Chapter

# Functional Safety of FPGA Fuzzy Logic Controller

*Mohammed Bsiss and Amami Benaissa*

## Abstract

In this paper we describe a methodology to implement a fuzzy logic controller in FPGA. The implementation of fuzzy logic controller (FLC) in FPGA requires a qualitative and a quantitative analysis to define the system safety integrity level (SIL). This level can be defined by the quantification of the probability of failure on demand (PFDavg). We propose to analyze the implementation advance safety architecture of fuzzy logic controllers with 1-out-of-2 controllers (1oo2) in FPGA using the reliability block diagram (RBD) and the Markov model. We demonstrate how from hardware characteristics parameters, such as rate of dangerous detected failure and undetected failure, the diagnostic coverage, proof test interval and other parameters to evaluate the PFDavg.

**Keywords:** fuzzy logic controller, safety integrity level (SIL), mean time to failure (MTTF), safe failure fraction (SFF), reliability block diagram (RBD), Markov model, average probability of dangerous failure on demand (PFDavg), field programmable gate array (FPGA), IEC standard 61508

## 1. Introduction

A synthesize fuzzy logic controller in field programmable gate array FPGA means that the VHDL code writing for the systems will be translated into gate, multiplexer, registers RAM, etc. Very low-level FPGA faults to high-level system hazards and common cause faults can put the FPGA-based systems in a dangerous state [1].

However, safety-related issues for FPGA-based systems remain to be not only verified but also following a safe methodology to design, implementation and evaluation such systems.

According to [2] the FPGA chip is classified as a type B with very complex structure. The first step was to perform failure modes, effects, and diagnostic analysis (FMEDA) for the safety related FPGA-based fuzzy logic controller.

FMEDA is a systematic process used in the development stage of an integrated circuit to ensure that it meets the pre-determined safety requirements. In the FMEDA, each component implemented in our FPGA is analyzed for possible failures and the consequences of these failures on the system.

The design, implementation and evaluation of a fuzzy logic controller in the field programmable gate array require a qualitative and quantitative analysis according to IEC 61508. Due to their usage in critical applications, the FLC have a very stringent average probability of failure on demand (PFDavg) requirement.

This requirement is usually determined by industry standards, such as the safety integrity level (SIL) rankings. The SIL is defined as a relative level of risk reduction provides by a safety function for safety function our FPGA-based FLC.

The safety function performed by the FLC maintains a safe state of the system relative to specific hazardous failures.

The four levels used in IEC 61508 are defined in **Table 1** [5] for various fractions of failures leading to a safe state as follows:

| Safety integrity level | Probably of failure on demand |
|---|---|
| SIL4 | $10^{-4}$ to $10^{-5}$ |
| SIL3 | $10^{-3}$ to $10^{-4}$ |
| SIL2 | $10^{-2}$ to $10^{-3}$ |
| SIL1 | $10^{-1}$ to $10^{-2}$ |

**Table 1.**
*Definition of SILs for low demand mode from IEC 61508-1.*

## 2. Definition and assumptions

### 2.1 Definition

Presented below is a glossary of terminology on topics related to functional safety used in this paper.

**Diagnostic coverage** represents the probability of discovering a failure. Diagnostic coverage of the test according to the safety standard Norm IEC 61508 is defined as the ratio of the rate of detected dangerous failures (by a diagnostic test) on the total failure of detected and undetected dangerous failure.

**Safe failure fraction** is used for calculating safety integrity levels (SIL).

**Mean time to failure** is the average time to the first failure.

**Mean time between failure (MTTR)** is time between two failures.

**Probability of failure on demand (PFD)** is a probability on the time interval that the system could not perform the function of safety for which it was at the time or the application of this function is made.

**The safe failure fraction** is defined by the ratio of average failures of safe $\lambda_S$ plus dangerous detected failures $\lambda_{DD}$ and safe plus dangerous detected and undetected $\lambda_{DU}$ failures. The calculation is based on the architecture of FLC and on a functional analysis by carrying out a Failure Modes Effects and Diagnostic Analysis (FMEDA).

**Safety integrity level (SIL)** – Given a SIL to a system is a decision to be taken in consequence of process hazard and risk analysis. SIL defines the probability of dangerous failure that a system can be authorized. There are four possibility levels (SIL1, SIL2, SIL3 and SIL4) defined by safety norm IEC 61508 [2].

**Component type A.** All failure modes are known and can be detected. The value of the security factor S for components of type A on a worst-case is defined as S = 10% [3].

**Component type B.** All failure modes are not completely known. The value of the security factor S for components of type B on a worst-case is defined as S = 50%.

**Proof test T-proof** is periodic tests offline directed to detect failures in a system so that the system can be repaired to return in a state equivalent to its initial state.

**Diagnostic test**s are online test to detect hazardous failure. The diagnostic tests have an in fluent at the level of component (internal) but not at the level of the function of the security. The watchdog Test, Walking Bit Test and Ram Test are some example of diagnostic test.

**Common mode failure** refers to the simultaneous failure that can appear in two or more channels in a system multiple channels. The introduction of common-mode failures is generally represented by a factor of β. The 61,508 standard distinguishes two types of factor for non-detected dangerous failures and detected dangerous failures. The values for the factors Beta and are generally between 0.5% and 5% [4].

**1oo2 architecture (one-out-of-two)** consists of two channels perform each security function. The security function is executed once a channel request. Only any dangerous failure will lead to the failure of the function of application of both channels to lead to the failure of the security function on demand.

**Reliability block diagram** is a safety analysis for SIL selection for estimating the performance of systems, other methods are fault tree [6] analysis and Markov diagrams [7].

### 2.2 Assumptions

The technique and results developed in this paper are based on the assumptions following:

- Component failure and repair rate is assumed a constant failure over the life of the system.
- The hardware failure rates used as inputs to the calculations for a single channel of the subsystem
- All channels in a voted group have the same failure rate and diagnostic coverage rate.
- The proof test interval is at least one order of magnitude greater than the diagnostic test interval
- The demand rate and expected interval between demands are not considered.
- For each component of the safety system, the PFDavg is calculated, for simplification only from the undetected dangerous failure rate, $\lambda_{DU}$ given in **Table 3** and the proof test interval, Ti.

Other assumptions can be referred to the Annex B of IEC 61508-6.

## 3. Architecture of fuzzy logic controller

For a simple architecture 1 out of 1 (1oo1), the fuzzy logic controller (FLC) contains a fuzzification process to change a real scalar input value to fuzzy value, a fuzzy inference engine for rule based expert systems and defuzzification to change fuzzy value into real scalar output. **Figure 1** presents the basis block diagram of simple fuzzy logic controller.

The parameter characterizing the present FLC are summarized in **Table 2**.

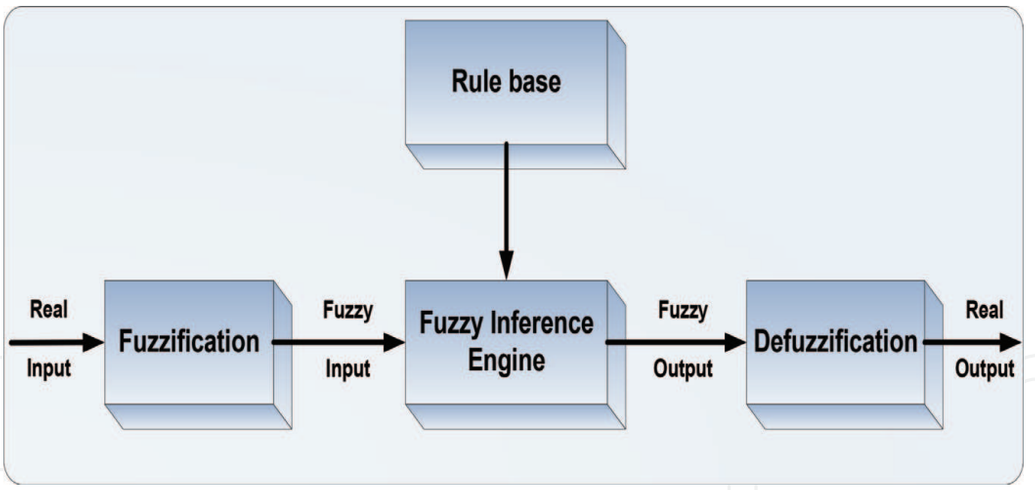


**Figure 1.**
*Basis block diagram of simple fuzzy logic controller.*

| **Fuzzy inference system** | |
|---|---|
| Inputs | 2 |
| Outputs | 1 |
| Outputs resolution | 12 bits |
| Antecedent MF's | 7 trapezoidal |
| Antecedent MF resolution | 14 bits |
| Consequent MF's | 3 singleton |
| Antecedent MF resolution | 12 bits |
| Aggregation method | Mandani Min-Max |
| Implication method | Product operator |
| Defuzzification | Weighted average |

**Table 2.**
*The parameter characterizing FLC.*

The FLC has two inputs, one with four linguistic terms and the other with three and an output with three linguistic terms. This makes a total of $4 \times 3 \times 3$ different rules that may be sued to describe the strategy of total control (**Figure 2**).

The FPGA-based fuzzy logic controller consists of two fuzzy logic controller (FLC) with the fuzzification process; rule evaluation process and defuzzification process in a redundant architecture (**Figure 3**).

In this kind of redundancy, the failure of one channel does not prevent the execution of the safety function. This architecture will be in dangerous state when both FLC have dangerous failures. The main advantage of this architecture is his low probability of failure on demand. Each FLC has diagnostic tests and the results of both FLC are controlled by the comparison module (**Figure 3**).

The safety function performed by the FLC maintains a safe state of the system relative to specific hazardous failures. The safety function is therefore the power loss for the analog outputs (de-energize-to-trip) of the system in case of dangerous failures by on-line diagnostics tests. These failures can be interconnect faults, stuck-at-fault, transition faults, the clock phase shift or a deviation of the value obtained respectively from the both controller.

**Figure 3** shows a basic model for a fuzzy logic controller with redundancy architecture 1oo2 designed in FPGA.

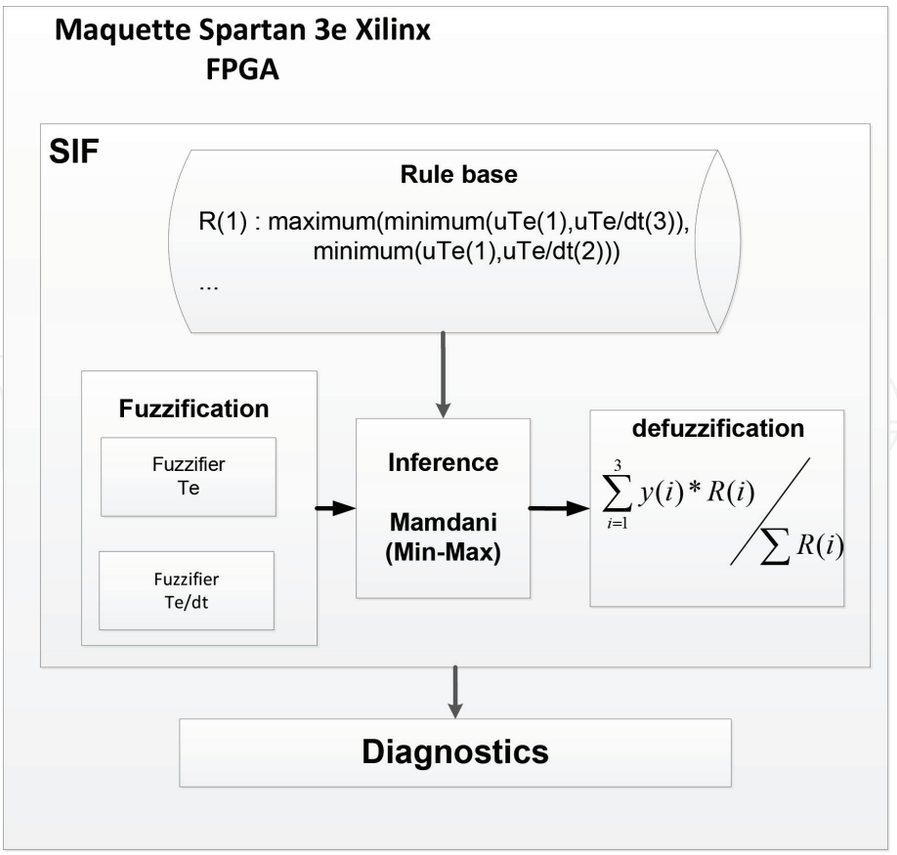


**Figure 2.**
*Design of the present implemented FLC on FPGA.*

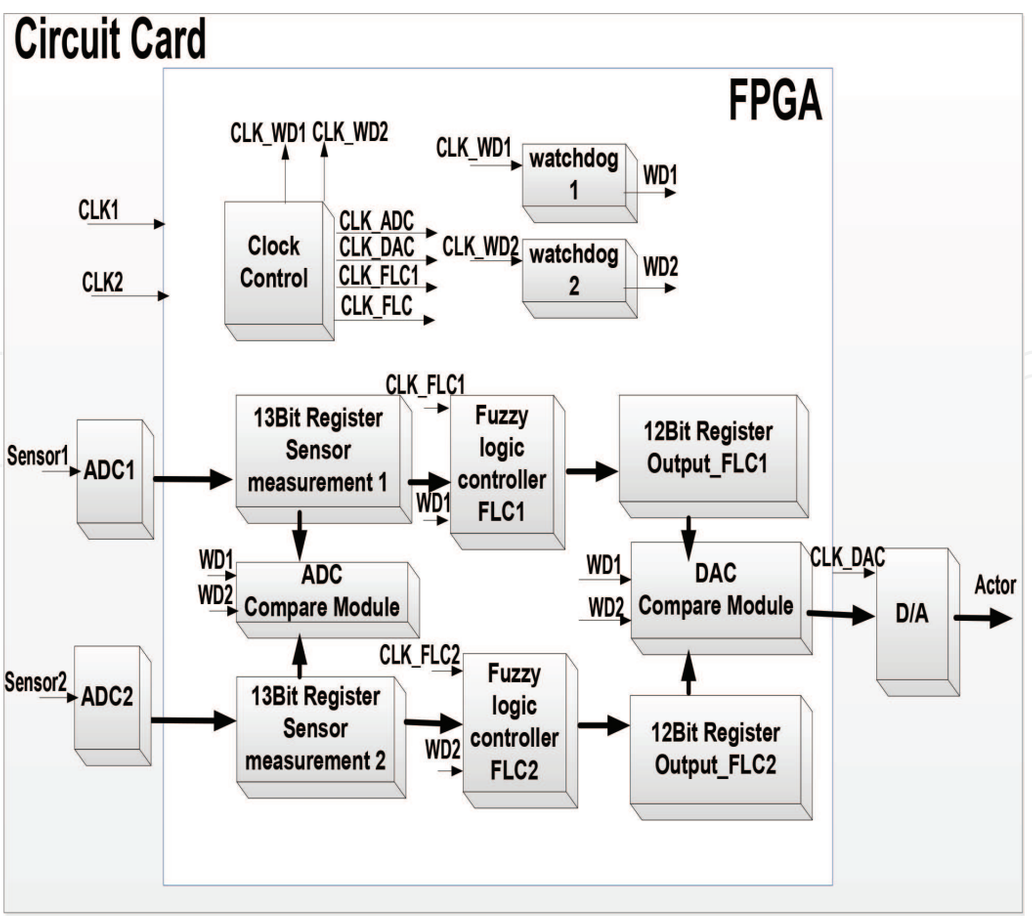


**Figure 3.**
*Block diagram of the fuzzy logic controller with 1oo2 structure.*

## 4. RBD and Markov model for safety integrity verification

### 4.1 Reliability block diagram

The reliability block diagram is a graphical representation of the system. Each component is represented by a function block in accordance with their logical relation of reliability (**Figure 4**). A series connection represent logic "and" of component and parallel connections represents logic "or", even as combination of series and parallel connections represents voting logic.

If a component fails in a series combination, the corresponding connection will be cut off. Conversely, in a parallel combination, the operation of a single instance is sufficient for the passage of the signal. System shutdown is only possible if all parallel instances fail.

**Figure 4** presents the reliability block diagram associated to the fuzzy logic controller with the 1oo2 structure. We take in consideration that the components have only two operating states (correct or faulty operation).

### 4.2 Auto diagnostic and common cause

The first step was to perform a failure modes, effects, and diagnostic analysis (FMEDA) to detecting the hazardous hardware failures of systems. A failure is called safe if it does not put the FLC in a dangerous state when a hazardous fault occurs. A dangerous failure puts the logic controller in a potentially dangerous state and makes the system inoperative.

They are failure rates partitioned into four categories:

- Safe failure rate $\lambda_s$ - do not have the potential to put the system in an hazardous state and is equal to the sum of safe detected failure rates $\lambda_{SD}$ and safe undetected failure rate $\lambda_{SU}$

- Dangerous failure rate $\lambda_D$ - have the potential to put the system in an hazardous state and is equal to the sum of dangerous detected failure rates $\lambda_{DD}$ and dangerous undetected failure rate $\lambda_{DU}$

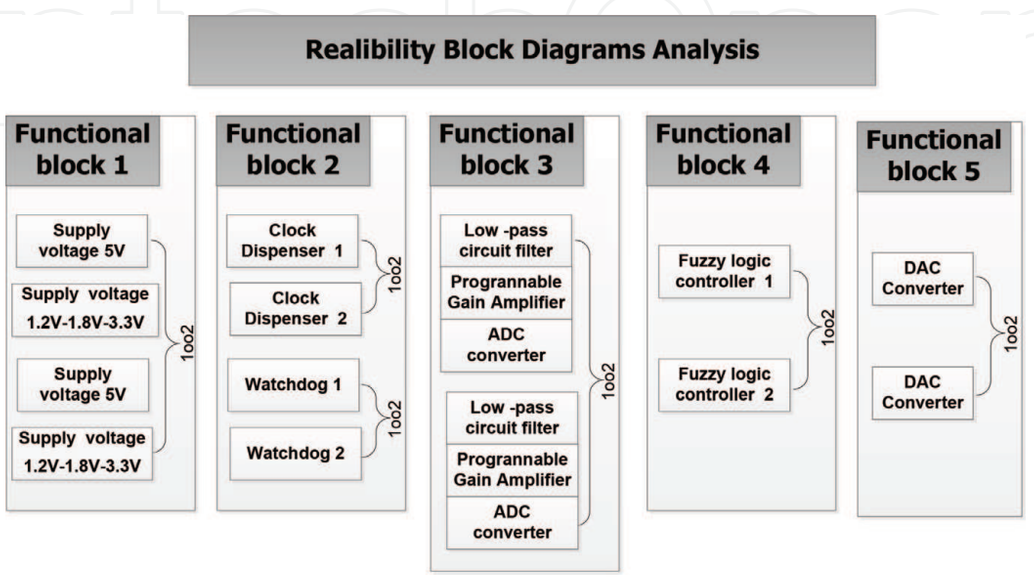


**Figure 4.**
*Reliability block diagrams analysis.*

- Dangerous detected failure $\lambda_{DD}$ - is detected by the on-line diagnostics tests and the system will be placed into safe state.

- Dangerous undetected failure $\lambda_{DU}$ - is undetected by on-line diagnostics tests and the system will not be placed into safe state.

By redundancy systems the combination of on-line diagnostic and common-cause was included. Since the failure is partitioned into eight categories [7].

- Safe, detected normal $\lambda_{SDN}$
- Safe, detected, common-cause $\lambda_{SDC}$
- Safe, undetected normal $\lambda_{SUN}$
- Safe, undetected common cause $\lambda_{SUC}$
- Dangerous, detected normal $\lambda_{DDN}$
- Dangerous, detected, common-cause $\lambda_{DDC}$
- Dangerous, undetected normal $\lambda_{DUN}$
- Dangerous, undetected common cause $\lambda_{DUC}$

The possible failures of the fuzzy inference engine implemented in FPGA and their classification are presented in **Table 3**.

| Type of failure | Potential causes | Diagnostic test | Classification of failure |
|---|---|---|---|
| Hazardous hardware failure in module fuzzification | Stuck-at Low or Stuck-at High anomaly at the internal FPGA component | Periodic comparison of the result of the redundancy controllers. | Dangerous detected Failure $\lambda_{DD}$ |
| Hazardous hardware failure in module inference rule | | | |
| Hazardous hardware failure in module defuzzification | | | |
| Failure of an internal element that does not intervene in the logic implemented in FPGA | Stuck-at Low or Stuck-at High anomaly at the internal FPGA component | No diagnostic | Since it does not affect the security function of the FLC then it is an undetected safe failure $\lambda_{SU}$ |
| Flash memory failure where logic (VHDL code) is stored. | Hardware fault, electrostatic disturbance, magnetic waves, high voltage frequencies, etc. | Examining of cyclic redundancy value | A failure in the flash memory during FLC operation can be detected only after the mission time delay Ti. It can therefore be classified as a detected safe failure $\lambda_{SD}$ |
| The drift of the clock | | Examining via eatchdog circuit | Dangerous detected Failure $\lambda_{DD}$ |

**Table 3.**
*Failure mode distribution for functional block 3 (FLC).*

### 4.3 Quantitative analysis using RBD

The structure of reliability block diagram (RBD) defines the logical interactions of failures within a fuzzy logic controller implemented in FPGA. Each component of the fuzzy logic controller is a functional block connected by a series for output module DAC and parallel structure for measurement units. **Figure 4** presents the reliability block diagram associated to each component. The unreliability data for each subsystem components is given in **Table 4**. The probability PFDavg is calculated by summing the probability of failure of all the functional blocks of a FLC. The quantification of average frequency of dangerous failure of our safety function is giving by Eq. [8]:

$$PFDavg = 2\left((1-\beta_D)\lambda^{DD} + (1-\beta)\lambda^{DU}\right)^2 t_{CE} t_{GE} + \beta_D \lambda^{DD} MTTR + \beta\lambda^{DU}\left(\frac{T_i}{2} + MTTR\right) \tag{1}$$

The time of unavailability of a channel $t_{CE}$ due to a detected dangerous failure is given by the following formula [8]:

$$t_{CE} = \frac{\lambda^{DU}}{\lambda^{D}}\left(\frac{T_i}{2} + MTTR\right) + \frac{\lambda^{DD}}{\lambda^{D}} MTTR \tag{2}$$

The time of unavailability of the other channel $t_{GE}$ is also added because of detected dangerous failure which is represented by the following formula [8]:

$$t_{GE} = \frac{\lambda^{DU}}{\lambda^{D}}\left(\frac{T_i}{3} + MTTR\right) + \frac{\lambda^{DD}}{\lambda^{D}} MTTR \tag{3}$$

This result gives a PFDavg of 2.7426E−03, which corresponds to a safety integrity level of SIL2.

The subsystem PFDavg contribution for the supply voltage is 2.1920E−03, for the fuzzy controller implemented in FPGA is 7.3616E−06. That means that the on-line diagnostics tests implemented for FLC systems in FPGA is with high performance and efficiency (**Figure 5**).

### 4.4 Quantitative analysis using Markov model

Markov modeling brings a good reliability and safety techniques for qualitative and quantitative analysis that uses state diagrams. This method take account for a realistic repair time, probability of correct repair, proof test effectiveness, and automatic diagnostic testing. The Markov system model for redundancy structure

| Component | HFT | PFDavg | % of total PFDavg | *SFF* |
|---|---|---|---|---|
| Supply power | 1 | 2.1920E−03 | 82.93% | 90.000% |
| Clock dispenser | 1 | 1.8785E−04 | 6.84% | 92.059% |
| ADC converter | 1 | 2.1818E−04 | 7.95% | 90.235% |
| Fuzzy controller | 1 | 7.3616E−06 | 0.68% | 99.500% |
| DAC controller | 1 | 5.4770E−05 | 1.99% | 95.000% |
| Total | | **2.7426E−03** | **100%** | **92.57%** |

**Table 4.**
*Failure mode distribution and SIL performance analysis for FLC system.*

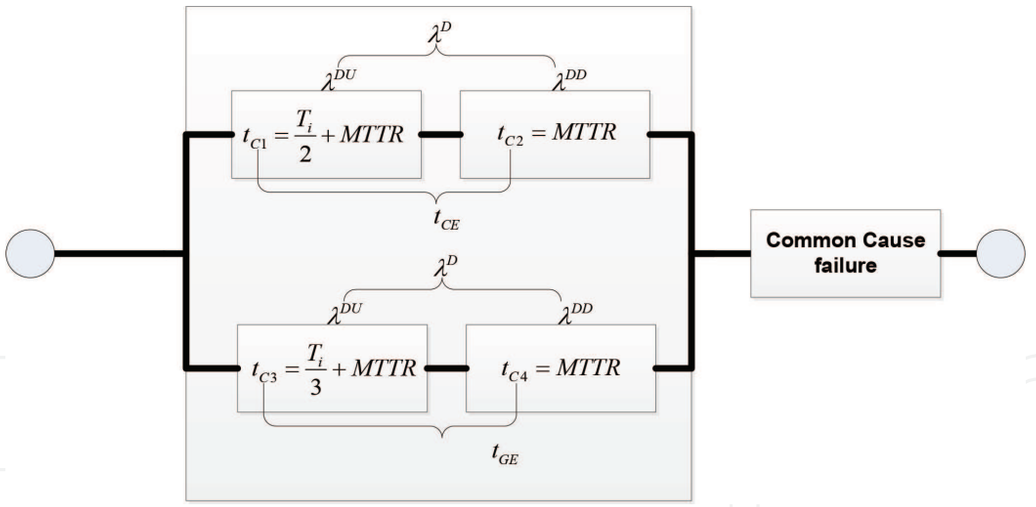


**Figure 5.**
*Schematic design of the reliability principle (1oo2).*

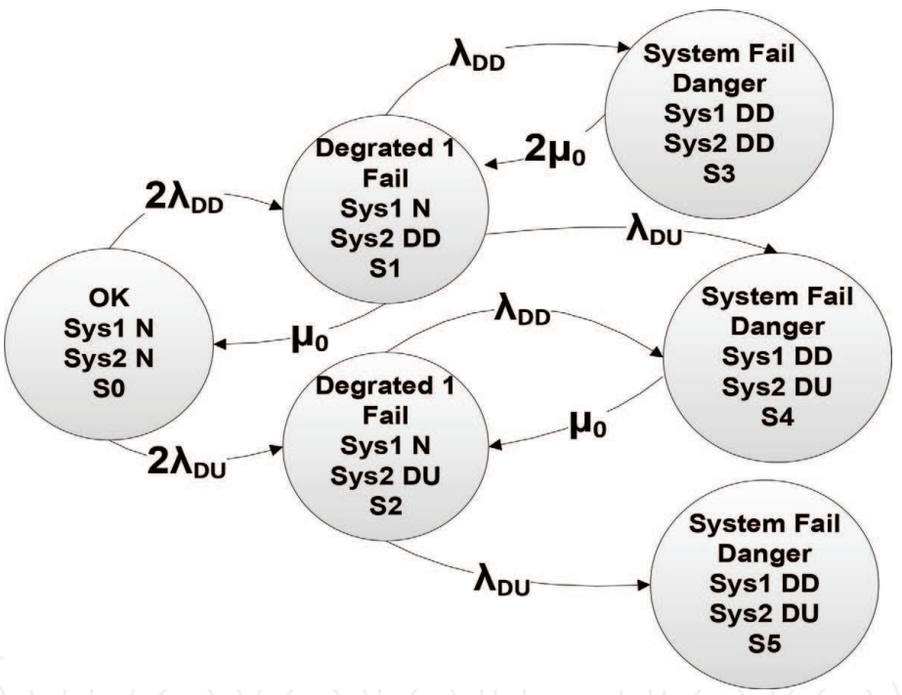


**Figure 6.**
*Markov model of the 1oo2 architecture diagnostic (no common cause).*

1oo2 with only on-line diagnostic is presented in **Figure 6**. This Markov model of the 1oo2 architecture contains 6 states [7]:

- The first state (S0): specifies the normal state where the booth controller properly works.
- The second state (S1): specifies the state where one controller of the system has a dangerous detected failure by diagnostic with transition probability of $2\lambda_{DD}$. The system can be repaired according to the transition rates $\mu_0$.
- The third state (S2): specifies the state where one controller of the system has a dangerous undetected failure with transition probability of $2\lambda_{DU}$ and the second work properly.

- States (S3), (S4) and (S5): specify a system fail state, where the booth controllers have a dangerous detected failure by on-line diagnostics tests (S3), or one controller has a dangerous detected failure also by on-line diagnostics tests and the other has a dangerous undetected failure (S4), or the booth channels have a dangerous undetected failure (S5) by on-line diagnostics tests.

A Markov model of 1oo2 structure that take in consideration combination of different failure modes, on-line diagnostic and common cause is draw in **Figure** 7 with six states [7].

It has the same state combinations as **Figure 6** with two additional failure lines. There is a dangerous detected common-cause failure rate from state (S0) to state (S3) and a dangerous undetected common-cause failure rate from state S0 directly to state (S5). The Markov model of the 1oo2 architecture contains 6 states, in that case the transition matrix P with dimension $(6 \times 6)$ is given by [7].

$$p = \begin{bmatrix} 1-(\lambda_{DC}+2\lambda_{DN}) & 2\lambda_{DDN} & 2\lambda_{DUN} & 2\lambda_{DDC} & 0 & \lambda_{DUC} \\ \mu_0 & 1-(\lambda_D+\mu_0) & 0 & \lambda_{DD} & \lambda_{DU} & 0 \\ 0 & 0 & 1-\lambda_D & 0 & \lambda_{DD} & \lambda_{DU} \\ 0 & 2\mu_0 & 0 & 1-2\mu_0 & 0 & 0 \\ 0 & 0 & \mu_0 & 0 & 1-\mu_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (4)$$

The transition matrix P is a matrix showing the probabilities‘ distribution of different states in one time interval. This matrix can be multiplied by itself to get transition probabilities for different time intervals.

The FLC system is starting always by one particular state (S0), so it contains a single one and a quantity of zeros. The starting probability S would be:

$$S^0 = [1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0] \quad (5)$$

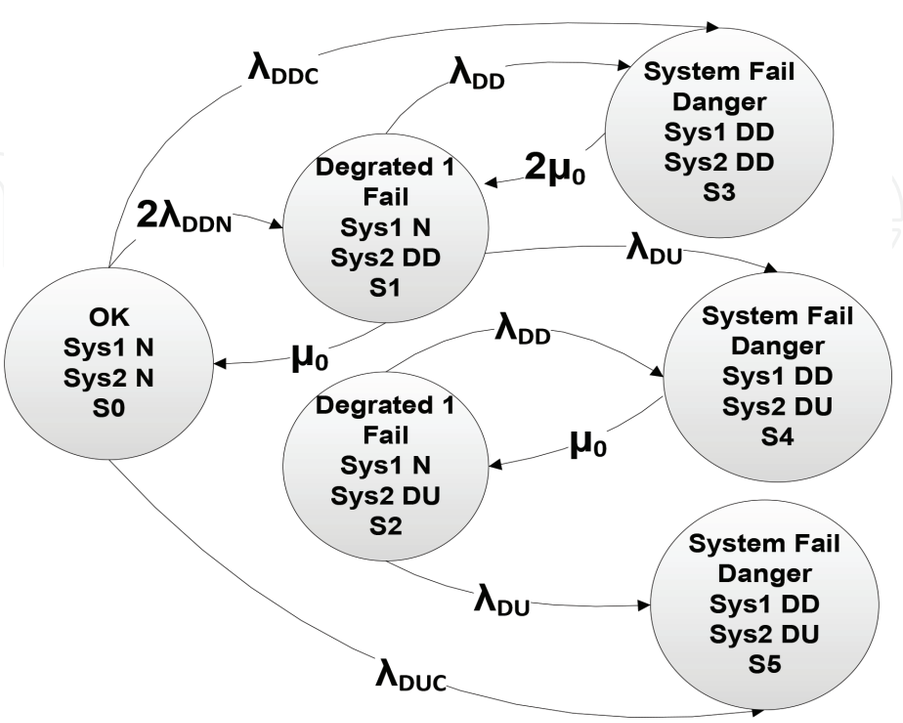


**Figure 7.**
*Markov model of the 1oo2 architecture—diagnostic and common cause.*

It means that the probability to be in normal state at initial time is 100 and 0% for the other states.

After 1 year, the system average frequency of dangerous failure of the safety function is the sum of the of all functional components probabilities of the 1oo2 FLC systems:

$$PFD_{avg} = \sum PFD_{avg\_Subsystem} \tag{6}$$

The FLC with 1oo2 structure is always starts in state zero. After n hours, the calculation process of the distribution probabilities $S^n$ is:

$$S^1 = S^0 \times P$$
$$S^2 = S^1 \times P$$

This process can be continued as necessary.

$$S^3 = S^2 \times P$$
$$S^4 = S^3 \times P$$
$$\ldots$$
$$S^n = S^{n-1} \times P$$

The $S^n$ matrix for any particular time interval is obtained by multiplying $S^{n-1}$ times P. This process can be continued as necessary, and the probability distribution increases progressively each time, then that remains unchanged as time progresses. If $S^{n+1} = S^n$ a limiting state probability is reached. This matrix is labeled $P^L$.

$$S^L = S^n \times P = S^{n-1} \times P$$

The FLC with 1oo2 structure has a safe failure rate of 6.6302E−07 failures per hour and a dangerous failure rate of 1.9118E−07 failures per hour. On-line diagnostic detect 95% of dangerous failure and 92% of safe failure. When failures are detected, the average system repair time is 24 hours.

The beta factor β is estimated to be 2%. The failure rates are divided by diagnostic capability. The following failure rates result:

$$\lambda^{SD} = \lambda^S \times 0.92$$
$$\lambda^{SU} = \lambda^S \times (1 - 0.92)$$
$$\lambda^{DD} = \lambda^D \times 0.95$$
$$\lambda^{DU} = \lambda^D \times (1 - 0.95)$$

These failure rates are multiplied by beta factor using following equations:

$$\lambda^{SDN} = (1 - \beta) \times \lambda^{SD}$$
$$\lambda^{SDC} = \beta \times \lambda^{SD}$$
$$\lambda^{SUN} = (1 - \beta) \times \lambda^{SU}$$
$$\lambda^{SUC} = \beta \times \lambda^{SU}$$
$$\lambda^{DDN} = (1 - \beta) \times \lambda^{DD}$$
$$\lambda^{DDC} = \beta \times \lambda^{DD}$$
$$\lambda^{DUN} = (1 - \beta) \times \lambda^{DU}$$
$$\lambda^{DUC} = \beta \times \lambda^{DU}$$

Where the failure rates and repair rates are substituted into the transition matrix P, the following solving for limiting state probabilities, the results are:

$$S_0^L = 0.9583$$
$$S_1^L = 0.0095$$
$$S_2^L = 0.0095$$
$$S_3^L = 0.0093$$
$$S_4^L = 0.0097$$
$$S_5^L = 0.0038$$

Since the system is down (failed) in state 5, the predicted average steady-state downtime is 0.0038. The control system is successful in state S0, S1 and S2; therefore, we add the limiting state probability of the success states equal to 0.9773%.

## 5. Conclusion

Markov analysis is used to analyze different states that take the system during its life cycle. Markov analysis provides information on the probability of FLC.

This application contains several important assumptions. First, notice that in Markov models M-out-of-N the probabilities in each row sum to one. Second, the probabilities in Markov models will not change over time. Third, the states are independent over time. In a Markov process after a number of periods (500 hours) have passed, the probability will approach steady state. For our example, the steady-state probabilities are:

- 13.5E−3 per hour = probability of the FLC to be in a dangerous undetected failure.

- 1.9E−2 per hour = probability of FLC degraded system fail.

However, the reliability block diagram analysis is based on the IEC 61508 international standard in the calculation of PFDavg. This standard considers all the parameters defined previously and there is a difference between both type components A and B. The type of components allows identifying the safety factor which contributes directly in the calculation of the PFDavg. Despite this difference between both standards, both analysis methods give the same results.

The FLC with redundancy structure 1oo2 has a redundant architecture with two controllers adopted by the FLC and the watchdog. This architecture has a majority voting arrangement for the output signals. If only one FLC gives a result which disagrees with the other FLCs, the output state does not change.

The probability of FLC with 1oo2 architecture to be in a dangerous undetected failure is 2.7426E−03 per hour, which relocates the system safety integrity level to SIL2.

## List of abbreviations

| | |
|---|---|
| ADC | analog digital converter |
| FMEDA | failure modes, effects, and diagnostic analysis |
| RBD | reliability block diagram |
| IEC | International Electrotechnical Commission |

| | |
|---|---|
| DAC | digital analog converter |
| DC | diagnostic coverage |
| E/E/PE | system electric, electronic, electronic programmable |
| FPGA | field programmable gate array |
| ISO | International Organization for Standardization |
| FLC | fuzzy logic controller |
| MTBF | mean time between failures |
| MTTF | mean time to failure |
| MTTR | mean time to repair |
| MooN | a system of N redundant channels has a M-out-of-N voting |
| PFD | probability of failure on demand |
| PFDavg | average probability of failure on demand |
| PFH | probability of a dangerous failure per hour |
| SFF | safe failure fraction |
| SIF | safety instrumented function |
| SIL | safety integrity level |
| SIS | safety instrumented system |
| VHDL | very high speed integrated circuit hardware description language |

## Author details

Mohammed Bsiss* and Amami Benaissa
Department of Computer Science, Systems and Telecommunications (LIST), Faculty of Science and Technology, Tangier, Morocco

*Address all correspondence to: fstbsisss@gmail.com

## References

[1] IEC. 61508-6: Functional safety of electrical/electronic/programmable electronic safety-related systems. e2.0d; 2010

[2] IEC. 61508-2:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PE, or E/E/PES). e2.0d, pp. 27, Table 3

[3] IEC. 61508-2:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PE, or E/E/PES). e2.0d, pp. 77

[4] IEC. 61508-6:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PE, or E/E/PES). e2.0d, pp. 92, Table D.4

[5] IEC. 61508-2:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PE, or E/E/PES). e2.0d, pp. 34, Table 3

[6] ISA TR84.0.0.2. Safety Instrumented Functions (SIF), Safety Integrity Level (SIL), Evaluation Techniques. Part 2: Determining the SIL of SIF Via Simplified Equations. North Carolina; 1998

[7] Goble LWM. Control Systems Safety Evaluation and Reliability. 3rd ed. Research Triangle Park, NC: International Society of Automation; 2010

[8] IEC. 61508-6:2010: Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PE, or E/E/PES). e2.0d, pp. 143-144