failures related to the diagnosis coverage rate \(DC\).

Computing the PFDoD_{avg} involves the components failure rates and also the CCF factors. A CCF is a multiple failure potentially leading to failure of the safety function. Thus, CCFs can result in the SIS failing to function when there is a process demand.

As previously mentioned, the performance evaluation must be obtained by quantitative methods and Markov chains are well suitable models (Dutuit et al., 2008).

### 2.4 Multiphase Markov Chains

Before introducing our approach concerning fuzzy multiphase Markov chain, let us recall some basic elements. The transition law of a Markov chain and the Chapman-Kolmogorov formula defined by 6 help to compute the probability distribution:

\[
p^{(n)} = p^{(n-1)}.A = p^{(0)}.A^n \quad (6)
\]

where \(p^{(0)}\) represents the probability vector of states at the initial time, \(p^{(n)}\) of dimension \((1 \times r)\) is the probability distribution of states at time \(n\) and, \(A\) of dimension \((r \times r)\) is the transition matrix.

The probability of each state \(S_j\) at each time \(n\) is computed by:

\[
p^{(n)}(S_j) = \sum_i p^{(n-1)}(S_i).a_{ij} \quad (7)
\]

where \(p^{(n)}(S_j)\) represents the probability of being in state \(S_j\) at time \(n\) and \(a_{ij}\) represents the transition probability from state \(S_i\) to state \(S_j\).

The state of a SIS is known at the test instants and its probability distribution on states is known. By considering one test interval, a matrix \(M\) allowing the assignment of the probability distribution to be in the various states \(S_j\) at inspection times \((k,t_i)\) towards the probability distribution of the various states \(S_j\) at time \((k,t_i + \Delta t)\) can be defined (see eq. 8).

\[
p^{(k,t_i+\Delta t)} = M.p^{(k,t_i)} \quad (8)
\]
with \( k \in \mathbb{N}, t_i \in \mathbb{R}, k.t_i \) are the inspection instants and \( \Delta t \) is the time period of the Markov chain.

As SIS are composed of several subsystems and components and, thanks to the test strategy chosen, it is possible that several transition matrices \( M_i \) are used during the SIS mission time even if the inspections are normally repeated with constant times intervals (Dutuit et al., 2008). Thanks to (6), (7), and (8), we can determine the probability of failure on demand of the SIS.

The \( PFD_{avg} \) which is the main reference to qualify the SIS performance is then computed by a discrete time integration using 9:

\[
PFD_{avg} = \frac{1}{n \Delta t} \sum_{k=0}^{n} \sum_{S_i} p^{(k)}(S_j) \Delta t \tag{9}
\]

with \( n \Delta t \in [0, T_M], T_M \) the mission time, \( S_j \) the states of dangerous failure and, \( P^{(k)}(S_j) \) the probability of being in one of these states at time \( t.k \).

### 3. IMPRECISE PERFORMANCE EVALUATION

When SIS are in low demand mode, feedback data is weak and handled probabilities may seem weakly credible, referring to the uncertainty principle (what is precise is more uncertain). The uncertainty on a parameter can be represented in several ways. A probabilistic view based on the Monte Carlo sampling led to the modelling of uncertain parameters by a uniform distribution on the set of values the parameters can take. Another simple representation of imprecision is obtained by interval valued probabilities (Buckley, 2005) where no assumption is made about the distribution. However, in some cases experts can provide more information than a single interval. For example, they can provide a series of nested intervals associated to a level of confidence they have on each interval of values, provided or they can optionally specify the value directly in a linguistic form. These representations correspond to the fuzzy numbers defined by Zadeh (1965).

#### 3.1 Fuzzy numbers

A fuzzy sub-set \( \tilde{A} \) on a universe of discourse \( \Omega \) is characterised by a membership function \( \mu_{\tilde{A}} \) which associates each element \( x \) of \( \Omega \) to a real number in \([0, 1]\):

\[
\mu_{\tilde{A}} : \Omega \rightarrow [0, 1] \tag{10}
\]

A fuzzy number is a subset satisfying the following conditions (Zadeh, 1965):

- \( \mu_{\tilde{A}}(x) \) is piecewise continuous.
- \( \mu_{\tilde{A}}(x) \) is convex.
- \( \mu_{\tilde{A}}(x) \) is normal (a value \( x_0 \) exists such that \( \mu_{\tilde{A}}(x_0) = 1 \)).

Let’s written \( L \rightarrow R \) fuzzy number as a 3-tuple \( \tilde{M} = \langle m, a, b \rangle > R. m \) is its modal value with \( \mu_{\tilde{M}}(m) = 1 \) i.e. the most waited value. \( a \) is the length of the support on the left of \( m \), also called the left spread parameter and \( b \) is the right spread parameter, on the real axis or to \([0, 1]\) for the probability case. The interest of \( L \rightarrow R \) fuzzy numbers is their ability to represent singular values, intervals, fuzzy numbers or fuzzy intervals. We can characterise a triangular fuzzy number by a set of nested intervals at different cut levels \( \alpha \). Indeed, if we consider a fuzzy number \( \tilde{A} \) with the membership function \( \mu_{\tilde{A}}(x) \), we obtain several nested intervals by using the \( \alpha \)-cut method (Kaufman and Gupta, 1991.). Thus, a convex interval is created by the \( \alpha \)-cut with a confidence index \((1 - \alpha)\). Each interval of level \( \alpha \) is bounded by its left bound \( A_L^{(\alpha)} \) and its right bound \( A_R^{(\alpha)} \). Thus, the fuzzy number can be represented by all its nested \( \alpha \)-cuts as follows:

\[
\tilde{A} \rightarrow [A_L^{(\alpha)}, A_R^{(\alpha)}], 0 \leq \alpha \leq 1 \tag{11}
\]

In addition, fuzzy numbers respect the property of monotonic inclusion which specifies that at a given level of knowledge the less precise a proposal is the more certain it is. Thus, we can write the monotony of inclusion for fuzzy numbers as:

\[
A^{(\alpha_1)} \subseteq A^{(\alpha_2)} \Rightarrow (1 - \alpha_1) \leq (1 - \alpha_2) \tag{12}
\]

An extension of the traditional approaches to take into account the imprecision is proposed by Buckley (2005). It takes as a starting point the extension principle of the traditional sets to the fuzzy sets proposed by Zadeh (1965). The approach proposed by Buckley (2005) consists in associating the fuzzy numbers of input variables and to combine them by using the concept of \( \alpha \)-cuts which brings back to an interval calculation problem.

#### 3.2 Fuzzy Markov Chains

Now, let’s suppose that \( a_{ij} \) are imprecise parameters represented by fuzzy numbers. For every coefficient \( a_{ij} \), a fuzzy value \( \tilde{a}_{ij} \) is associated. The following restriction on the \( \tilde{a}_{ij} \) holds: \( \tilde{a}_{ij} \) exists at least an \( a_{ij} \in \tilde{a}_{ij} \) so that \( \tilde{A} = (\tilde{a}_{ij}) \) is the transition matrix of the Markov chain (Buckley, 2005).

In order to compute \( \tilde{A}^{(\alpha)} \), the restricted multiplication of fuzzy matrices is defined. However, Buckley (2005) recalls the constraint on the transition matrix described by 13:

\[
C = \{a = (a_1, a_2, \ldots, a_r) | a_i \geq 0, \sum_{i=1}^{r} a_i = 1 \} \tag{13}
\]

where \( a_i \) is the \( i^{th} \) component of the vector \( a \).

Thus, the \( \alpha \)-cuts domain \( Dom[a] \) is defined by:

\[
Dom[a] = (\prod_{i=1}^{r} \tilde{a}_{ij}^{(\alpha)}) \cap C, \tag{14}
\]

with \( \tilde{a}_{ij}^{(\alpha)} \) the \( \alpha \)-cut of fuzzy transition probability \( \tilde{a}_{ij} \). 

\( Dom[a] \) is the Cartesian product of the \( r \) intervals \([a_{ij}, \tilde{a}_{ij}^{(\alpha)}] \) related to the level cuts \( \alpha \) producing a 'hyper-rectangle' in the space of dimension \( r \) which is intersected with set \( C \) (Buckley, 2005).

\[
Dom[a] = \prod_{j=1}^{r} Dom[a_j], 0 \leq \alpha \leq 1, 1 \leq j \leq r \tag{15}
\]
Considering \( f_{ij}^{(n)} \) a function of \((a_{11},\ldots,a_{rr}) \in \text{Dom}[\alpha] \), the lines of \( f_{ij}^{(n)} \) on \( \text{Dom}[\alpha] \) can be formulated as follows:

\[
\tilde{a}_{ij}^{(n),(\alpha)} = f_{ij}^{(n)}(\text{Dom}[\alpha])
\]  

(16)

In order to compute all \( \tilde{a}_{ij}^{(n),(\alpha)} \), the interval bounds have to be determined. For that, (17) should be solved (Buckley, 2005):

\[
\begin{align*}
\tilde{a}_{ij,L}^{(n),(\alpha)} &= \arg \min_{a_{ij}} f_{ij}^{(n)}(\text{Dom}[\alpha]) \\
\tilde{a}_{ij,R}^{(n),(\alpha)} &= \arg \max_{a_{ij}} f_{ij}^{(n)}(\text{Dom}[\alpha])
\end{align*}
\]

(17)

with \( \tilde{a}_{ij}^{(n),(\alpha)} \rightarrow [\tilde{a}_{ij,L}^{(n),(\alpha)}, \tilde{a}_{ij,R}^{(n),(\alpha)}] \), for all \( \alpha \).

The bounds defined for each \( \alpha \)-cuts in (17) are obtained by an optimization algorithm. It is thus a question of using the optimal formulation of the Markov chain in (6) and (17).

Fuzzy probability \( \tilde{p}^{(n),(\alpha)}(S_j) \) of being in different states \( S_j \) at instant \( n \) is computed by (18):

\[
\begin{align*}
\tilde{p}_{L}^{(n),(\alpha)}(S_j) &= \sum_{i} \tilde{p}^{(0)}(S_i) \cdot \tilde{a}_{ij,L}^{(n),(\alpha)} \\
\tilde{p}_{R}^{(n),(\alpha)}(S_j) &= \sum_{i} \tilde{p}^{(0)}(S_i) \cdot \tilde{a}_{ij,R}^{(n),(\alpha)}
\end{align*}
\]

(18)

3.3 Fuzzy modelling of SIS characteristic parameters

We model the imprecision of the CCF factor \( \beta \) by triangular fuzzy numbers as defined in section 3.1.

Fuzzy CCF factor \( \tilde{\beta}^{(\alpha)} \) is defined by the set of its \( \alpha \)-cuts. \( \tilde{\beta}^{(\alpha)} \) is the interval bounded by two values \([\beta_{L}^{(\alpha)}, \beta_{R}^{(\alpha)}] \). Parameter \( \tilde{\beta} \) integrates directly the characteristic transition matrix of the studied system. Then, we are dealing with fuzzy multiphase Markov chains which require the use of (18) to compute the upper and lower probabilities at several inspection times by (19):

\[
\begin{align*}
\tilde{p}_{L}^{(k,t_{i}+\Delta t),(\alpha)} &= M \cdot \tilde{p}_{L}^{(k,t_{i}),(\alpha)} \\
\tilde{p}_{R}^{(k,t_{i}+\Delta t),(\alpha)} &= M \cdot \tilde{p}_{R}^{(k,t_{i}),(\alpha)}
\end{align*}
\]

(19)

with \( k \in \mathbb{N}^{+} \).

The \( PFDA_{avg} \) is computed when the safety function is in low demand mode. It is equal to the average unavailability computed over the mission duration \( T_i \) or possibly on the test interval \([0,T_i] \), if all the components are simultaneously tested. As fuzzy numbers are involved in this approach, \( PFDA_{avg} \) is now computed by (20):

\[
PFDA_{avg} = \frac{1}{n \cdot \Delta t} \sum_{k=0}^{n} \sum_{S_j} \tilde{p}^{(k)}(S_j) \cdot \Delta t
\]

(20)

4. APPLICATION: STUDY OF A HIPS

A HIPS (High Integrity Protection System) is a SIS with a high safety integrity level. The system given in Fig. 1 has been studied in (Dutuit et al., 2008), and is used for application of the proposed approach. This HIPS is dedicated to the protection of the downstream portion of an offshore production system against overpressure due to its upstream (oil well W1). Three pressure sensors are responsible for detecting the pressure increase above a specified threshold. These three sensors send information to a logic solver (LS) which implements a 2oo3 logic. If at least two of the three signals received from sensors confirm the presence of an overpressure in the pipeline, the logic solver controls the opening of solenoid valve SV, which results in shutting off hydraulic supply that kept valve SDV open. Then, SDV is closed and reduces the risk of overpressure in the downstream circuit. The undesired event is the inhibition of the SIS which is characterized by the non-closure of the relief valve SDV.

Fig. 1. Studied HIPS

The studied HIPS is composed of:

- the sensor part structured in 2oo3 architecture, made up of three pressure sensors \( PT_i \), the logic unit part (Logic Solver) in 1oo1 architecture, the actuator part structured in 1oo2 architecture, made up by valves SV and SDV.

The reliability block diagram of the HIPS is given in Fig. 2.

Fig. 2. HIPS Reliability Block-Diagram

Our goal is to compute the probability of failure on demand of the SIS starting from its imprecise characteristic parameters such as the CCF factor, by using the fuzzy multiphase Markov chains (Dutuit et al., 2008). The HIPS \( PFDA_{avg} \) can be computed by the combination of probability of failure of all sub-system providing the set of safety function. This approach allows simplifying the model of the HIPS. It is expressed by the following formulas under the assumption of rare events:

\[
PFDA_{HIPS}^{(\alpha)} = \tilde{F}_{\text{Sens}}^{(\alpha)} + \tilde{F}_{\text{LS}}^{(\alpha)} + \tilde{F}_{\text{Act}}^{(\alpha)}
\]

(21)

where \( \tilde{F}_{\text{Sens}}^{(\alpha)} \), \( \tilde{F}_{\text{LS}}^{(\alpha)} \) and \( \tilde{F}_{\text{Act}}^{(\alpha)} \) represent respectively the fuzzy failure probability of the sensor layer, of the logic solver layer and of the actuator layer.

4.1 Epistemic approach

Using the fuzzy multiphase Markov chains method proposed in this paper associated to \( \alpha \)-cuts, the HIPS \( PFDA \) is determined according to the characteristic parameters.
of components modelled by fuzzy numbers. The characteristic parameters of the HIPS components are given in table 2. The CCF factor $\beta$ of each subset of components is described by a 3-tuple of parameters $<m_i,a_i,b_i>$ provided by only one expert. Considering only the imprecision on $\beta$, we can evaluate its influence on the SIS performance. The reader can note that multiple experts can provide fuzzy numbers but aggregated values (see e.g. (Simon and Weber, 2009)) are to be provided before computing the fuzzy Markov chain.

<table>
<thead>
<tr>
<th>SIS Components</th>
<th>$\lambda_p(h^{-1})$</th>
<th>$DC(%)$</th>
<th>$MTTR(h)$</th>
<th>$T_i(h)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$PT_i$</td>
<td>$4.06e^{-5}$</td>
<td>0.3</td>
<td>5</td>
<td>730</td>
</tr>
<tr>
<td>$SDV$</td>
<td>$5.10e^{-7}$</td>
<td>0.1</td>
<td>8</td>
<td>1460</td>
</tr>
<tr>
<td>$SV$</td>
<td>$5.10e^{-7}$</td>
<td>0.1</td>
<td>8</td>
<td>1460</td>
</tr>
<tr>
<td>LogicSolver</td>
<td>$1.50e^{-7}$</td>
<td>0.7</td>
<td>10</td>
<td>2190</td>
</tr>
</tbody>
</table>

Table 2. Numerical data

To compute $PFD_{avg}$, a test interval time $T_i$ is associated to the test frequency of the HIPS. In this study, different test intervals are used for each subsystem. Moreover, we assume that each subsystem is functionally tested independently from each other.

Fig. 3 described the multiphase Markov chain of the sensor layer. From the initial state 1 where all components are OK, the detected failure of one sensor gives a transition to state 2 with probability $3(1 - \beta_D)\lambda_{DD}$.

![Fig. 3. Multiphase Markov model of sensors subsystem](image)

The repair of this failed component is considered with the repair rate $\mu_{DD}$. Similarly, the undetected failure of one out of the sensors can occur with the probability $3(1 - \beta_D)\lambda_{DD}$ and allows a transition from state 1 to state 3. The sensor layer is OK in states 1, 2 and 3. From states 2 and 3, a new failure (detected or not) can occur and causes the failure of the layer (state 4, 5, 6, 7 and 8) and thus the failure of the HIPS. The occupation probabilities of states at the starting time $d_i$ of phase $i$ are computed from those obtained at final time $f_{i-1}$ in the end of period ($i - 1$) through (22):

$$p_i(d_i) = M.p_i(f_{i-1}), i = 1, ..., 8$$

$$\begin{bmatrix}
    p_1(d_i) \\
    p_2(d_i) \\
    p_3(d_i) \\
    p_4(d_i) \\
    p_5(d_i) \\
    p_6(d_i) \\
    p_7(d_i) \\
    p_8(d_i)
\end{bmatrix} = \begin{bmatrix}
    1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix} \begin{bmatrix}
    p_1(f_{i-1}) \\
    p_2(f_{i-1}) \\
    p_3(f_{i-1}) \\
    p_4(f_{i-1}) \\
    p_5(f_{i-1}) \\
    p_6(f_{i-1}) \\
    p_7(f_{i-1}) \\
    p_8(f_{i-1})
\end{bmatrix}$$

where $M$ is the passage matrix between two contiguous phases.

From the Markov graph represented in Fig. 3, the proposed fuzzy approach to compute the upper and lower bounds of the 2oo3 architecture $PFD_{avg}$ for each $\alpha$-cut is applied by using (19) and (22).

The HIPS $P\tilde{FD}_{avg}$ is computed by the combination of the failure probability of all subsystems providing together the safety function according to (21).

![Fig. 4. $P\tilde{FD}$ and $P\tilde{FD}_{avg}$ of the HIPS](image)

Fig. 4 shows the fuzzy HIPS unavailability $P\tilde{FD}(t)$ and its average value $P\tilde{FD}_{avg}$ for ($\alpha = 0$). We determine, for each $\alpha$-cut, the upper and lower bounds of the fuzzy HIPS $P\tilde{FD}_{avg}$.

The resulting $PFD(\alpha=0)$ varies between two bounds. In the case where, the $PFD$ is maximum, the HIPS passes more than 64% of its time in the SIL 3 domain, which leads to an average value, $PFD_{avg}$ is equal to $1.112 \times 10^{-4}$. Whereas the variation of the $PFD$ minimal, allows to classify the HIPS on SIL 4 level.

![Fig. 5. Fuzzy $P\tilde{FD}_{avg}$ of the HIPS](image)

Fig. 5 shows the triangular fuzzy number representing the imprecision on the HIPS $P\tilde{FD}_{avg}$ induced by the imprecise CCF factors. The support of this fuzzy number varies from $0.836 \times 10^{-4}$ to $1.112 \times 10^{-4}$ for ($\alpha = 0$) which corresponds to a confidence degree of 100%. In this case, the SIL of the studied HIPS varies from a SIL4 ($PFD_{avg} \in [10^{-5}, 10^{-4}]$) to SIL3 ($PFD_{avg} \in [10^{-4}, 10^{-3}]$) according to table 1.

As shown, the imprecision on the CCF factors lead to a possible change in the HIPS level of SIL. If the SIL target is SIL 3, the uncertainty on the HIPS has no influence. The
HIPS is perhaps too efficient and costly. But, if the SIL target is SIL 4, the HIPS SIL level is clearly uncertain due to epistemic uncertainty on \( \beta \). If we seek a performance classification without ambiguity, it is then necessary to change either the set of components or the SIS architecture (level of redundancy) or increase our knowledge on the CCF factors to reduce its uncertainty.

### 4.2 Aleatory approach

When dealing with imperfect knowledge in the probability framework, dependability studies of systems consider probability distributions. This section is dedicated to show the exactness of our previous results by considering second order probabilities in this section. By considering the value of \( \beta \) within a range corresponding to the support of the fuzzy number \([(\beta_L^{(0)}, \beta_R^{(0)})]_e\), the insufficient principle of Laplace (everything which is equiplausible is equiprobable) leads us to consider uniform probability distribution over the range \([\beta_L^{(0)}, \beta_R^{(0)}]_L\) defined by (23). The considered values for the distribution are taken in table 2:

\[
\beta_i \rightarrow U(\beta_i^{(0)}_L, \beta_i^{(0)}_R)
\]  

(23)

Thanks to a Monte Carlo sampling, we can determine the distribution of \( \text{PFD}_{avg} \) modelled by the multiphase Markov chains through (7). For this experiment, the Monte Carlo sampling consists in randomly choosing 2000 3-tuples of values for \( \beta \) according to (23). The distribution of the \( \text{PFD}_{avg} \) is represented in Fig. 6.

![Fig. 6. Distribution of \( \text{PFD}_{avg} \)](image1)

This distribution can be compared to a normal distribution (central limit theorem) but our interest for sake of comparison is the variation range. From this distribution, we can compute the lower and upper bounds of \( \text{PFD}_{avg} \):

\[
\text{PFD}_{avg} \in [0.845e^{-4}, 1.078e^{-4}].
\]

The support of \( \tilde{\text{PFD}}_{avg} \) is \([0.836e^{-4}, 1.112e^{-4}]\) and contains the upper and lower bounds of the probability distribution obtained by Monte Carlo sampling. Nevertheless, to obtain the same results with a Monte Carlo sampling method, the number of samples should increase towards infinity.

5. CONCLUSION

In this article, a fuzzy approach in Markov chains to analyze the SIS performances in low demand mode has been proposed. This approach is based on the use of fuzzy numbers since CCF factors are poorly known and can be estimated by experts in a linguistic form. By considering \( L-R \) fuzzy numbers to represent CCF factors, the paper shows the influence on the \( \text{PFD}_{avg} \). The proposed approach gives guaranteed results without pessimism due to repeated events and can be extended to other kind of system, parameters or evaluation method. Its application to multiphase Markov chains for the evaluation of the SIS performance leads to exact results that cannot be obtained from Monte Carlo Markov chains.

## REFERENCES


