Development and evaluation of a 2oo3 safety controller in FPGA using fault tree analysis and Markov models

Fatima Ezzahra Nadir[1], **Mohammed Bsiss**[2], **Benaissa Amami**[2]

[1]Laboratory of Engineering Sciences and Energy Management, Research Team: Optimization of Industrial Systems, Higher School of Technology, Ibn Zohr University, Agadir, Morocco

[2]Intelligent Automation and BioMedGenomics Laboratory, Faculty of Sciences and Technologies, Abdelmalek Essaâdi University, Tangier, Morocco

Article Info

Article history:

Received Jul 21, 2023
Revised Oct 28, 2023
Accepted Nov 17, 2023

Keywords:

M out of N voting architecture
Fault tree analysis
Field programmable gate array
Hardware fault tolerance
Markov models
Probability of failure on demand per hour
Safety integrity level

ABSTRACT

The Safety integrity level (SIL) is a measure of the reliability and availability of a safety instrumented system. SIL determination involves qualitative and quantitative analysis based on international standards such as IEC 61508 and IEC 61511. Several techniques can be used to analyze safety instrumented systems, including reliability block diagrams, fault tree analysis, and Markov models. The aim of this paper is to design and evaluate a pressure control system for a compressed nitrogen tank using a PID controller implemented in a field programmable gate array with 2 out of 3 architecture. This architecture ensures the safety of measurements and command of the system through a voting arrangement. The availability of the system is determined by the redundancy and the one hardware failure tolerance. The quantitative analysis is performed by calculating the probability of failure on demand per hour using Markov models or a relevant probabilistic approach based on fault tree analysis. The Markov model method gives the probability of failure of the system in different states during the system life cycle. The fault tree analysis method determines the probability of failure of the system using its equivalent failure rate. Furthermore, this paper compares the SIL result obtained by each model.

Corresponding Author:

Fatima Ezzahra Nadir
Electrical Engineering Department, Agadir Higher School of Technology, Ibn Zohr University
BP: S33 – Agadir, Agadir 80150, Morocco
Email: f.nadir@uiz.ac.ma

1. INTRODUCTION

The process industry is becoming increasingly complex, which means that potential hazards must be adequately controlled to prevent risks and protect the system and its environment. To manage risk in industrial installations, a safety instrumented system must be implemented to either prevent the risk from occurring or to protect against the consequences of a malfunction. The design of a safety instrumented system requires the selection of the appropriate instrumentation: sensors, actuators, and logic solvers, and the definition of the redundancy and voting logic necessary to achieve a safety integrity level compatible with the level of risk required. The safety instrumented system classification is performed by assigning a safety integrity level in [1], [2]. In this regard, we propose the design and evaluation of a safety proportional integral derivative controller implemented in a field programmable gate array with a 2oo3 architecture used to control a pressure regulation system for a compressed nitrogen tank. The 2oo3 architecture ensures the measurement and control safety of the system by employing a voting mechanism. The availability of the system is ensured by redundancy. The credibility assessment of this system requires a quantitative analysis to assign a safety integrity level (SIL). This level can be determined in terms of the probability of failure on demand per hour (PFH). According to the international standards IEC 61511 [3] or IEC 61508 [4], several methods are proposed to evaluate a safety instrumented system, such as fault tree analysis in [5]-[9], and Markov models in [10]-[20]. In terms of qualitative analysis, Markov models represent different states of the system throughout its life cycle. It depends on the architecture of the system, which is generally described by M out of N (MooN) architecture and can tolerate N-M failures to perform the system safety function. Fault tree analysis provides logical combinations of causes that can lead to a dangerous failure. In terms of quantitative analysis, the Markov models method gives the system's future probability of failure in function of the current state. Using fault tree analysis, a relevant method is proposed to calculate the equivalent failure rate of the system based on its reliability, which is estimated as the system PFH.

Many research papers use the Markov models method to evaluate safety instrumented systems (SIS). In [11]-[13], the authors evaluate the SIS performance using a multiphase Markov chain analysis. They also present Markov models for different architectures (1oo1, 1oo2, 2oo3) without considering the safe state. In [14]-[16], the authors propose Markov chain to represent the unavailability of redundant SIS while excluding the consideration of common cause failures. In [17], [18], the authors suggest to review the IEC 61508 PFH formulas and introduce new ones based on the Markovian approach. The 2oo3 model used in this approach does not illustrate the different states that the system can take. In [19], [20], the authors perform a comparative analysis of different architectures to be implemented in safety critical computing systems. They employ Markov models to evaluate safety levels and various design parameters for different system configurations and find that both 1oo2 and 2oo3 configurations can effectively reduce the average probability of failure. However, the 2oo3 architecture has the ability to implement the voting arrangement, and relies on considering the safe output when two channels provide the same results. In [8], [9], the authors evaluate the safety integrity level using reliability and fault tree analysis. In a serial configuration, the probability is the sum of the individual component probabilities. In a parallel configuration, the probability is the product of all component probabilities. In this case, using the reliability equations in [21], [22], new equations are proposed for redundant architectures. In [23]-[25], the authors present the parallel processing capabilities of FPGA to efficiently implement multiple tasks to be executed simultaneously, which can significantly reduce the system execution time. In [26]-[28], the authors present the design and implementation of the 1oo4 redundant architecture in FPGA. Although the 1oo4 configuration improves system availability, it does not incorporate a voting mechanism to increase safety. In this article, we propose the design of SPIDC 2oo3, using the 2oo3 architecture, as a means to guarantee the safety and availability of the system's measurement and control. The evaluation is performed using Markov models and fault tree analysis to compare the obtained SIL. These analyses require the definition of the basic parameters of each subsystem. For the Markov approach, we propose Markov models of the architectures used in the SPIDC 2oo3 and consider the safe state and common cause failures in the models. Using fault tree analysis, new PFH formulas are suggested for redundant architectures based on reliability formulas.

2. VOTING PID CONTROLLER 2OO3 SYSTEM

2.1. Voting PID controller 2oo3 function blocks

The voting PID controller 2oo3 (SPIDC 2oo3) manages a single safety function, which is the emergency shutdown of the gas flow if a dangerous failure is detected in the system components. In this system, three pressure sensors operate in parallel and are responsible for measuring and transmitting any deviation of the pressure parameter towards a dangerous state. The logic processing system is based on FPGA technology with 2oo3 architecture in [23]-[28]. Its role is to collect the signals from the sensors, process them, and control the associated actuator. The actuator is a valve that is responsible for stopping the flow of gas to the tank and bringing the entire process to a safe position and maintaining it. Figure 1 illustrates the SPIDC 2oo3 associated with the emergency shutdown. This subsystem is needed to stop the flow in case of a dangerous failure.

The SPIDC 2oo3, with three PID controllers, guarantees safety because it has a majority voting arrangement for the output signals (if there is only one controller that gives a conflicting result with the other two controllers, the output state remains unchanged) and the failure of a PID controller or a sensor does not affect the safety function of the system. This architecture guarantees high availability by tolerating one hardware failure (HFT=1). Voting architecture 2oo3 is used for the analog-todigital converter (ADC) converter, which requires three Spartan 3E Starter Kit boards from Xilinx [29]. These boards use smartplant instrumentation

(SPI) communication between a master board and two slave boards to transfer ADC converter values. Safe transmission is achieved by implementing a cyclic redundancy check (CRC) calculator in each slave board, and checking the CRC values at the master board. Majority voting arrangement is performed by the measurement comparator component and the order comparator component. Figure 2 illustrates the SPIDC 2oo3 block diagram.

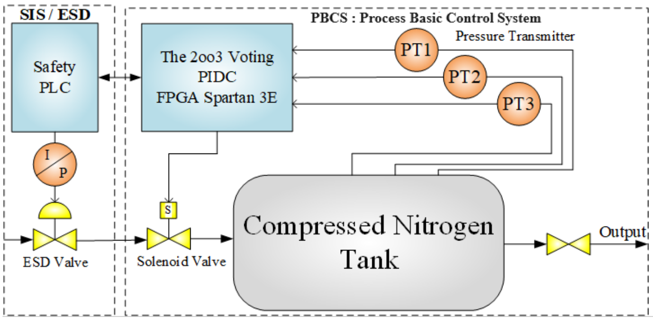


Figure 1. Subsystems used to regulate the tank pressure

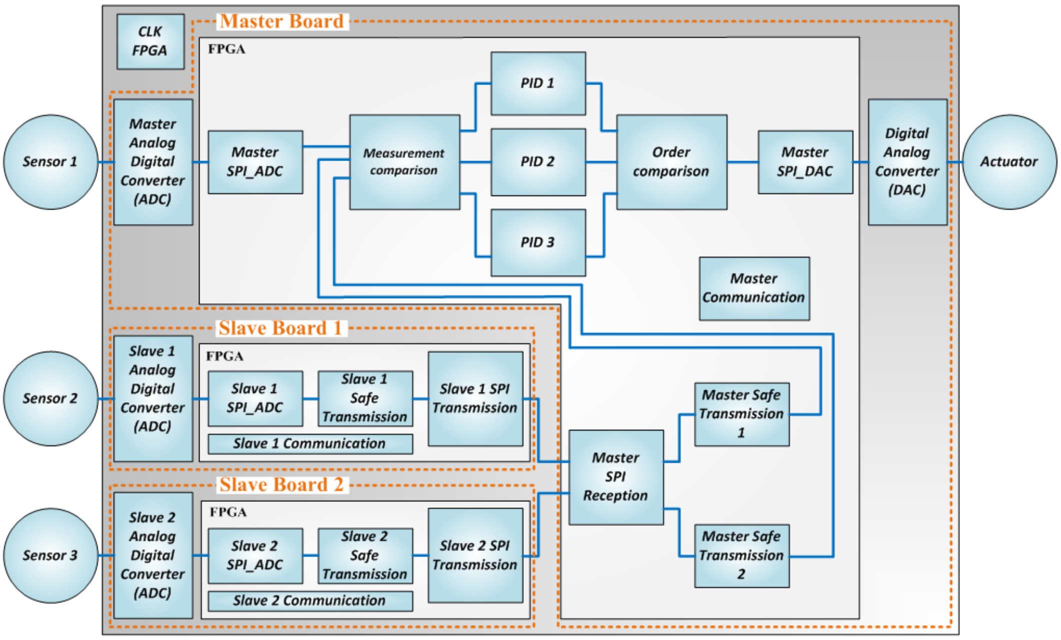


Figure 2. SPIDC 2oo3 block diagram

2.2. SPIDC 2oo3 system element failure rate

To perform a quantitative analysis, the failure rate of each component in the SPIDC 2oo3 system must be defined. The Spartan 3E Stater kit board incorporates many hardware components that contribute to the system logic solver. In addition, three sensors measure the process pressure and a solenoid valve controls the system output.

2.2.1. Sensor failure rate

The chosen system uses a pressure transmitter whose failure rate λ is specified by Exida [30] in terms of failure modes and effects analysis (FMEA). This is an important step to achieve functional safety certification of the device according to IEC 61508. The transmitter is classified as a type B device according to IEC 61508 [31], which associates a safety factor S of 50%, it has a hardware fault tolerance that allows a diagnostic coverage DC of 90%. Table 1 gives the sensor basic parameters.

Table 1. Sensor basic parameters

Component	λ(/h)	S(%)	DC(%)
Pressure transmitter	4,96E-7	50	90

2.2.2. Logic solver components failure rate

The hardware components included in the failure rate calculation are the LTC1407A-1 analog-to-digital converter (ADC), the LTC6912-1 dual programmable gain amplifier (AMP), the LTC2624 digital-to-analog converter (DAC), and the TPS75003 power supply (PWR). An approach calculating the failure rate is taken from part 2 of Siemens standard (SN 29500-2) [32]. The basic failure rate λ depends on the reference failure rate λ_{ref} in failure in time (FIT), reference average ambient temperature, reference virtual junction temperature, actual virtual junction temperature. The reference failure rate λ_{ref} should be understood for operation under the reference conditions specified in the device datasheets. In the case of the FPGA clock (CLK), the failure rate calculation is presented in part 4 of Siemens standard (SN 29500-4) [33]. Table 2 lists various parameters of hardware components: Hardware components basic failure rate λ, safety fraction S, diagnostic coverage DC. The FIT is equal to one failure in 10^9 component hours, which means, $1FIT = 10^{-9}/h$.

The devices implemented in the X3C500E Spartan 3E FPGA are configured using a very high-level design language (VHDL). The failure rate of each component is defined by the number of slices occupied in the XC3S500E Spartan 3E FPGA target and the FPGA failure rate of 3,97E-7 per hour is reported by Xilinx in [34]-[36]. The basic parameters of the XC3S500E FPGA components are listed in Table 3.

Table 2. Hardware components basic parameters

Component	$\lambda(/h)$	S(%)	DC(%)
ADC	6,11E-8	50	90
DAC	6,11E-8	50	60
AMP	1,95E-8	50	60
PWR	4,89E-8	50	60
CLK	7,33E-8	50	60

Table 3. XC3S500E FPGA components basic parameters

Component Instantiation	λ (/h)	S(%)	DC(%)
XC3S500E FPGA Target	3,97E-7	50	90
SPI_ADC	1,48E-8	50	90
Measurement Comparator	2,13E-9	50	60
SPID	9,97E-9	50	90
Order Comparator	2,13E-9	50	60
SPI_DAC	8,61E-9	50	60
Master SPI Reception	1,28E-8	50	60
Slave SPI Transmission	2,72E-9	50	90
Master Safe Transmission	9,37E-9	50	90
Slave Safe Transmission	8,52E-9	50	90
Master Communication	1,44E-8	50	60
Slave Communication	2,3E-9	50	90

2.2.3. Actuator failure rate

In order to control the process pressure, a solenoid valve is used as the final control element. The SPIDC 2oo3 output signal range from 0% up to 100% represents the valve opening. The failure rate of the solenoid valve is given by Exida [30], related to failure mode and effect analysis (FMEA). The solenoid valve is classified as a Type A device according to IEC 61508 [37], which associates a safety factor S of 10%. The 1oo1 architecture does not have hardware fault tolerance, which allows a diagnostic coverage DC of 60%. Table 4 lists solenoid valve basic parameters.

Table 4. Solenoid valve basic parameters

Component	λ(/h)	S(%)	DC(%)
Solenoid valve	7,02E-7	10	60

3. PFH CALCULATION USING THE FAULT TREE ANALYSIS

3.1. Qualitative analysis using fault tree method

Fault tree analysis (FTA) is a deductive method used to represent causes that contribute to SPIDC 2oo3 dangerous undetected failures. This method provides a binary representation that distinguishes between various causes that generate a SPIDC 2oo3 dangerous undetected failures in [5]-[9]. Figure 3 shows the SPIDC 2oo3 fault tree analysis, the dangerous undetected failures of the system can occur if any of the following subsystems are unsuitable for use due to a dangerous undetected failure: Components using the 1oo1 architecture, such as the valve, or both components of subsystems using the 1oo2 architecture, such as the slave1 SPI transmission, or any combination of two components of subsystems using the 2oo3 architecture, such as the pressure transmitter, have dangerous undetected failures.

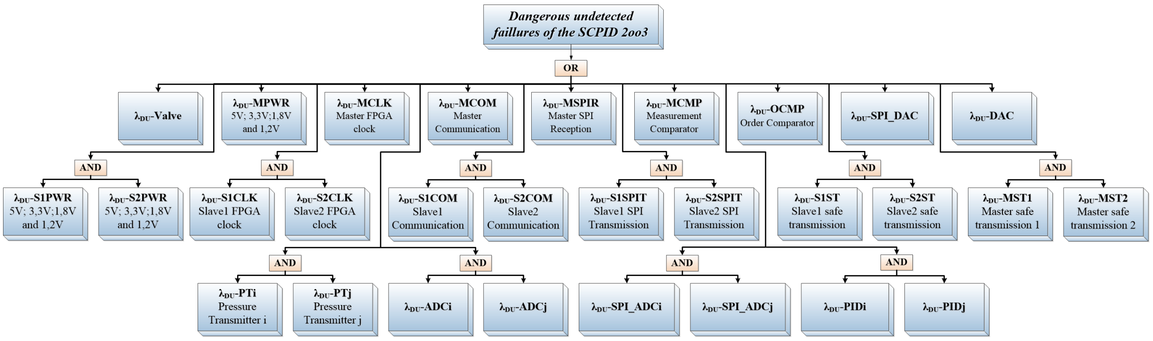

Dangerous undetected faillures of the SCPID 2oo3
OR
λ_{DU}-Valve
λ_{DU}-MPWR 5V; 3,3V;1,8V and 1,2V
λ_{DU}-MCLK Master FPGA clock
λ_{DU}-MCOM Master Communication
λ_{DU}-MSPIR Master SPI Reception
λ_{DU}-MCMP Measurement Comparator
λ_{DU}-OCMP Order Comparator
λ_{DU}-SPI_DAC
λ_{DU}-DAC
AND
AND
AND
AND
AND
AND
λ_{DU}-S1PWR 5V; 3,3V;1,8V and 1,2V
λ_{DU}-S2PWR 5V; 3,3V;1,8V and 1,2V
λ_{DU}-S1CLK Slave1 FPGA clock
λ_{DU}-S2CLK Slave2 FPGA clock
λ_{DU}-S1COM Slave1 Communication
λ_{DU}-S2COM Slave2 Communication
λ_{DU}-S1SPIT Slave1 SPI Transmission
λ_{DU}-S2SPIT Slave2 SPI Transmission
λ_{DU}-S1ST Slave1 safe transmission
λ_{DU}-S2ST Slave2 safe transmission
λ_{DU}-MST1 Master safe transmission 1
λ_{DU}-MST2 Master safe transmission 2
AND
AND
AND
AND
λ_{DU}-PTi Pressure Transmitter i
λ_{DU}-PTj Pressure Transmitter j
λ_{DU}-ADCi
λ_{DU}-ADCj
λ_{DU}-SPI_ADCi
λ_{DU}-SPI_ADCj
λ_{DU}-PIDi
λ_{DU}-PIDj

Figure 3. SPIDC 2oo3 system fault tree analysis

3.2. Quantitative analysis using fault tree method

The fault tree analysis, shown in Figure 3, outlines how the various components of the SPIDC 2oo3 system are interconnected in parallel and serial configurations. These configurations serve as the basis for formulating logical equations that evaluate system reliability and calculate the probability of failure on demand per hour (PFH). This probability can be thought of as the component failure rate, using (1) [4]:

$$PFH(T) = \lambda_{DU} \tag{1}$$

In a series configuration, the proper functioning of all components is necessary to perform the system's safety function. System reliability R_S can be expressed as a logical equation, if each component has a constant failure rate λ_{Ci}. The equation representing R_S is as (2) [21], [22], [38]:

$$R_S = \prod_{i=1}^{n} R_i \tag{2}$$

where:

$$R(t) = e^{-\lambda t} \tag{3}$$

The equation (4) determines the system failure rate λ_S [21], [22], [38]:

$$\lambda_S = \sum_{i=1}^{n} \lambda_{Ci} = \lambda_{C1} + \lambda_{C2} + ... + \lambda_{Cn} \tag{4}$$

In a parallel configuration, multiple components perform the same function. However, the system reliability R_S is the complement of the system unreliability and it can be calculated by (5) [21], [22], [38].

$$R_S = 1 - \prod_{i=1}^{n} (1 - R_i) \tag{5}$$

Equation (5) is only used for 1ooN architectures, since the system will only fail if all of its components fail. For voting architectures (MooN, where $M \geq 2$), the logical equations must be used to calculate the system reliability R_S. This approach can be applied to all MooN architectures.

In a 1oo2 architecture, at least one device must function properly in order to perform the defined safety function. System reliability R_S is expressed by (6) [21], [22], [38]:

$$R_{S(1oo2)} = \bar{R}_1 R_2 + R_1 \bar{R}_2 + R_1 R_2 \tag{6}$$

where the equivalent failure rate is calculated by using (7).

$$\lambda = \frac{1}{\int_0^\infty R(t)\, dt} \tag{7}$$

The 1oo2 equivalent failure rate is defined as (8).

$$\lambda_{S(2oo3)} = \frac{2\lambda_{DU}}{3} \tag{8}$$

In a 2oo3 architecture, two components take a hand to perform a voting mechanism, then make the appropriate decision and execute the defined function. System reliability R_S is expressed by (9) [21], [22], [38].

$$R_{S(2oo3)} = \bar{R}_1 R_2 R_3 + R_1 \bar{R}_2 R_3 + R_1 R_2 \bar{R}_3 + R_1 R_2 R_3 \tag{9}$$

The 2oo3 equivalent failure rate is defined as (10).

$$\lambda_{S(2oo3)} = \frac{6\lambda_{DU}}{5} \tag{10}$$

As shown in Table 5, the PFH of the SPIDC 2oo3 system is equal to the system's undetected dangerous failure rate, which is 1,14E-07 per hour and is classified as SIL2. The probabilistic approach calculates the PFH using the system's equivalent failure rate without considering the proof test interval and common cause failures rate for redundant architectures.

Table 5. Calculation results of the PFH of SPIDC 2oo3 using fault tree analysis

Component instantiation	MooN	PFH(/h)
Master power supply	1oo1	9,78E-09
Master FPGA clock	1oo1	1,47E-08
Slave power supply	1oo2	1,63E-09
Slave FPGA clock	1oo2	2,44E-09
ADC+AMP	2oo3	4,84E-09
SPI_ADC	2oo3	8,88E-10
Slave safe transmission	1oo2	2,84E-10
Slave SPI transmission	1oo2	9,07E-11
Master SPI reception	1oo1	2,56E-09
Master safe transmission	1oo2	3,12E-10
Measurement comparator	1oo1	4,26E-10
SPID	2oo3	5,98E-10
Order comparator	1oo1	4,26E-10
SPI_DAC	1oo1	1,72E-09
DAC	1oo1	1,22E-08
Master communication	1oo1	2,88E-09
Slave communication	1oo2	7,67E-11
Pressure transmitter	2oo3	2,98E-08
Solenoid valve	1oo1	2,81E-08
	PFH(/h)	1,14E-07

4. MARKOV MODELS ANALYSIS

Markov models are one of the approaches provided by the IEC 61508 standard [4] to evaluate a safety instrumented system. This technique is often used in the safety function to model a system that contains repairable components with a constant failure rate. These models provide a dynamic analysis of the system. Safety instrumented systems are always performed by periodic tests called proof test interval. It is an off-line system verification to identify undetected dangerous failures using an FMEA. After this, the system is generally considered new. The state of the SIS and its probability are defined at test time using multiphase Markov chains. However, there is a single matrix M to calculate the probability distribution of all states Sj at $(k.T_1 + \Delta T)$ using the probability distribution at $(k.T_1)$ [11]:

$$p^{(kT_1+\Delta t)} = p^{(kT_1)}.M \tag{11}$$

where:

$$M = \begin{pmatrix} 1-\lambda_{00} & \lambda_{01} & \cdots & \lambda_{0r} \\ \lambda_{10} & 1-\lambda_{11} & \cdots & \lambda_{1r} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_{r0} & \lambda_{r1} & \cdots & 1-\lambda_{rr} \end{pmatrix} \tag{12}$$

The probability distribution calculation given by (11) is based on the probability distribution at the initial time $P^0 = (1 \quad 0 \quad 0 \quad ... \quad 0)$ (a row vector with 1 for the perfect state and 0 for the others) and the transition matrix M. On successive iterations, the vector $P^{(i)}$ is equal to $P^{(i-1)}.M$. Where PFD is $P^{(i)}(S_r)$, it defines the probability that the system is in out-of-service state (S_r) due to a dangerous undetected failure at time i. The probability of failure on demand per hour PFH can be calculated by the probability of a dangerous undetected failure PFD_i at time T_1 over entire interest time T_1 ($PFH = PFD/T_1$).

4.1. Markov chain models

4.1.1. Markov model of the 1oo1 architecture

Markov model of the 1oo1 architecture is shown in Figure 4, this model contains 4 states [10], [39]-[42]. E_1 represents the normal state, where the system works properly. E_2 represents the safe state, where the system has a safe failure according to the transition rate λ_S, it does not affect the system's safety function. The system can be repaired according to the transition rate $\mu_0 = \frac{1}{\tau_{test}}$. E_3 represents the state where the system has a dangerous detected failure. The system returns to a normal state according to the transition rates μ_0 and $\mu_R = \frac{1}{MTTR}$. E_4 represents a state where the system has a dangerous undetected failure. The system returns to a normal state according to the proof test interval. After that, the system is considered as new.

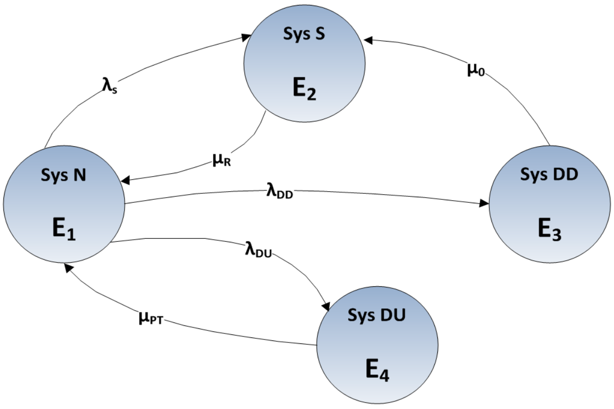


Figure 4. Markov model of the 1oo1 architecture

The (4×4) transition matrix M is given by [10], [39]-[42]:

$$M = \begin{pmatrix} 1-(\lambda_S+\lambda_D) & \lambda_S & \lambda_{DD} & \lambda_{DU} \\ \mu_R & 1-\mu_R & 0 & 0 \\ 0 & \mu_0 & 1-\mu_0 & 0 \\ \mu_{PT} & 0 & 0 & 1-\mu_{PT} \end{pmatrix} \tag{13}$$

4.1.2. Markov model of the 1oo2 architecture

Markov model of the 1oo2 architecture contains 7 states [10], [39]-[42], as shown in Figure 5. The critical state is the E_7 state when the booth channels of subsystems using the 1oo2 architecture, have a dangerous undetected failure. The (7×7) transition matrix N is given by [10], [39]-[42]:

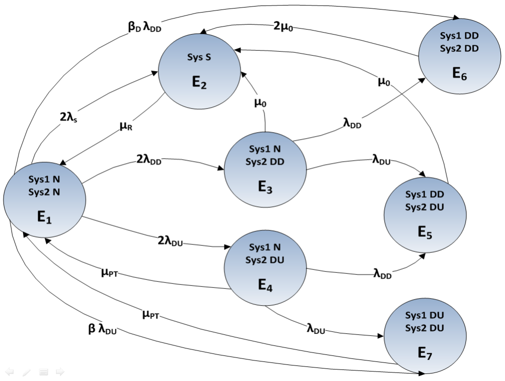


Figure 5. Markov model of the 1oo2 architecture

$$N = \begin{pmatrix} N_1 & 2\lambda_S & 2\lambda_{DD} & 2\lambda_{DU} & 0 & \beta_D\lambda_{DD} & \beta\lambda_{DU} \\ \mu_R & N_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mu_0 & N_3 & 0 & \lambda_{DU} & \lambda_{DD} & 0 \\ \mu_{PT} & 0 & 0 & N_4 & \lambda_{DD} & 0 & \lambda_{DU} \\ 0 & \mu_0 & 0 & 0 & N_5 & 0 & 0 \\ 0 & 2\mu_0 & 0 & 0 & 0 & N_6 & 0 \\ \mu_{PT} & 0 & 0 & 0 & 0 & 0 & N_7 \end{pmatrix} \tag{14}$$

where:

$$N_j = \lambda_{jj} = 1 - \sum_{\substack{k=0 \\ k \neq j}}^{7} \lambda_{jk} \tag{15}$$

4.1.3. Markov model of the 2oo3 architecture

Markov model of the 2oo3 architecture contains 11 states [10], [39]-[42], as presented in Figure 6. Critical states E_7, E_9, and E_{11} are states when any combination of two channels of subsystems using the 2oo3 architecture, have dangerous undetected failures, or all channels have dangerous failures. The (11×11) transition matrix P is given by [10], [39]-[42]:

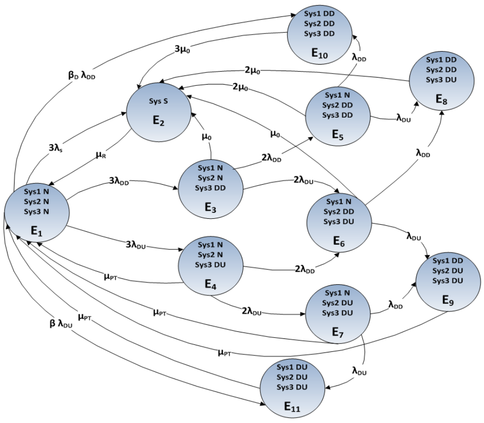


Figure 6. Markov model of the 2oo3 architecture

$$P = \begin{bmatrix} P_1 & 3\lambda_S & 3\lambda_{DD} & 3\lambda_{DU} & 0 & 0 & 0 & 0 & 0 & \beta_D\lambda_{DD} & \beta\lambda_{DU} \\ \mu_R & P_{22} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \mu_0 & P_3 & 0 & 2\lambda_{DD} & 2\lambda_{DU} & 0 & 0 & 0 & 0 & 0 \\ \mu_{PT} & 0 & 0 & P_4 & 0 & 2\lambda_{DD} & 2\lambda_{DU} & 0 & 0 & 0 & 0 \\ 0 & 2\mu_0 & 0 & 0 & P_5 & 0 & 0 & \lambda_{DD} & 0 & \lambda_{DU} & 0 \\ 0 & \mu_0 & 0 & 0 & 0 & P_6 & 0 & \lambda_{DD} & \lambda_{DU} & 0 & 0 \\ \mu_{PT} & 0 & 0 & 0 & 0 & 0 & P_7 & 0 & \lambda_{DD} & 0 & \lambda_{DU} \\ 0 & 2\mu_0 & 0 & 0 & 0 & 0 & 0 & P_8 & 0 & 0 & 0 \\ \mu_{PT} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_9 & 0 & 0 \\ 0 & 3\mu_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{10} & 0 \\ \mu_{PT} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{11} \end{bmatrix}$$

where:

$$P_j = \lambda_{jj} = 1 - \sum_{\substack{k=0 \\ k\neq j}}^{11} \lambda_{jk} \tag{16}$$

4.2. PFH calculation using the Markov models

The probability of failure on demand per hour (PFH) is the sum of all functional components PFH in the SPIDC 2oo3 [4]:

$$PFH = \sum PFH_{functionnel\ block(MooN)} \tag{17}$$

In Markov models, we choose a test time τ_{Test} of 24 hours, a mean time to repair (MTTR) of 8 hours, a lifetime of 12 years, and a proof test interval T_1 of one year. However, the component repair rate is μ_R, the component test is μ_0, and the component proof test rate is $\mu_{PT} = \frac{1}{T_1}$. For a simple architecture, the probability distribution at initial time is given by the row vector $P^0 = (1 \quad 0 \quad 0 \quad ... \quad 0)$; that is, the probability of being in the normal state at initial time is 100% and 0% for the other states. The probability distribution $P^{(n)}$ at a given time interval is determined by multiplying $P^{(0)}$ by $M^{(n)}$; where n is the time chosen to predict the probability of being in any state of the SPIDC 2oo3. For the power supply, the $M(4\times4)$ transition matrix is given by (13) is:

$$M = \begin{pmatrix} 9,99E-8 & 2,44E-8 & 1,46E-8 & 9,78E-9 \\ 1,25E-1 & 8,75E-1 & 0 & 0 \\ 0 & 4,16E-8 & 9,58E-1 & 0 \\ 1,14E-4 & 0 & 0 & 9,99E-1 \end{pmatrix}$$

The process of calculating the distribution probabilities $P^{(n)}$ is as follows:

$$p^{(1)} = p^{(0)}.M = (9,99E-8 \quad 2,44E-8 \quad 1,46E-8 \quad 9,78E-9)$$

$$...$$

$$p^{(n)} = p^{(n-1)}.M$$

This iterative process can continue indefinitely, and in each iteration, the probability distribution gradually increases. After 50790 hours, it has a stationary distribution row $P_L^{50790} = (9,99E-1 \quad 3,12E-7 \quad 3,52E-7 \quad 8,54E-5)$. This means that after 50790 hours, the probability of being in a dangerous undetected state is 8,54E-8 per hour, and this probability remains unchanged over time. The same steps are applied to different subsystems (sensor, logic solver, solenoid valve). The SPIDC 2oo3 probability of dangerous undetected failure over the system life time is illustrated in Figure 7; this probability is the sum of all component probabilities of being in a dangerous undetected failure. As it is shown by Figure 7, SPIDC 2oo3 system probability gradually increases over a period of time, then it has a limiting probability of failure. After 56510 hours, the SPIDC 2oo3 limit probability of being in the dangerous undetected failure state is 7,34E-4 per hour. According to the IEC 61508 standard, the system's PFH after one year is equal to the PFD over the entire operating time, resulting in a PFH of 5,30E-8 and thus SIL3.

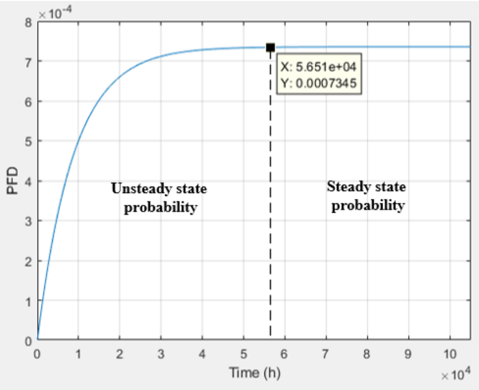


Figure 7. SPIDC 2oo3 system dangerous undetected state probabilities during 12 years

5. RESULTS AND DISCUSSION

SPIDC 2oo3 fault tree analysis shows that the system's dangerous undetected failure can be produced if either one of the subsystems using 1oo1 architecture, or both components of subsystems using 1oo2 architecture, or any combination of two components of subsystems using 2oo3 architecture, have dangerous undetected failures. Based on this approach, a proposed method was introduced to calculate PFH by considering the system as a single equivalent functional block, and its failure rate is determined by analysing the binary connections between different subsystems. In this method, the system has a PFH of 1,14E-07, which is associated with SIL2. Markov's approach is used to model the transitions between different states of a system throughout its life cycle, and to determine the system's probability to be in a particular state at a given time. The SPIDC 2oo3 probability of a dangerous undetected failure increases continuously with time and then has a limiting probability. Steady-state probability is the probability that the system will be in a determined state after a large number of transition periods, it does not mean that SPIDC 2oo3 system stays in one state, but it continues to move from one state to another over time periods. However, after an iterative process, the system's probability approaches its steady state. For the SPIDC 2oo3 system, after 56510 hours, the limit probability of being in a dangerous undetected failure state is 7,34E-4. After one year, SPIDC 2oo3 PFH value is 5,30E-08 per hour, using Markov models. Therefore, the system's safety integrity level is SIL3.

The fault tree analysis method estimates the system's PFH as its equivalent failure rate; it does not take into account common cause failures in the case of redundant architectures, and proof test interval. This difference in calculation can explain the different assignments of safety integrity levels. In addition, using the Markov models method, the probability of failure increases over time until the system reaches a steady state probability. However, the probabilistic method assigns the same probability of failure throughout the system life cycle. On the other hand, the 2oo3 voting architecture chosen in the measurement subsystem and the logic solver subsystem ensures the system safety and its availability in case of a dangerous undetected failure.

6. CONCLUSION

In this work, the 2oo3 architecture is used as a means to ensure the safety and availability of the measurement and control of the SPIDC 2oo3. This system uses a safety PID controller implemented in FPGA with 2oo3 architecture to control a pressure regulation system for a compressed nitrogen tank. The evaluation of the SPID 2oo3 is performed by the fault tree analysis and the Markov models to assign a safety integrity level. In order to evaluate the SPIDC 2oo3, the basic parameters (failure rate λ, diagnostic coverage DC, safety factor S) of each component of the system are defined. Using fault tree analysis, we have developed logical equations to evaluate the system's reliability. These equations are used to calculate the system's equivalent failure rate, which is considered as the system's probability of dangerous failure per Hour (PFH) according to the IEC 61508 standard. Under this method, the system has a PFH of 1,14E-07, and is assigned SIL2. In the case of Markov models, after one year, the SPIDC 2oo3 PFH value is 5,30E-08 per hour, this probability assigns SIL3 to the system. The difference in the SIL obtained can be explained by the fact that the fault tree analysis method estimates the system's PFH as its equivalent failure rate; it does not consider common cause failures in the context of the redundant architectures or the proof test interval.

REFERENCES

[1] IEC, "Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems," IEC 61508-2:2010, International Electrotechnical Commission, 2010. Accessed Nov 1, 2023. [Online] Available: https://webstore.iec.ch/publication/5516

[2] S. Eisinger and L. F. Oliveira, "Evaluating the safety integrity of safety systems for all values of the demand rate," *Reliability Engineering and System Safety*, vol. 210, Jun. 2021, doi: 10.1016/j.ress.2021.107457.

[3] ICE, "Functional safety: safety instrumented systems for the process industry sector. Part 1, Framework, definitions, system, hardware and application programming requirements," IEC 61511-1, International Electrotechnical Commission Geneva, Switzerland: International Electrotechnical Commission, 2017. Accessed Nov 1, 2023. [Online] Available: https://webstore.iec.ch/preview/infoiec61511-1

[4] ICE, "Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3," IEC 61508-6, International Electrotechnical Commission, 2010. Accessed Nov 1, 2023. [Online] Available: https://nobelcert.com/DataFiles/FreeUpload/IEC

[5] J. Fu, H. Li, Y. Chi, J. Zhen, and X. Xu, "nSIL evaluation and sensitivity study of diverse redundant structure," *Reliability Engineering and System Safety*, vol. 210, 2021, doi: 10.1016/j.ress.2021.107518.

[6] B. Galy and L. Giraud, "Risk mitigation strategies for automated current and future mine hoists," *Safety Science*, vol. 167, 2023, doi: 10.1016/j.ssci.2023.106267.

[7] H. Metatla and M. Rouainia, "Functional and dysfunctional analysis of a safety instrumented system (SIS) through the common cause failures (CCFs) assessment. Case of high integrity protection pressure system (HIPPS)," *International Journal of System Assurance Engineering and Management*, vol. 13, no. 4, pp. 1932–1954, 2022, doi: 10.1007/s13198-021-01608-8.

[8] K. Babouri and R. Bendib, "Assessment of safety integrity requirements for fired heater system in accordance with IEC 61508," *International Journal of Latest Engineering Science (IJLES)*, vol. 2, no. 5, 2019.

[9] B. Naoual, R. Bendib, Z. Youcef, and A. Tedjani, "Fuzzy approach for safety integrity level evaluation to improve the safety of an industrial fired heater," *International Journal of System Assurance Engineering and Management*, vol. 14, no. 6, pp. 2497–2513, 2023, doi: 10.1007/s13198-023-02103-y.

[10] W. M. Goble, *Control systems safety and reliability*. International Society of Automation, 2010.

[11] W. Mechri, C. Simon, F. Bicking, and K. Ben Othman, "Fuzzy multiphase Markov chains to handle uncertainties in safety systems performance assessment," *Journal of Loss Prevention in the Process Industries*, vol. 26, no. 4, pp. 594–604, 2013, doi: 10.1016/j.jlp.2012.12.002.

[12] H. Azizpour and M. A. Lundteigen, "Analysis of simplification in Markov-based models for performance assessment of safety instrumented system," *Reliability Engineering and System Safety*, vol. 183, pp. 252–260, 2019, doi: 10.1016/j.ress.2018.09.012.

[13] S. Wu, L. Zhang, A. Barros, W. Zheng, and Y. Liu, "Performance analysis for subsea blind shear RAM preventers subject to testing strategies," *Reliability Engineering and System Safety*, vol. 169, pp. 281–298, 2018, doi: 10.1016/j.ress.2017.08.022.

[14] P. Chen, Q. Lin, and X. Han, "Taking 2oo3 as an example to study the improvement of Markov model considering periodic function test," *Journal of Physics: Conference Series*, vol. 2264, no. 1, 2022, doi: 10.1088/1742-6596/2264/1/012008.

[15] S. Alizadeh and S. Sriramula, "Unavailability assessment of redundant safety instrumented systems subject to process demand," *Reliability Engineering and System Safety*, vol. 171, pp. 18–33, 2018, doi: 10.1016/j.ress.2017.11.011.

[16] A. Wakankar, A. Kabra, A. K. Bhattacharjee, and G. Karmakar, "Architectural model driven dependability analysis of computer based safety system in nuclear power plant," *Nuclear Engineering and Technology*, vol. 51, no. 2, pp. 463–478, 2019, doi: 10.1016/j.net.2018.10.019.

[17] H. Omeiri, B. Hamaidi, F. Innal, and Y. Liu, "Verification of the IEC 61508 PFH formula for 2oo3 configuration using Markov chains and Petri nets," *International Journal of Quality and Reliability Management*, vol. 38, no. 2, pp. 581–601, 2021, doi: 10.1108/IJQRM-09-2019-0305.

[18] H. Omeiri, F. Innal, and Y. Liu, "Consistency checking of the IEC 61508 PFH Formulas and New Formulas Proposal Based on the Markovian Approach," *Journal Europeen des Systemes Automatises*, vol. 54, no. 6, pp. 871–879, 2021, doi: 10.18280/jesa.540609.

[19] H. Ahangari, Y. İ. Özkök, A. Yıldırım, F. Say, F. Atik, and O. Ozturk, "Architecture for safety–critical transportation systems," *Microprocessors and Microsystems*, vol. 98, Apr. 2023, doi: 10.1016/j.micpro.2023.104818.

[20] W. Jiakun, C. Yuan, M. A. Lianchuan, and D. U. Siqi, "Design and analysis of double one out of two with a hot standby safety redundant structure," *Chinese Journal of Electronics*, vol. 29, no. 3, pp. 586–594, 2020, doi: 10.1049/cje.2020.03.015.

[21] J. Menčík, "Reliability of systems," in *Concise Reliability for Engineers*, InTech, 2016.

[22] F. E. Nadir;Hadj Baraka;Amami, "PFH calculation of a PID controller 2oo3 system implemented in FPGA using reliability block diagram," *International Journal of Research in Business and Technology*, vol. 10, no. 2, 2018, doi: 10.17722/ijrbt.v10i2.496.

[23] A. T. Hashim, A. M. Hasan, and H. M. Abbas, "Design and implementation of proposed 320 bit RC6-cascaded encryption/decryption cores on altera FPGA," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 6, pp. 6370–6379, Dec. 2020, doi: 10.11591/ijece.v10i6.pp6370-6379.

[24] S. Q. Hadi, A. A. Jafaar, B. M. Alameri, and S. A. Malallah, "Field programmable gate array implementation of multiwavelet transform based orthogonal frequency division multiplexing system," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 5, pp. 5136–5144, 2022, doi: 10.11591/ijece.v12i5.pp5136-5144.

[25] F. A. Silaban, S. Budiyanto, and W. K. Raharja, "Stepper motor movement design based on FPGA," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 151–159, 2020, doi: 10.11591/ijece.v10i1.pp151-159.

[26] M. Abdelawwad, A. Hayek, A. Alsuleiman, and J. Borcsok, "FPGA implementation of a safety system-on-chip based on 1oo4 architecture using LEON3 processor," in *2018 International Conference on Computer and Applications*, pp. 231–235, 2018, doi: 10.1109/COMAPP.2018.8460288.

[27] A. R. Khatri, A. Hayek, and J. B¨orcs¨ok, "Validation of the proposed hardness analysis technique for FPGA designs to improve reliability and fault-tolerance," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 12, pp. 1–8, 2018, doi: 10.14569/IJACSA.2018.091201.

[28] M. Abdelawwad, A. Hayek, A. Alsuleiman, and J. Borcsok, "FPGA implementation of a safety system-on-chip based on 1oo4 architecture using LEON3 processor," in *2018 International Conference on Computer and Applications (ICCA)*, Aug. 2018, pp.

231–235, doi: 10.1109/COMAPP.2018.8460288.

[29] Xilinx Corporation, *Spartan-3E FPGA starter kit board user guide*, UG230 (v1.2), January 20, 2011, Accessed: Nov 1, 2023. [Online] Available: https://docs.xilinx.com/v/u/en-US/ug230

[30] W. M. Goble, *Field failure data – the good, the bad and the ugly*, Exida, February 2012, Accessed: Nov 1, 2023. [Online] Available: https://www.exida.com/images/uploads/Field_Failure_Rates-good_bad_and_ugly_Feb_2012.pdf

[31] R. Chalupa, "Failure modes, effects and diagnostic analysis, project: 3051 pressure transmitter with 4-20 mA," Exida, February 2023, Accessed: Nov 1, 2023. [Online] Available: https://www.emerson.com/documents/automation/functional-safety-certificate-fmeda-report-3051-pressure-transmitter-en-89446.pdf

[32] Siemens Norm, *Part 2: Expected values for integrated circuits*, Edition 2004-12, 2004, Accessed: Nov 1, 2023. [Online] Available: https://fr.scribd.com/document/630346312/SIEMENS-SN-29500-2-2004

[33] Siemens Norm, *Part 4: Expected values for passive components*, Edition 2004-3,2004, Accessed: Nov 1, 2023. [Online] Available: https://fr.scribd.com/document/630346419/SIEMENS-SN-29500-4-2004

[34] *Spartan-3E FPGA family data sheet*, Xilinx, 2018, Accessed: Nov 1, 2023. [Online] Available: https://docs.xilinx.com/v/u/en-US/ds312

[35] Xilinx Corporation, *Spartan-3E libraries guide for HDL designs*, UG617 (v14.7), October 2, 2013, Accessed: Nov 1, 2023. [Online] Available: http://hep.bu.edu/~jlraaf/Xilinx/S3E_libraries_hdl.pdf

[36] *Device reliability report*, UG116 (v10.5.1), May 17, 2023, Accessed: Nov 1, 2023. [Online] Available: https://docs.xilinx.com/r/en-US/ug116

[37] I. van Beurden, "IEC 61508 functional safety assessment, project: series 307 selenoid valves," Exida, Accessed: Nov 1, 2023. [Online] Available: https://www.exida.com/images/upload_13/ASC_10-10-022_R001_V1_R2_IEC_61508_Assessment_307_Solenoid.pdf

[38] F. Ciutat, "SIL - automation and safety: integrity of safety automated functions," (in French), APTA, 2nd Ed, 2011, pp. 235-245.

[39] S. Alizadeh and S. Sriramula, "Impact of common cause failure on reliability performance of redundant safety related systems subject to process demand," *Reliability Engineering and System Safety*, vol. 172, pp. 129–150, 2018, doi: 10.1016/j.ress.2017.12.011.

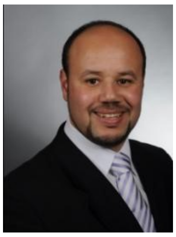
[40] S. Alizadeh and S. Sriramula, "Reliability modelling of redundant safety systems without automatic diagnostics incorporating common cause failures and process demand," *ISA Transactions*, vol. 71, pp. 599–614, 2017, doi: 10.1016/j.isatra.2017.09.007.

[41] A. Hayek, M. Al Bokhaiti, M. H. Schwarz, and J. Boercsoek, "Sophisticated calculation of the 1oo4-architecture for safety-related systems conforming to IEC61508," *Journal of Physics: Conference Series*, vol. 364, no. 1, 2012, doi: 10.1088/1742-6596/364/1/012059.

[42] R. Thum and J. Borcsok, "Enhancement of reliability and precision of navigation by odometry," in *2021 18th International Multi-Conference on Systems, Signals and Devices (SSD)*, Mar. 2021, pp. 638–643, doi: 10.1109/SSD52085.2021.9429385.

BIOGRAPHIES OF AUTHORS

Fatima Ezzahra Nadir received the Ph.D. degree in embedded systems and automation from the Faculty of Sciences and Technologies Tangier, Morocco and the M.E. degree in electronics, electrotechnics and automation from the same faculty in 2013. She is currently professor of electrical engineering at the Higher School of Technology, Agadir, Ibn Zohr University and member of the Laboratory of Engineering Sciences and Energy Management (LASIME), in the research team: optimization of industrial systems (EROSI). Her research interests include safety embedded systems, automation systems, and robotics. She can be contacted by email: f.nadir@uiz.ac.ma.



Mohammed Bsiss received Ph.D. in embedded systems and automatics from the Faculty of Sciences and Technology Tangier in 2014. Currently, professor of electrical engineering at the Faculty of Science and Technology, Tangier, Morocco. He specializes in process control and embedded systems. He can be contacted by email: mbsiss@uae.ac.ma.

Benaissa Amami received Ph.D. from Paris 6 University in 1992, professor of electrical engineering at the Faculty of Science and Technology, Tangier, Morocco. He specializes in process control and embedded systems. Currently, expert of the ANEAQ organization in Morocco. He can be contacted by email: b.amami@uae.ac.ma.