TECHMIND RESEARCH
ISSN: 2291-2118
International Journal of Research in Business and Technology
Volume 10 No. 2 December 2017

PFH Calculation of a PID Controller 2oo3 system Implemented in FPGA Using Reliability Block Diagram

Fatima Ezzahra NADIR[1*], Ibrahim HADJ BARAKA[2], Benaissa AMAMI[3]
Laboratory of Computer Science, Systems and Telecommunications (LIST),
Faculty of Sciences and Technologies, 90 000 BP, Tangier, Morocco
[1]fatimzahra-nadir@hotmail.fr, [2]i.baraka@gmail.com, [3]b_benaissa@hotmail.com
*Corresponding Author

Abstract-*The Safety control and command system requires a compromise between reliability, availability and security. In this way, the implementation of a system containing a Proportional Integral Derivative Controller (PID) with 2oo3 architecture in FPGA allows the system reliability and reduces the controller conception life cycle. The availability is given by the system redundancy, which is represented by M out of N (MooN), and can tolerate M-N hardware failures to execute the safety function. The system safety is provided by the majority voting arrangement adopted by the active redundancy. To accord credibility to these types of systems, the analysis of a safety related system is an important phase for the classification of the system according to its safety integrity level (SIL). This kind of system can be performed by different methods that are related to international standards such as IEC 61508 [1]. This paper proposes the analysis of a system involving a PID Controller with 2oo3 architecture implemented in FPGA [2] and [3] using a qualitative and a quantitative analysis provided by this standard. The quantitative analysis is performed by the calculation of the system average frequency of dangerous failure (PFH) to define its safety integrity level (SIL). The qualitative analysis is based on the Reliability Block Diagram method [4], [5], and [6]. The results based on IEC 61508 standard will be compared to those obtained by the probabilistic method which uses the system equivalent failure rate in the PFH calculation.*

Keywords- *Proportional Integral Derivative Controller (PID); Safety Integrity Level (SIL); Hardware Failure Tolerant (HFT); Reliability Block Diagram (RBD); Average Frequency of Dangerous Failure per Hour (PFH); 1 out of 2 Architecture (1oo2); 2oo3 voting architecture (2oo3).*

1. INTRODUCTION

The conception and implementation of a Proportional Integral Derivative Controller require the implementation of calculation algorithms in microprocessors, microcontrollers, and the application of specific integrated circuit (ASIC) on software platforms (Labview, Matlab, C language ...). These technologies present several problems such as the complexity of mathematical calculations and they are very costly in terms of computation time. These difficulties require the implementation of FPGA technology development that allows more reliability and minimizes the conception of the life cycle thanks to the rapid transition from the virtual to the real prototype. On the other hand, its material complexity causes hardware failures such as: interconnection faults, delay faults, stuck at fault; consequently, we implement a voting architecture 2oo3 of a PID controller and an acquisition subsystem in FPGA to control hardware failures and lead the system to the safe state [7].

To accord credibility to this System, the safety integrity level [8] is to be evaluated; it depends, inter alia, on the system architecture adopted. Generally, the M out of N architecture (MooN) can tolerate (M-N) failures to execute the safety function. Several parameters can influence the probability calculation such as: the diagnostic coverage DC which is related to tests that control hardware failures [9] and [10], the proof test interval T_1 which is defined as the time interval between two consecutive inspections or maintenances of the system [10] and [11], the common cause failure factors β and β_D which present the interaction between channels [10] and [12].

For a safety related system used in continuous or high demand mode, the average frequency of dangerous failure per hour (PFH) calculation is based on formulas that are related to international standards and used to perform the safety function of Electrical, Electronic and Programmable Electronic Systems (E/E/PE). The international standard IEC 61508 adopts the Reliability Block Diagram, the Fault Tree Analysis, and Markov Models. This paper proposes the analysis of a system involving a PID Controller with 2oo3 architecture (PIDC 2oo3) implemented in FPGA [2] and [3] using a qualitative and a quantitative analysis provided by this standard. The quantitative analysis is performed by the calculation of the system average frequency of dangerous failure per hour (PFH) to define its safety integrity level (SIL). The qualitative analysis is based on the Reliability Block Diagram method [4], [5] and [6]. The results based on IEC 61508 standard will be compared to those obtained by the probabilistic method which uses the system equivalent failure rate in the PFH

calculation. The identification of PFH value associates a safety integrity level to the PID Controller with 2oo3 architecture. The proposed architecture contains three PID Controllers and three acquisition subsystems. To insure the system safety, the 2oo3 architecture uses the majority voting arrangement inside the FPGA to make the comparison even if one controller or acquisition subsystem has a dangerous hardware failure. We will use the Spartan 3E Starter Kit Board FPGA from Xilinx for the implementation of the system [14].

2. A REDONDANT PID CONTROLLER CONCEPTION

The Figure 1 presents the bloc diagram of the PIDC 2oo3. In addition to the FPGA, there are many hardware components such as converters, dual programmable gain amplifiers, the power supply and the FPGA clock. There are also different components implemented in the X3S500E Spartan 3E FPGA. The implementation of a PID controller in processing units such as FPGA requires the algorithm given by the following equation [15]:

$$U_n = K_P\varepsilon_n + U_{n-1} + K_P\frac{T_e}{T_i}\varepsilon_n + K_P\frac{T_d}{T_e}(\varepsilon_n - \varepsilon_{n-1}) \quad (1)$$

Where:

- ε_n is the current error.
- ε_{n-1} is the previous error.
- U_n is the current command.
- U_{n-1} is the previous command.
- K_p is the proportional gain.
- T_i is the integral time.
- T_d is the derivative time.
- T_e is the sampling time.

The proposed system contains three PID Controllers and three acquisition subsystems. The 2oo3 architecture has a majority voting arrangement for the output signals and can tolerate only one hardware failure (HFT=1) [8]; consequently, the failure of one PID controller or one acquisition subsystem does not influence the execution of the system safety function. For the PID controller, the majority voting arrangement is based on at least two channels, if only one controller gives a result which disagrees with the other two controllers, the output state does not change.

Generally, a safety related control system contains three elements or subsystems to ensure together the safety function [1]. The acquisition subsystem is performed by the analog digital converter "ADC" with 2oo3 architecture, the logic subsystem is performed by the PID controller with 2oo3 architecture and the control subsystem is performed by the digital analog converter "DAC".

The voting architecture 2oo3 adopted for the ADC converter requires three Spartan 3E Starter Kit Boards from Xilinx[15]. These boards adopt a SPI communication with a master board and two slave boards to transmit the ADC converter values. To ensure a safe transmission, we associate to each slave a cyclic redundancy check (CRC) calculator, and at the master board, we recalculate the CRC values. The majority voting arrangement is performed by the measurement comparison component and the order comparison component.

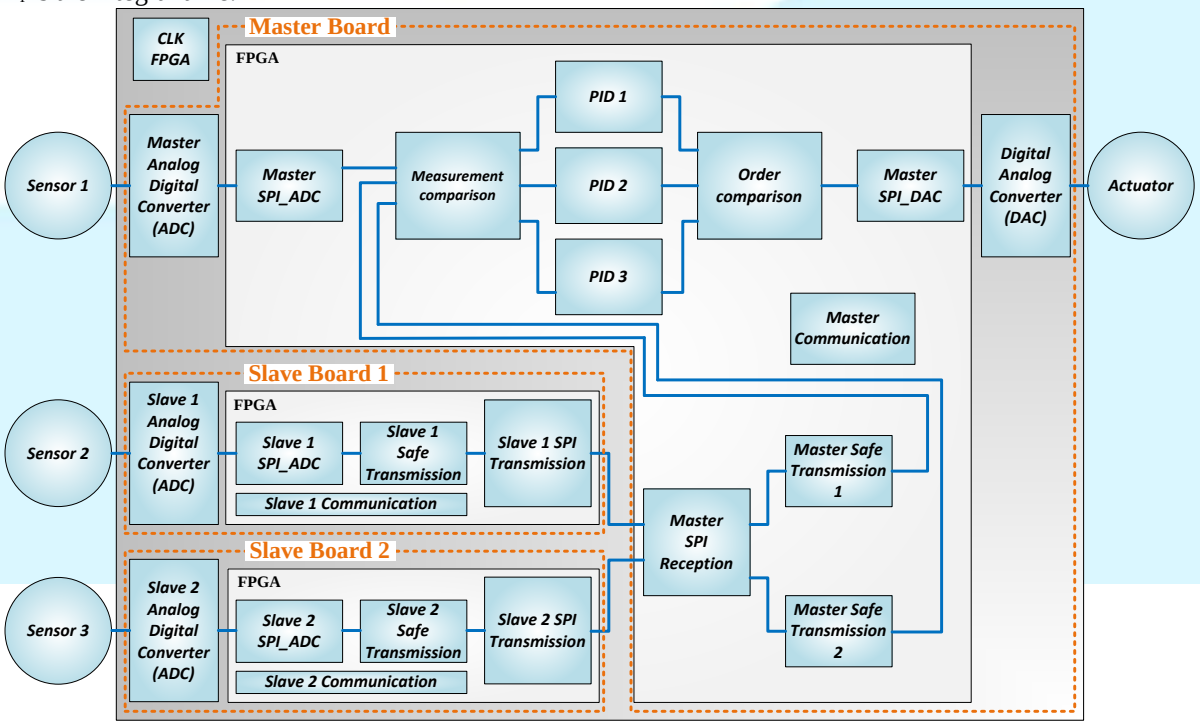

Fig 1: Bloc diagram of the PIDC 2oo3.

3. CALCULATION OF THE AVERAGE PROBABILITY OF A DANGEROUS FAILURE PER HOUR USING THE RELIABILITY BLOCK DIAGRAM

3.1 The qualitative Analysis

The structure of the Reliability Block Diagram (RBD) defines the logical interaction between the different PIDC 2oo3 components that are required to sustain the system operation. Each component of the PIDC 2oo3 is a functional block connected by a series or a parallel configuration; it's a graphical method that helps present the possible path to success. In a series configuration, if one functional block has a dangerous failure, the safety function is not executed, all elements or components of the system are necessary to perform the function. In a parallel configuration, the failure of one component or channel does not cause the loss of the defined safety function.

The PIDC 2oo3 system implemented in FPGA and presented in Figure 1, contains different subsystems. For the analogical digital converters, the SPI_ADC components, and the PID components are in active redundancy, with 2oo3 architecture presented in a parallel configuration in the reliability block diagram; which means two components are sufficient to execute the safety function. In case of the master safe transmission, the slave safe transmission, the slave communication and the SPI transmission, the 1oo2 architecture is adopted, and then presented by two blocks in a parallel configuration; consequently, only one block is needed to execute the function. The other components are in simple architecture, either because they present results comparison components, or hardware components such as the power supply.

The figure 2 presents the Reliability Block Diagram associated to the PIDC 2oo3 system structure.

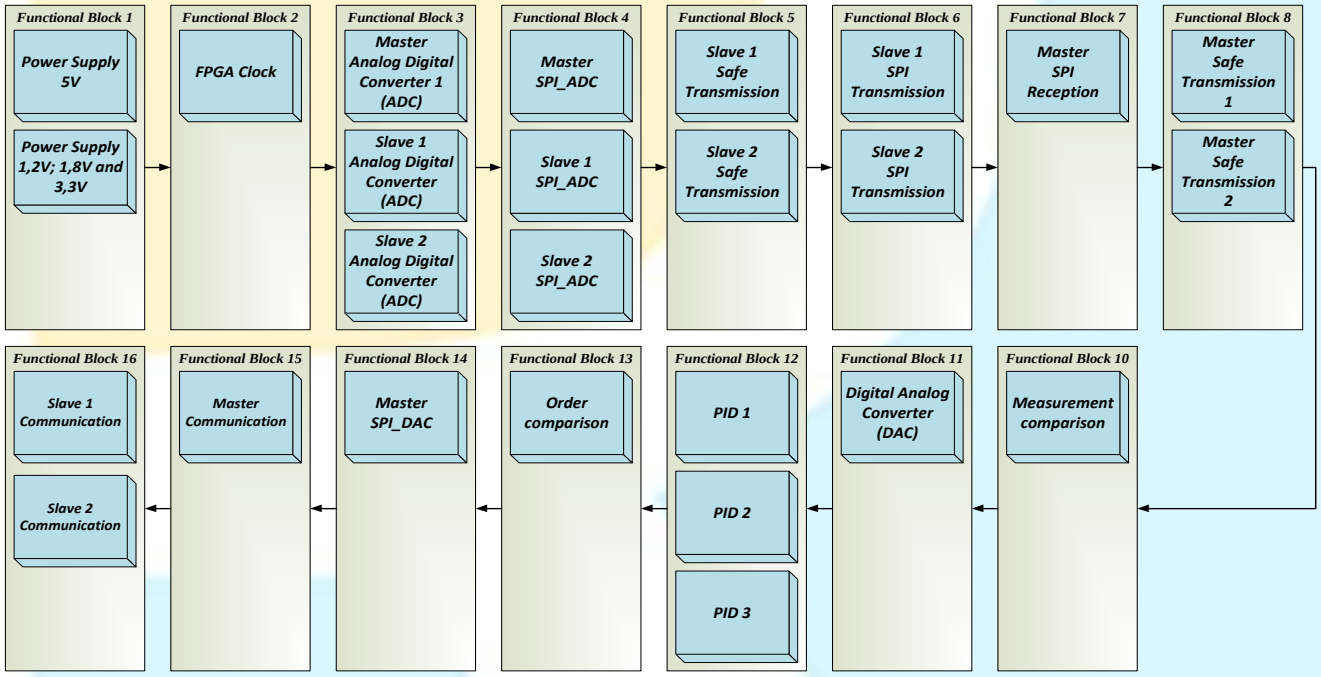

Fig 2: Reliability Bloc Diagram associated to the PIDC 2oo3 system.

3.2 The Quantitative Analysis Related to the Functional Blocks Architecture:

After one year, the average probability of dangerous failure per hour PFH of the PIDC 2oo3 system is the sum of the probabilities of its functional blocks [1]:

$$PFH(T_1) = \sum PFH_{\,functional\ block(MooN)}(T_1) \qquad (2)$$

The calculation of the PFH depends on the architecture adopted to each subsystem. The system analysis using the RBD is based on the international standard IEC 61508 [1], [3] and [4], this standard accords to each architecture a formula to calculate the PFH [1]:

- ***1oo1 architecture:***

$$PFH = \lambda_{DU} \qquad (3)$$

Where:

- λ_{DU} is the undetected dangerous failure rate.

- ***1oo2 architecture:***

$$PFH = 2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU} t_{CE} + \beta\lambda_{DU} \qquad (4)$$

Where:

- λ_{DD} is the detected dangerous failure rate.
- β and β_D the common cause failure factors.
- t_{CE} is the channel equivalent mean down time and depends on λ_{DD} and λ_{DU}, it's given by :

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad (5)$$

- ***2oo3 architecture:***

$$PFH = 6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU} t_{CE} + \beta\lambda_{DU} \quad (6)$$

As required in the IEC 61508 standard, we calculate the PFH of the PIDC 2oo3 system for one year with[1]:

- Mean time to restoration (MTTR) of 8 hours.
- Mean repair time (MRT) of 8 hours.
- Commun cause failure factors β_D = 1% and β = 2%

The calculation results presented in table 1 depend on:

- The safety factor S which indicates the number of failures leading to the loss of the safety function, it's given as a percentage. The type of component A or B can identify the safety factor value. Therefore, the type A components have a safety factor of 10%, and their failures are defined (transistor, resistance, capacitor…). The type B components have a safety factor of 50%, and their failures are not all defined (converters, programmable gates,…). This factor can be determined by a Failure Mode and Effects Analysis (FMEA) using the following equation [16]:

$$S = \frac{\lambda_D}{\lambda_S + \lambda_D} \quad (7)$$

- The diagnostic coverage DC which is related to tests that control hardware failures. These failures are defined by a FMEA. For the PIDC 2oo3 system, components adopting a simple architecture have a diagnostic coverage of 60%. The redundant architectures have a diagnostic coverage of 90%.
- The failure rate of the component λ which can be defined using Siemens standard (SN-25900) [17].
- The architecture MooN of each component which means M channels among N channels must properly work to execute the defined safety function.

TABLE 1. CALCULATION RESULTS OF THE PFH OF THE PIDC 2OO3 USING THE IEC 61508 STANDARD .

Component	Architecture	λ (per hour)	S (%)	DC (%)	PFH (per hour)
Power Supply	1oo1	4,89E-8	50	60	9,78E-09
FPGA Clock	1oo1	7,33E-8	50	60	1,47E-08
ADC+AMP	2oo3	8,06E-8	50	90	8,10E-11
SPI_ADC	2oo3	1,48E-8	50	90	1,48E-11
Slave safe transmission	1oo2	8,52E-9	50	90	8,52E-12
Slave SPI Transmission	1oo2	2,72E-9	50	90	2,72E-12
Master SPI Reception	1oo1	1,28E-8	50	60	2,56E-09
Master safe transmission	1oo2	9,37E-9	50	90	9,37E-12
Measurement Comparison	1oo1	2,13E-9	50	60	4,26E-10
PID	2oo3	9,97E-9	50	90	9,98E-12
Order Comparison	1oo1	2,13E-9	50	60	4,26E-10
SPI_DAC	1oo1	8,61E-9	50	60	1,72E-09
DAC	1oo1	6,11E-8	50	60	1,22E-08
Master Communication	1oo1	1,44 E-8	50	60	2,88E-09
Slave Communication	1oo2	2,3 E-9	50	60	2,30E-12
		Total			4,48E-08

As we can see in table 1, after one year, the PFH of the PIDC 2oo3 system is equal to 4,48E-8 per hour, which allows to associate SIL3 as system safety integrity level.

3.3 The Quantitative Analysis Related to the system failure rate:

The system average frequency of dangerous failure per hour PFH can be calculated by the unreliability F (T) over the period of interest T; The system PFH is calculated by the following equation[18]:

$$PFH(T) = \frac{F(T)}{T} \quad (8)$$

The unreliability F(t) is calculated using the system reliability R(t), and given by [19]:

$$F(T) = 1 - R(t) \quad (9)$$

Where:

$$R(t) = e^{-\lambda t} \quad (10)$$

The system PFH is given by:

$$PFH(T) = \frac{1 - e^{-\lambda T}}{T} \quad (11)$$

Since λT<< 1, the equation (11) becomes:

$$PFH(T) = \lambda \quad (12)$$

For the PIDC 2oo3, we need to calculate the system probability of dangerous undetected failure per hour, consequently the equation (12) becomes:

$$PFH(T) = \lambda_{DU} \quad (13)$$

In a serial configuration, all components must properly work to execute the system safety function. The description can be presented as a logical equation, if each component has a constant failure rate λ_{Ci}, the system reliability R_S is given by the following equation [19]:

$$R_S = \prod_{i=1}^{n} R_i \quad (14)$$

The system failure rate λ_S is given by the following equation [20]:

$$\lambda_S = \sum_{i=1}^{n} \lambda_{Ci} = \lambda_{C1} + \lambda_{C2} + \ldots + \lambda_{Cn} \quad (15)$$

In a parallel configuration, several components execute the same operation; consequently, the system reliability R_S can be obtained as the complement of the system unreliability; which is given by the following equation:

$$R_S = 1 - \prod_{i=1}^{n} (1 - R_i) \quad (16)$$

The equation (16) can be used only for the 1ooN architectures. For the voting architectures (MooN, with M≥2), we must use the logical equation to calculate the system reliability R_S as shown below. The logical equation method can be used for all MooN architectures.

For the 1oo2 architecture, one component is sufficient to execute the system safety function defined. The system reliability R_S is given by the logical equation [21]:

$$R_{S(1oo2)} = \overline{R_1} R_2 + R_1 \overline{R_2} + R_1 R_2 \quad (17)$$

For the 2oo3 architecture, two components are sufficient to execute the voting arrangement that allows taking the decision to perform the function defined. The system reliability R_S is given by the logical equation [20]:

$$R_{S(2oo3)} = \overline{R_1} R_2 R_3 + R_1 \overline{R_2} R_3 + R_1 R_2 \overline{R_3} + R_1 R_2 R_3 \quad (18)$$

Where:

$$\overline{R} = (1 - R) \quad (19)$$

In a parallel configuration, all components have the same failure rate; therefore, the same reliability R. The 1oo2 architecture reliability is given by the following equation [20] and [21]:

$$R_{S(1oo2)}(t) = 2R - R^2 = 2e^{-\lambda t} - e^{-2\lambda t} \quad (20)$$

The same result can be obtained using the equation (16).

The 2oo3 architecture reliability is given by the following equation [20] and [21]:

$$R_{S(2oo3)}(t) = 3R^2 - 2R^3 = 3e^{-2\lambda t} - 2e^{-3\lambda t} \quad (21)$$

In the general case, the system failure rate λ is calculated using the system reliability by the following equation [21]:

$$\lambda = \frac{1}{\int_0^{\infty} R(t)dt} \quad (22)$$

The 1oo2 architecture equivalent failure rate λ_{1oo2} is [20]:

$$\lambda_{1oo2} = \frac{1}{\int_0^{\infty} R_{S(1oo2)}(t)dt} = \frac{2\lambda}{3} \quad (23)$$

The 2oo3 architecture equivalent failure rate λ_{2oo3} is [20]:

$$\lambda_{2oo3} = \frac{1}{\int_0^{\infty} R_{S(2oo3)}(t)dt} = \frac{6\lambda}{5} \quad (24)$$

The system PFH calculation results are presented in table 2:

TABLE 2. CALCULATION RESULTS OF THE λ_{DU} OF THE PIDC 2OO3 USING THE PROBABILISTIC METHOD.

Component	λ_{DU} (per hour)
Power Supply	9,78E-09
FPGA Clock	1,47E-08
ADC+AMP	4,84E-09
SPI_ADC	8,88E-10
Slave safe transmission	2,84E-10
Slave SPI Transmission	9,07E-11
Master SPI Reception	2,56E-09
Master safe transmission	3,12E-10
Measurement Comparison	4,26E-10
PID	5,98E-10
Order Comparison	4,26E-10
SPI_DAC	1,72E-09
DAC	1,22E-08
Master Communication	2,88E-09
Slave Communication	7,67E-11
	5,18E-08

As we can see in table 2, the PFH of the PIDC 2oo3 system is equal to the system undetected dangerous

failure rate with 5,18E-08 per hour, which allows to associate SIL3 as system safety integrity level. The probabilistic method uses the system equivalent failure rate in the PFH calculation.

4. CONCLUSION

To control the system hardware failure, the PIDC 2oo3 system adopts the 2oo3 voting architecture at the PID controller subsystem and the acquisition subsystem. This architecture has a majority voting arrangement for output signals. If only one PID Controller or measurement component gives a result which disagrees with the other, the output state doesn't change; consequently, the safety system is insured.

In terms of qualitative analysis, the reliability block diagram is used to define the various blocks that make the system, and logical interactions between the different PIDC 2oo3 system components that are required to sustain the system operation.

In terms of quantitative analysis, to calculate the PFH, the first method based on IEC 61508 formulas uses the common cause failures in case of redundant architecture. In addition, the probability of failure is the sum of the probabilities of the PIDC 2oo3 system functional components which is calculated for each subsystem related to its architecture. On the other hand, the probabilistic method based on the system equivalent failure rate, presents the PIDC 2oo3 system as one equivalent functional block, its failure rate is calculated using the interaction between different subsystems given by the reliability block diagram. For this method, the system PFH represents the system failure rate; it doesn't take account of common cause failures. This difference in the calculation method doesn't influence the system safety integrity level.

5. REFERENCES

[1] IEC, "61508-6: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems", e2.0d, pp.21-75, 2010.

[2] M. Bsiss, B. Amami, "Safety Fuzzy Logic Controller of 1oo2 Architecture for FPGA Implementation", International Journal of Computer Science and Network Security (IJCSNS), vol. 11, no. 04, pp. 105-110, 2011.

[3] G. Kaczor, S. Młynarski, M. Szkoda, "Verification of safety integrity level with the application of Monte Carlo simulation and reliability block diagrams", Journal of Loss Prevention in the Process Industries, pp. 31-39, 2016.

[4] M. Bsiss, I. H. Baraka, B. Amami, "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.

[5] M. Bsiss, F. E. Nadir, and B. Amami, "SIL of a Safety Fuzzy Logic Controller 1oo2 using Fault Tree Analysis (FTA) and Reliability Block Diagram (RBD)", International Journal of Modern Trends in Engineering and Research (IJMTER), vol. 02, no. 08, pp. 383–390, 2015.

[6] L. W. M. Goble, "Control Systems Safety Evaluation and reliability", Research Triangle Park, NC 27709, International Society of Automation, pp 103-116, Edition 3, 2010.

[7] F. Sassi, M. Abbes, A. Mami, "FPGA Implementation of PID Controller", International Conference on Control, Engineering & Information Technology Proceedings, pp. 1-13, 2014.

[8] IEC, "61508-2: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)", e2.0d, pp.46 table 3, 2010.

[9] IEC, "61508-6: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems" e2.0d, pp.76-79, 2010.

[10] F.E. Nadir, I. H Baraka, M. Bsiss, B. Amami, "Influence of Failure Modes and Effects Analysis on the Average Probability of Failure on Demand for a Safety Instrumented System", IEEE 4th Edition of International Colloquium on Information Science and Technology, 24-26 October, 2016, Tangier, Morocco.

[11] IEC, "61508-4: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)", e2.0d, pp.45, 1998.

[12] IEC, "61508-6: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems" e2.0d, pp.80-94, 2010.

[13] IEC, "61508-6: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems" e2.0d, pp.27-29, 2010.

[14] Xilinx Corporation, Spartan-3E FPGA Starter Kit Board User Guide, UG230: XILINX, January 20, 2011.

[15] Gene F. Franklin, J. David Powell, Michael L. Wokman, "Digital control of dynamic systems", Second Edition, June, 1990.

[16] Börcsök, Josef "FunktionaleSicherheitGrundzügesicherheitstechnisc

hersysteme".ISBN 978-3-8007-3590-7 pp. 321-325, 2011.

[17] Siemens Norm, "Expected values, General, Date of issue", SN 29500-1, Edition 2009-07, 2004.

[18] IEC, "61508-6: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems", e2.0d, pp.24, 2010.

[19] R. Billinton, R. N. Allan, "Reliability Evaluation of Engineering Systems Concepts and Techniques", pp. 82-86, 1992.

[20] Allion Science and Technology, "Calculating Failure Rates of Series/Parallel Networks", The Journal of System Reliability Center, 2006.

[21] F. Ciutat, "SIL - Automatismeetsécurité: Intégrité des fonctionsautomatisées de sécurité", PP.235-245, Second Edition, 14 November, 2011.

Author's Biography

Fatima Ezzahra NADIR received the M.E. degree in

electronics, Electrotechnics and Automation degree in 2013 from AbdelmalekEssaadi University in Morocco. Since 2014, she has been a PhD student in the Faculty of Sciences and Technologies, Tangier, Morocco. Her research interests include the safety embedded systems.

Ibrahim HADJ BARAKA received the M.E. degree in

electronics, Electrotechnics and Automation degree in 2013 from National School of Electricity and Mechanics (ENSEM), Casablanca, Morocco. Professor of Electrical Engineering at the Faculty of Sciences and Technologies, Tangier, Morocco. Member of Laboratory of Computer Science, Systems and Telecommunications. His research interests include embedded systems and static converters in renewable energies.

Benaissa AMAMI received PhD from Paris 6 University

in 1992, Professor of Electrical Engineering at the Faculty of Sciences and Technologies, Tangier, Morocco. Currently, member of Laboratory of Computer Science, Systems and Telecommunications. His research interests include the safety embedded systems.