Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

SIL of a Safety Fuzzy Logic Controller 1oo2 using Fault Tree Analysis (FAT) and realiability Block Diagram (RBD)

Dr.-Ing Mohammed Bsiss[1], Fatima Ezzahra Nadir[2], Prof. Amami Benaissa[3]
[1,2,3] *Faculty of Science and Technology, 90 000 BP, Tangier, Marocco*
Department of Computer Science Systems and Telecommunications (LIST)

Keywords: Safety Fuzzy Logic Controller (SFLC), Safety Integrity Level (SIL), Mean Time To Failure (MTTF), Safe Failure Fraction (SFF), Reliability Block Diagram (RBD), Fault Tree Analysis (FTA), Average Probability of Dangerous Failure on Demand (PFDavg), Field Programmable Gate Array (FPGA).

Abstract: This paper investigates how is processed the modeling of hardware failures. The target of this modeling is to assess the average probability of dangerous failure on demand of safety fuzzy logic controller [1] implemented in FPGA. Two evaluation methods are applied. The first method of evaluation uses the reliability block diagram [2]; the second is based on the fault tree analysis [2] and [3].We will demonstrate how to calculate the average probability of dangerous failure on demand. Consequently we'll able to determine the safety integrity level [6] for a SFLC. The main characteristics parameters for determining this SIL are rate of dangerous detected and undetected failure [4], the diagnostic coverage [5], proof test interval and other parameters

I. INTRODUCTION

The design and implementation of a safety fuzzy logic controller with a safety integrity level of SIL3 requires ~~a~~ qualitative and quantitative analysis of the components implemented in the field programmable gate array. Due to their usage in critical applications, the SFLC have a very stringent average probability of failure on demand requirement. This requirement is usually determined by industry standards, such as the safety integrity level (SIL) rankings defined in the IEC 61508 standard. The reliability block diagram and the fault tree analysis we'll be used to calculate an average probability of dangerous failure on demand PFD_{avg} for a SFLC and therefore determine what SIL ranking applies to the function of the SFLC.

The FPGA chip is according to [7] from B-Type. That means the behavior and failure modes are very complex.

The first step of qualitative analysis is to determine the value of the safe failure fraction [7], which allows us to evaluate the consequences of a dangerous failure.

A failure is called safe if it doesn't put the SFLC in a dangerous state when a fault occurs. A dangerous failure puts the safety fuzzy logic controller in a potentially dangerous state and makes the system inoperative.

The safe failure fraction is defined by the ratio of average failures of safe λ_S plus dangerous detected failures λ_{DD} and safe plus dangerous detected and undetected λ_{DU} failures. The calculation is based on the architecture of SFLC and on a functional analysis by carrying out a FMEDA, Failure Modes Effects and Diagnostic Analysis.

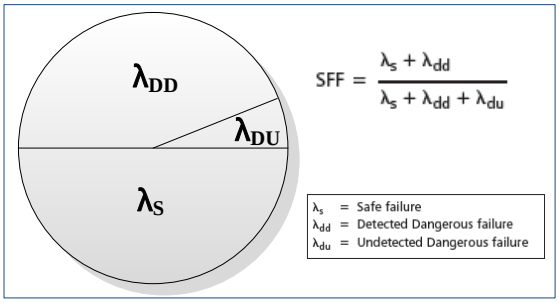

Figure 1: SFF of 99% means that 1% of the failures are dangerous and undetected

We have got 99% for the value of SFF using failure rates (table 1). The SFLC must have according to [7] a redundant architecture with safety integrity level of SIL3.

Table 1: Failure rate of SFLC

λ_S (h-1)	λ_{DU} (h-1)	λ_{DD} (h-1)
2,977E-9	9,93E-12	9,83E-07

In this sense, several methods for the analysis of failure modes have been developed. The possibilities are the failure analysis by the fault tree analysis [8], the reliability block diagram and markov process [9] and [10]. These methods don't allow only the calculation of the PFDavg but also the quantification of the system by determining the safety integrity level.

II. ARCHITECTURE OF SFLC

The SFLC consists of two Fuzzy Logic Controller (FLC) with the fuzzification process; rule evaluation process and defuzzification process in a redundant architecture 1out-of 2. Figure 2 shows a basic model for a fuzzy logic controller.

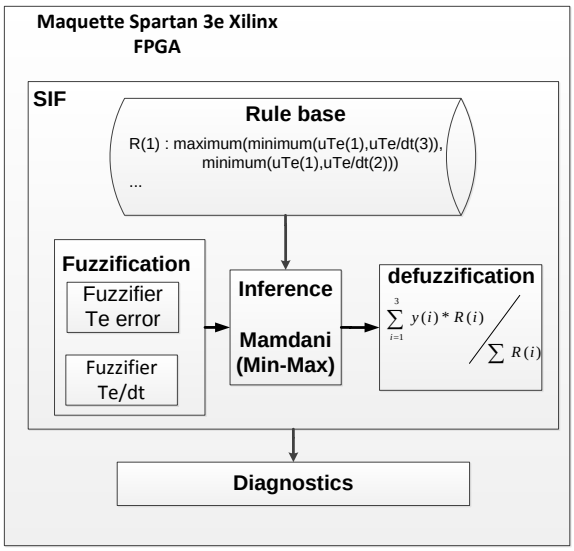

Figure 2 : Basic model for a fuzzy logic controller

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 SFLC 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 in the material. 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 FLC1 and FLC2.
Figure 3 shows a basic model for a safety fuzzy logic controller with redundancy architecture.

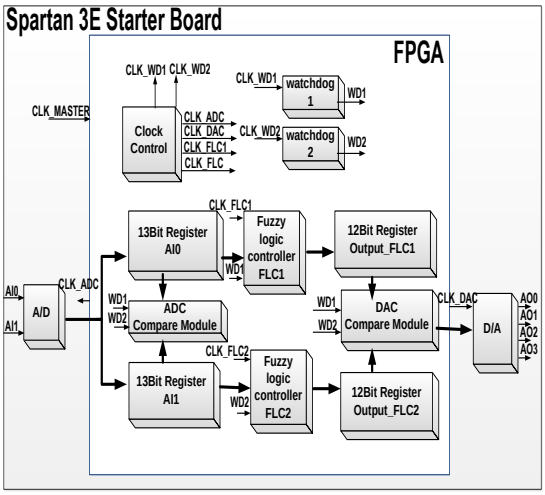

Figure 3: The Safety Fuzzy Logic Controller of 1oo2 architecture

III. SAFETY INTEGRIT LEVEL OF SFLC USING RBD AND FAILURE TREE ANALYSIS

III.1 Reliability Block Diagram

The reliability block diagram is a graphical representation of the system. Each component is represented by a function block (Figure 4)
All the elements come together to achieve the calculation of average probability of dangerous failure on demand. We take in consideration that the components have only two operating states (correct or faulty operation).

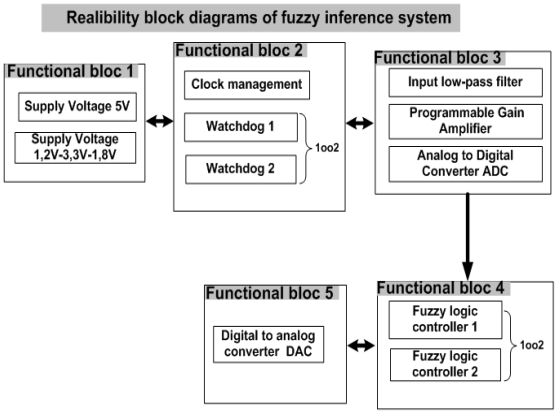

Figure 4: Decomposition of the SFLC in 5 functional blocks

The probability PFD_{avg} [11] is calculated by summing the probability of failure of all the functional blocks of a SFLC. The formulas used to calculate the probability PFD_{avg} of a SFLC depend on the component architecture.

The power supply module, the clock of the FPGA [12], the analog-digital converter [13] and the digital-analog converter has a simple architecture 1oo1. The calculation of PFD_{avg} like following [11]:

$$PFD_{avg} = \lambda_D \times t_{CE}$$
$$= (\lambda_{DU} + \lambda_{DD}) \times t_{CE}$$

The system down time t_{CE} is given by

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \times \left(\frac{T_1}{2} + MTTR) \right) + \frac{\lambda_{DD}}{\lambda_D} \times MTTR$$

The mean down time t_{CE} is calculated by adding the individual down times from both components, ($T_1/2$ +MTTR) and (MTTR).
On other hand, the watchdog and fuzzy logic controller component have redundant structures 1oo2. The calculation like following:

The system down time t_{CE} is given by

$$PFD_{avg} = 2 \cdot ((1-\beta_D) \cdot \lambda_{DD} + (1-\beta) \cdot \lambda_{DU})^2 \cdot t_{CE} \cdot t_{CE}$$
$$+\beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + MTTR \right)$$
$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{3} + MTTR) \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

The probability PFDavg is calculated for different proof test intervals (Ti = 3 years, 5 years and 10 years) with MTTR (mean time to repair) is equal MTTR = 8 hours

Table 2: Probability PFD_{avg} [1/h] for different proof test intervals

	Proof test interval T_i [year]		
	3	**5**	**10**
PFD_{avg}	3.44E-04	5.73E-04	1.15E-03

For a three-year mission time the value of the average probability of failure is 3.44 10^{-04}, that is significantly smaller as the value calculated with a ten years mission time that is 1.15 10^{-03}. The safety integrity level of a SFLC has been removing from a SIL 3 of a SIL 2, if the proof test interval takes place in 10 years.

III.2 Fault Tree Analysis

The basic events typically represent component failures or other hazards or events that can contribute to the TOP event hazard. If the failure rate for the base events are known, boolean algebra and probability laws ca be applied to calculate an average probability of dangerous failure for the TOP event. In this way, fault tree analysis is also quantitative.
The FTA of SFLC, describes in Figure 5, consists of two watchdog module WD1 and WD2, two fuzzy logic controllers FLC1 and FLC2, a supply voltage, an ADC converter, a DAC converter and a FPGA. The failure of any one of these subsystems will cause a dangerous failure of SFLC, the basic template will have an OR gate as the TOP gate, with each of those six subsystems as inputs, as Figure 5.

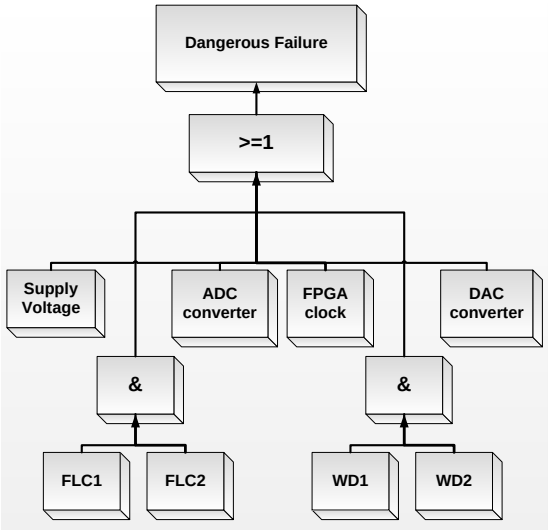

Figure 5: Failure Tree analysis of SFLC

The analysis by fault tree is performed by two phases; which is a qualitative, where determining the logical function of the system in terms of all its minimum failure (Figure 5) and the other is quantified by the calculation of probability of occurrence of the adverse event PFDavg.

For an architecture at 1 out of 1(1oo1), the average probability of dangerous failure is expressed by the following formula according to [08].

$$PFD_{\text{avg}} = (\lambda_{DU} + \lambda_{DD}) \times \frac{T_i}{2}$$

For an architecture at 1 out of 2 (1oo2), the average probability of dangerous failure is expressed by the following formula according to [08].

$$PFDavg = ((1-\beta)\lambda_{DU})^2 \times \frac{T_i^2}{3} + \left[(1-\beta)\lambda_{DU}\,\lambda_{DD}\,MTTR \times T_i\right] + \beta\,\lambda_{DU} \times \frac{T_i}{2} + \lambda_D \frac{T_i}{2}$$

The common mode failure refers to the simultaneous failure that can appear in the both FLC. The introduction of common-mode failures is generally represented by a beta factor β. The values for the factors beta are generally between 0.5% and 5%.
For a beta factor of a value β = 2%, respectively, representing the proportion of detecting common cause failures related to DC diagnostic coverage, and from each component failure rates, the probability of failure on demand by fault tree is calculated from formulas as mentioned above, and defined as follows:

$$PFD_{SIFS}(T_i) = (\lambda_{DU} \times \frac{T_i}{2} + \lambda_D \frac{T_i}{2})_{ALI} + (\lambda_{DU} \times \frac{T_i}{2} + \lambda_D \frac{T_i}{2})_{ADC}$$
$$+ (\lambda_{DU} \times \frac{T_i}{2} + \lambda_D \frac{T_i}{2})_{DAC}$$
$$+ (\lambda_{DU} \times \frac{T_i}{2} + \lambda_D \frac{T_i}{2})_{CLK\_FPGA} + (((1-\beta)\lambda_{DU})^2 \times \frac{T_i^2}{3}$$
$$+ [(1-\beta)\lambda_{DU}\, \lambda_{DD}\, MTTR \times T_i]$$
$$+ \beta\, \lambda_{DU} \times \frac{T_i}{2} + \lambda_D \frac{T_i}{2})_{SIF} + (((1-\beta)\lambda_{DU})^2 \times \frac{T_i^2}{3}$$
$$+ [(1-\beta)\lambda_{DU}\, \lambda_{DD}\, MTTR \times T_i]$$
$$+ \beta\, \lambda_{DU} \times \frac{T_i}{2} + \lambda_D \frac{T_i}{2})_{WD}$$

The probability of PFDavg is calculated by the combination of the average probability dangerous of failure on demand of all the elements ensuring the entire safety function. For using the calculated probability PFDavg the numerical values of characteristic parameters of components such as the failure rate, the DC coverage and the common cause failure factor.

The probability PFDavg is represented for different proof test interval (Ti = 3 years, 5 years and 10 years) with an mean time to repair equal MTTR = 8 hours

Table 3: Probability PFD_{avg} [1/h] for different proof test interval

	Proof test interval T_i [year]		
	3	**5**	**10**
PFD_{avg}	7.17E-4	1.19E-4	2.39E-3

For a three-year mission time the value of the average probability of failure is 7.17 10^{-04}, that is significantly smaller as the value calculated for a ten year mission time that is 2.39 10^{-03}. The safety integrity level of A SFLC has been removing from a SIL 3 of a SIL 2, if the proof test interval in 10 years takes place

IV. CONCLUSIONS

Both approaches include Boolean techniques representing the logic function linking the failures of individual components in the overall system failure.

We perceive that the method of reliability block diagrams models the system block diagram of the blocks and allows a system architecture view. As against the method of fault tree requires in addition to the functional analysis the determination of dangerous failures and events that may be associated that cause the loss of the safety function.
The results of both methods are almost similar if we consider that the β factor and the coverage DC are accurate.

The PFDavg value resulting from the FT analysis is 7, 17 10^{-03} for a proof test interval Ti = 3 years, is widely small for a mission time of Ti = 10 years with a value of 2, 39 10^{-02}, giving a variation of the safety integrity level of the SIF studied, a level of SIL 3 at a level of SIL 2 in a 5 year mission time instead of 10 years obtained by the method of Reliability Block Diagram.

REFERENCES

[1] M. Bsiss, I. H Baraka, A. Benaissa,. "Quantified Safety Analysis for Safety Fuzzy Logic Controller 1oo2 Reliability Block Diagrams", IEEE International Conference on Control Systems Computing and Engineering, 23-25 Nov. 2012 Penang, Malaysia.

[2] IEC, "61508-6:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)," e2.0d, pp.166-168.
[3] W.M.Goble, «Control Systems Safety Evaluation and reliability,» Research Triangle Park, NC 27709, International Society of Automation, 3 Edition 2010, pp 103-116
[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.193 Annex C
[5] IEC, "61508-4:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)," e2.0d, pp.43.
[6] 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.
[7] 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.
[8] ISA TR84.0.0.2.Safety instrumented System, Safety integrity Level, Evaluation techniques. Part 1 Introduction, version 4, North Carolina, 1997
[9] Guo, H. and Yang, X. (2008). Automatic creation of markov models for reliability assessment of safety instrumented systems. Reliability Engineering and System Safety, 93:807815
[10] IEC, "61508-6:2010 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)," e2.0d, pp.57-68
[11] 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
[12] XILINX, Spartan-3E FPGA Starter Kit Board User Guide, UG230: XILINX, January 20, 2011.
[13] L. T. Limited, Datasheet of LTC 2604 family, LT.

