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

Fatima Ezzahra Nadir¹, Mohammed Bsiss², Benaissa Amami²

¹Laboratory of Engineering Sciences and Energy Management, Research Team: Optimization of Industrial Systems, Higher School of Technology, Ibn Zohr University, Agadir, Morocco
²Intelligent Automation and BioMedGenomics Laboratory, Faculty of Sciences and Technologies, Abdelmalek Essaâdi University, Tangier, Morocco

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.

This is an open access article under the CC BY-SA license.

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
The SPIDC 2003, 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 is used for the analog-to-digital 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 2003 block diagram.

Figure 1. Subsystems used to regulate the tank pressure

Figure 2. SPIDC 2003 block diagram

### 2.2. SPIDC 2003 system element failure rate

To perform a quantitative analysis, the failure rate of each component in the SPIDC 2003 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 \( \lambda \) is specified by Exida 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, 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.
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 $\lambda$ depends on the reference failure rate $\lambda_{ref}$ in failure in time (FIT), reference average ambient temperature, reference virtual junction temperature, actual virtual junction temperature. The reference failure rate $\lambda_{ref}$ 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 $\lambda$, 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

<table>
<thead>
<tr>
<th>Component</th>
<th>$\lambda$/h</th>
<th>S(%)</th>
<th>DC(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADC</td>
<td>$6.11E-8$</td>
<td>50</td>
<td>90</td>
</tr>
<tr>
<td>DAC</td>
<td>$6.11E-8$</td>
<td>50</td>
<td>60</td>
</tr>
<tr>
<td>AMP</td>
<td>$1.95E-8$</td>
<td>50</td>
<td>60</td>
</tr>
<tr>
<td>PWR</td>
<td>$4.89E-8$</td>
<td>50</td>
<td>60</td>
</tr>
<tr>
<td>CLK</td>
<td>$7.33E-8$</td>
<td>50</td>
<td>60</td>
</tr>
</tbody>
</table>

Table 3. XC3S500E FPGA components basic parameters

<table>
<thead>
<tr>
<th>Component Instantiation</th>
<th>$\lambda$/h</th>
<th>S(%)</th>
<th>DC(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>XC3S500E FPGA Target</td>
<td>$3.97E-7$</td>
<td>50</td>
<td>90</td>
</tr>
<tr>
<td>SPI_ADC</td>
<td>$1.48E-8$</td>
<td>50</td>
<td>90</td>
</tr>
<tr>
<td>Measurement Comparator</td>
<td>$2.13E-9$</td>
<td>50</td>
<td>60</td>
</tr>
<tr>
<td>SPID</td>
<td>$9.97E-9$</td>
<td>50</td>
<td>90</td>
</tr>
<tr>
<td>Order Comparator</td>
<td>$2.13E-9$</td>
<td>50</td>
<td>60</td>
</tr>
<tr>
<td>SPI_DAC</td>
<td>$8.61E-9$</td>
<td>50</td>
<td>60</td>
</tr>
<tr>
<td>Master SPI Reception</td>
<td>$1.28E-8$</td>
<td>50</td>
<td>60</td>
</tr>
<tr>
<td>Slave SPI Transmission</td>
<td>$2.72E-9$</td>
<td>50</td>
<td>90</td>
</tr>
<tr>
<td>Master Safe Transmission</td>
<td>$9.37E-9$</td>
<td>50</td>
<td>90</td>
</tr>
<tr>
<td>Slave Safe Transmission</td>
<td>$8.52E-9$</td>
<td>50</td>
<td>90</td>
</tr>
<tr>
<td>Master Communication</td>
<td>$1.44E-8$</td>
<td>50</td>
<td>60</td>
</tr>
<tr>
<td>Slave Communication</td>
<td>$2.3E-9$</td>
<td>50</td>
<td>90</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Component</th>
<th>$\lambda$/h</th>
<th>S(%)</th>
<th>DC(%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solenoid Valve</td>
<td>$7.02E-7$</td>
<td>10</td>
<td>60</td>
</tr>
</tbody>
</table>
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 2003 dangerous undetected failures. This method provides a binary representation that distinguishes between various causes that generate a SPIDC 2003 dangerous undetected failures in [5]-[9]. Figure 3 shows the SPIDC 2003 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 1001 architecture, such as the valve, or both components of subsystems using the 1002 architecture, such as the slave1 SPI transmission, or any combination of two components of subsystems using the 2003 architecture, such as the pressure transmitter, have dangerous undetected failures.

![Figure 3. SPIDC 2003 system fault tree analysis](image)

3.2. Quantitative analysis using fault tree method

The fault tree analysis, shown in Figure 3, outlines how the various components of the SPIDC 2003 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]:

\[ PFH(T) = \lambda_{DU} \]  

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 \( \lambda_{C_i} \). The equation representing \( R_S \) is as (2) [21], [22], [38]:

\[ R_S = \prod_{i=1}^{n} R_i \]  

where:

\[ R(t) = e^{-\lambda t} \]  

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

\[ \lambda_S = \sum_{i=1}^{n} \lambda_{C_i} = \lambda_{C1} + \lambda_{C2} + \ldots + \lambda_{Cn} \]  

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]:

\[ R_S = 1 - \prod_{i=1}^{n} (1 - R_i) \]
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]:

\[
R_{S(1oo2)} = \bar{R}_1 R_2 + R_1 \bar{R}_2 + R_1 R_2
\]  

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

\[
\lambda = \frac{1}{\int_0^{\infty} R(t) \ dt}
\]  

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

\[
\lambda_{S(2oo3)} = \frac{2\lambda_{DU}}{3}
\]  

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]:

\[
R_{S(2oo3)} = \bar{R}_1 R_2 R_3 + R_1 \bar{R}_2 R_3 + R_1 R_2 \bar{R}_3 + R_1 R_2 R_3
\]  

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

\[
\lambda_{S(2oo3)} = \frac{6\lambda_{DU}}{5}
\]  

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

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

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 $S_j$ at $(k.T_1 + \Delta T)$ using the probability distribution at $(k.T_1)$:

$$p^{(kT_1+\Delta t)} = p^{(kT_1)} \cdot M \quad (11)$$

where:

$$M = \begin{pmatrix}
1 - \lambda_{00} & \lambda_{01} & \ldots & \lambda_{0r} \\
\lambda_{10} & 1 - \lambda_{11} & \ldots & \lambda_{1r} \\
\vdots & \vdots & \ddots & \vdots \\
\lambda_{r0} & \lambda_{r1} & \ldots & 1 - \lambda_{rr}
\end{pmatrix} \quad (12)$$

The probability distribution calculation given by (11) is based on the probability distribution at the initial time $P^0 = (1 \ 0 \ 0 \ldots \ 0)$ (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 $P^{(i-1)} \cdot M$. 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 $\lambda_S$, 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 proof test interval. After that, the system is considered as new.

![Figure 4. Markov model of the 1oo1 architecture](image)

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

$$M = \begin{pmatrix}
1 - (\lambda_S + \lambda_D) & \lambda_S & \lambda_{DD} & \lambda_{DU} \\
\mu_R & 1 - \mu_R & 0 & 0 \\
0 & \mu_0 & 1 - \mu_0 & 0 \\
\mu_{PT} & 0 & 0 & 1 - \mu_{PT}
\end{pmatrix} \quad (13)$$
4.1.2. Markov model of the 1002 architecture

Markov model of the 1002 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 1002 architecture, have a dangerous undetected failure. The $(7 \times 7)$ transition matrix $N$ is given by [10], [39]-[42]:

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

(14)

where:

$$N_j = \lambda_{jj} = 1 - \sum_{k=0}^{7} \lambda_{jk}$$

(15)

4.1.3. Markov model of the 2003 architecture

Markov model of the 2003 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 2003 architecture, have dangerous undetected failures, or all channels have dangerous failures. The $(11 \times 11)$ transition matrix $P$ is given by [10], [39]-[42]:

Figure 5. Markov model of the 1002 architecture

Figure 6. Markov model of the 2003 architecture
of being in any state of the SPIDC 2oo3. For the power supply, the time interval is determined by multiplying \( P \)
the normal state at initial time is 100% and 0% for the other states. The probability distribution \( P \)
tion at initial time is given by the row vector \( \mu \):
\[ P = \begin{bmatrix} P_1 & 3\lambda_s & 3\lambda_{DD} & 3\lambda_{DU} & 0 & 0 & 0 & 0 & 0 & \beta_D \lambda_{DD} & \beta \lambda_{DU} \\ \mu_R & P_{22} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \mu_0 & P_3 & 0 & 2\lambda_{DD} & 2\lambda_{DU} & 0 & 0 & 0 & 0 & 0 & 0 \\ \mu_{PT} & 0 & P_4 & 0 & 2\lambda_{DD} & 2\lambda_{DU} & 0 & 0 & 0 & 0 & 0 \\ 0 & 2\mu_0 & 0 & 0 & P_5 & 0 & 0 & \lambda_{DD} & 0 & \lambda_{DU} & 0 \\ 0 & \mu_0 & 0 & 0 & 0 & P_6 & 0 & \lambda_{DD} & \lambda_{DU} & 0 & 0 \\ 0 & 2\mu_0 & 0 & 0 & 0 & 0 & 0 & P_7 & 0 & \lambda_{DD} & 0 & \lambda_{DU} \\ 0 & \mu_0 & 0 & 0 & 0 & 0 & 0 & 0 & P_8 & 0 & 0 & 0 \\ 0 & 3\mu_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & P_{10} & 0 \end{bmatrix} \]
where:
\[ P_j = \lambda_{jj} = 1 - \sum_{\substack{k=0 \atop k \neq j}}^{11} \lambda_{jk} \]  
\[ (16) \]

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]:
\[ PFH = \sum PFH_{functionel block(MooN)} \]  
\[ (17) \]
In Markov models, we choose a test time \( T_{test} \) 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 \( \mu_R \), the component test is \( \mu_0 \), 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 \( P^0 = (1 \ 0 \ 0 \ ... \ 0) \); that is, the probability of being in the normal state at initial time is 100% and 0% for the other states. The probability distribution \( P^{(n)} \) 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 \( M(4 \times 4) \) 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:
\[ p^{(1)} = p^{(0)} \cdot M = (9.99E-8 \ 2.44E-8 \ 1.46E-8 \ 9.78E-9) \]
\[ ... \]
\[ p^{(n)} = p^{(n-1)} \cdot M \]
This iterative process can continue indefinitely, and in each iteration, the probability distribution gradually increases. After 50790 hours, it has a stationary distribution row \( P_{50790} = (9.99E-1 \ 3.12E-7 \ 3.52E-7 \ 8.54E-5) \). 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.
5. RESULTS AND DISCUSSION

SPIDC 2003 fault tree analysis shows that the system’s dangerous undetected failure can be produced if either one of the subsystems using 1001 architecture, or both components of subsystems using 1002 architecture, or any combination of two components of subsystems using 2003 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 2003 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 2003 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 2003 system, after 56510 hours, the limit probability of being in a dangerous undetected failure state is 7.34E-4. After one year, SPIDC 2003 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 2003 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 2003 architecture is used as a means to ensure the safety and availability of the measurement and control of the SPIDC 2003. This system uses a safety PID controller implemented in FPGA with 2003 architecture to control a pressure regulation system for a compressed nitrogen tank. The evaluation of the SPID 2003 is performed by the fault tree analysis and the Markov models to assign a safety integrity level. In order to evaluate the SPIDC 2003, 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 derived 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 2003 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


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.