Design of an innovative proximity detection embedded-system for safety application in industrial machinery

Stefano Dalpez, Alessandro Vaccari
FBK-REET Research Group,
Fondazione Bruno Kessler,
Italy
sdalpez@fbk.eu

Roberto Passerone, Alberto Penasa
Department of Information Engineering
and Computer Science,
University of Trento, Italy
roberto.passerone@unitn.it

Abstract

Safety of machine operation is an increasingly important matter in industrial applications. In this context, embedded systems have successfully been employed to build active barriers that react in real time to prevent injuries and accidents. In this paper, we present a novel safety barrier, based on the capacitive coupling effect, to detect the proximity of the hands to a dangerous zone. Our study focuses on the safety design phases of the system, according to rule IEC 62061, including safety hazard analysis, SIL allocation, and hardware design applied to a real industrial machine for "stone cutting" purpose. Compliance checking of reliability and safe failure fraction was performed through FMEA methods ensuring that the system can satisfy the SIL 2 safety level constraints.

1. Introduction

The use of information technologies and of embedded systems in particular in industrial processes has been instrumental in recent years to improve the safety of human operated machines and avert accidents and injury due to system malfunctions and/or lack of attention. Embedded systems, in particular, are used to detect potentially hazardous situations by processing the information that sensors provide about the environment, and by reacting in real time to build virtual barriers that prevent negative consequences from taking place. In this context, the correctness and reliability of the control embedded systems is of particular importance to ensure its full availability and to guarantee a predictable behavior. A set of regulations have been devised in the form of standards to ensure that systems comply with the desired level of safety. In this paper, we present a case study on the design of a safety critical embedded system, from the detection technology to the safety-related design process according to the relevant norms.

Nowadays capacitive sensors are widely used in many industrial applications [17], especially on consumer devices and handled computers, due to the low cost production and excellent operating characteristics. The application of these capacitive sensors in industrial environments where safety plays a major role is a common practice in recent years, though often limited to passive proximity detection of metal objects or limiting switches for industrial automation [2]. Less often, these techniques are used for directly detection of human presence to prevent risk and hazard in industrial machines where safety is a main issue. With this aim we developed a new proximity detection methodology [3] designed ad hoc for processing machines, such as presses and work tools built to break natural or artificial stones. Our case study is mainly focused on "stone-breaking" machines that consist in two cutting tools vertically moving over a horizontal table where stones are manually placed for cutting.

Our work has two main purposes: to present a new capacitive sensing technique and to apply this for designing of a new safety barrier in accordance to the rule IEC 62061 [14] and other sector rules. Design aspects involved hardware and functional issues with an evaluation of safety implications that resulted in a SIL 2 level for our application. We have then developed an advanced embedded prototype to evaluate the performance of the system with good repeatability and accuracy. This ensures an adequate level of "freedom from unacceptable risks" [13], as required by regulations, without interfering with the worker productivity, which is otherwise drastically affected by traditional safety barriers.

Our adopted methodology for safety analysis and verification of qualitative and quantitative constraints adheres to the current European rules and applies a conservative checking method [19] with a reduced computation complexity. Our conclusion is that the quantitative safety analysis of the Safe Failure Fraction (SFF) and reliability can reduce development time and costs if done in the early stages of design. The estimation of safety parameters and the design results have been obtained conservatively, due to the current lack of accurate reliability and failure modes data for various new components used in the system. Improving these aspects is part of our future work.

978-1-4673-4737-2/12/$31.00 ©2012 IEEE

2. Related work

Industry standards are the starting point for designing a safety-related embedded systems for industrial application. The general rule in this context is IEC 61508 [13] and, in particular, the new rule IEC 62061 [14] represents an essential reference for the design of safety related systems in industrial machinery. Rules define general methodologies and requirements that systems must meet to be certified as "safe". Our approach will mainly follow these rules with some improvements where degrees of freedom are left to the designer. In the following we discuss work related to our case study, from the preliminary design stages, to hardware design and to compliance checking.

For hazard analysis, Anderson [1] presents a methodology, based on a quantitative point of view that can be applied during a machine development process. The method is mainly focused on hazard classification and evaluation based on a list of risks commonly found in industrial machine environment. This methodology can be applied to our case, ensuring a quantitative classification. This method is compatible with rule IEC 62061 [14] and is used in our work for hazard classification.

After hazard classification, designers must select the system architecture and its components. These choices can heavily affect the cost of the design. Related to this matter, Griessnig *et al.* [7] propose a programmable logic approach to implement the analysis and control logic instead of the classical CPU/DSP approach. FPGA and CPLD devices requires minor software development due to the lack of RAM and CPU that otherwise require online and startup tests. On the other hand, Salewski *et al.* [18] focus on development issues of programmable logic that can be more complex in safety industrial applications, but with clear benefits due to their performance and the parallel nature of these components. Programmable logic also allows systems with on-chip redundancy and diagnostic features to be built, as shown in the work of Girardey *et al.* [6]. Our approach adheres to a programmable logic design for the greater simplicity of hardware and software and for the performance that are more suitable in this case study.

To check safety designed parameters, Catelani *et al.* [4] propose a method for the assessment of the intrinsic safety of the designed system. They use Failure Mode and Effect, Diagnostic Analysis (FMEDA) to evaluate the Safe Failure Fraction (SFF) of the system. Our approach will be slightly different and closer to the requirements of rule IEC 62061 [14], although some estimates have been made using their approach for failure mode classification and requirements checking.

3. Proximity detection

Various possible detection mechanisms for the position of the operator's hands have been devised, in such a way that a control volume around the moving blade is constantly monitored and, when either one or both the hands enter that volume of space, an alert signal is emitted. Various solutions exploit magnetic fields through the use of inductances whose values are locally perturbed by the hands, but these do not provide sufficient vertical sensitivity and are expensive. Hands could also be detected by means of a radiofrequency signals in the $15 \div 30$ GHz range. This solution would be extremely expensive, giving raise to problems in receiving and transponding the signal.

3.1. Capacitive coupling

The detection principle chosen in this work is based on electrostatic induction, or capacitive coupling, between conducting gloves covering the operator's hands and two conducting sensing bars located on both sides of the moving blade. The sensing bars expose a large part of their surface to the free space in such a way that the approaching "active gloves", equipped with a small battery-powered signal generator integrated in each glove, can shift the bars electric potential away from the reference level, represented by the ground potential of the splitting machine chassis. The induced potential is distance-dependent, a fact which can be used to gauge the extension of the control volume. The frequency of the inducing signals is high, around 100 kHz, to avoid interference with static or power supply fields ($50 \div 60$ Hz and their harmonics), yet the wavelength is sufficiently long that the field distribution is like an electrostatic one, and the magnetic field can be neglected.

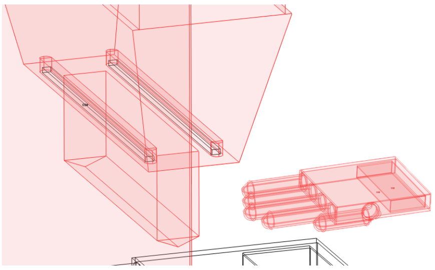


Figure 1. Detail of the sensing elements and conducting glove

Figure 1 shows details of the blade supporting block with the sensing bars housed in re-entrant grooves and of the model of the operator hand with glove. From an electrostatic point of view, the detection mechanism is based on four distinct conducting objects, numbered from 1 to 4 in Figure 2, which are mutually isolated and represent respectively:

1. The splitting machine chassis, including the blade supporting block, for which $V_1 = 0$ (reference or ground potential);
2. either one of the sensing bars, which assumes a potential $V_2 = 0$, with respect to ground, in response to

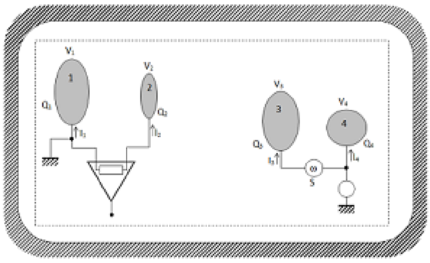


Figure 2. Electric schematic of the system

the hand-with-glove proximity;

3. either one of the gloves, which has a potential $V_3 = S$ by means of an onboard miniaturized signal generator;
4. Operator's body, which is electrically connected to ground through a noise generator. In what follows it is assumed $V_4 = 0$, neglecting the noise voltage.

In Figure 2 the enclosing boundary represents the surrounding space which at infinity is at zero potential like the ground, and which also means that the four objects are isolated from the rest of universe, but with the dashed rectangle remarking us that we are really modeling only a finite volume of space. Figure 2 depicts also schematically the input stage of the amplifier, which detects the potential induced on the sensing bars and indicates the positive electric currents I on the four objects.

The potentials V and the currents I are related through the linear relations:

$$\begin{cases} I_1 = j\omega\,(c_{11}V_1 + c_{12}V_2 + c_{13}V_3 + c_{14}V_4) \\ I_2 = j\omega\,(c_{21}V_1 + c_{22}V_2 + c_{23}V_3 + c_{24}V_4) \\ I_3 = j\omega\,(c_{31}V_1 + c_{32}V_2 + c_{33}V_3 + c_{34}V_4) \\ I_4 = j\omega\,(c_{41}V_1 + c_{42}V_2 + c_{43}V_3 + c_{44}V_4) \end{cases} \tag{1}$$

where $j = \sqrt{-1}$ is the imaginary unit and the c_{mn} are the capacity coefficients (measured in Farad), which depend on the system geometry only and are symmetrical in the m, n indexes. These linear relations derive from the purely electrostatic ones, which hold true among the electric charges Q on the objects and their respective potentials V, due to the linear superposition principle valid for the solutions of the Laplace equation.

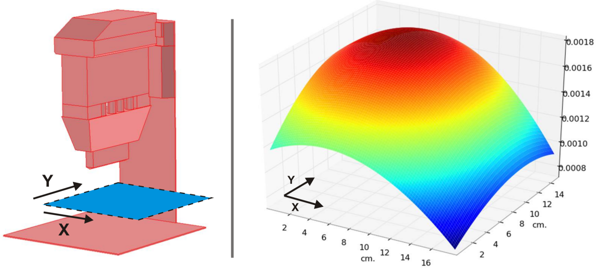
By means of the above linear relations and from the charge conservation principle $I_1 + I_2 + I_3 + I_4 = 0$, one could get the Thévenin equivalent voltage generator of the system at the amplifier input:

$$V_2 = -\frac{c_{23}}{c_{22}} S \tag{2}$$

which is proportional to the c_{23} coefficient measuring the coupling between the conducting glove and the sensing bar (in presence of the remaining objects) and which is amenable to decrease, for given sizes, with the distance. One could also get the equivalent capacitive output impedance of the generating signal system.

3.2. Simulation result

Rather than studying the system response by analyzing, via numerical simulation, the behavior of these capacity coefficients with a varying operator's hand position, we give directly graphs of the numerically calculated induced potential V_2 on one sensing bar, normalized to the voltage of the glove signal generator, as a function of the distance from the bar, on an area of about 14 cm. × 14 cm. at a given fixed height as shown in Figure 3a.



(a)

(b)

Figure 3. Simulated Induced potential as a function of hand position: (a) observation plane (b) result graph

The blade effectively runs on the left edge in the graph, thus qualitatively showing a decaying induced potential with an increasing distance from the bar, and a peak located near the bar centre. This is the expected ideal response of the system. The behavior of a real system is given in Figure 4, which shows the measured induced potential, normalized to its maximum value instead of to the inducing signal amplitude, for various positions of the active glove on a (smaller) area of 7 cm. × 7 cm. below and to the right of the splitting blade (which as before stays along the left edge of the graph).

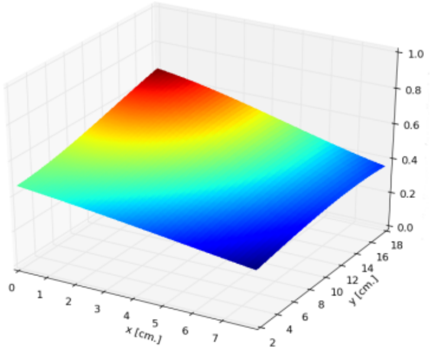


Figure 4. Measured potential as a function of the distance

Although less ideal, with the peak backwardly shifted and more flattened than the numerically calculated one (which was necessarily obtained from a simplified copy of the splitting machine and with ideal truncation at the exterior boundaries of the model volume) the decaying behavior of the sensed potential around the blade, which is at the base of the detection mechanism, persists also in a real situation. Having thus established the rationale of the electrostatic (or capacitive) coupling, we can briefly analyze the response of one side of the generating signal system by means of the following equivalent electric circuit (Figure 5), made of lumped dipole elements:

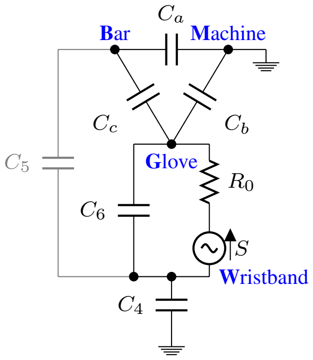


Figure 5. Equivalent electric circuit

In the electric circuit the four objects, previously introduced in the scheme of Figure 2, are represented as nodes denoted by the letters B (sensing bar) for object no. 1, M (machine) for object no. 2, G (glove) for object no. 3, W (wristband) for object no. 4 respectively. The wristband is electrically connected to the operator's body and is introduced as a distinct equipment part due to the necessity of an electric contact for one of the poles of the onboard signal generator S. The other pole is connected to the conducting sheet of the glove, with a possibly non ideal internal resistance R_o. The equivalent voltage and output impedance of the network can be calculated as seen between the nodes B and M, which are the entrance dipole of the detecting amplifier input. The equivalent voltage will be directly proportional to S through a coefficient which depends on the various lumped capacitances appearing in the network and which plays the same role as the ratio $-c_{23}/c_{22}$ previously seen in the framework of the Laplace equation. Figure 6 shows how, as a consequence of the model of Figure 5 the calculated normalized voltage (per unit voltage of the signal generator amplitude) of the node B (with respect to node M) according to the model of Figure 5, rises as expected when the capacitance of C_c varies in the range 0 ÷ 10 pF (i.e., decreasing the distance between the glove and the blade), for two values of the internal resistance R_o, assuming very high (infinite) the capacitance value of C_4.

4. Safety issue and European rules

Industrial machines are often dangerous, especially when they are designed to work with moving parts and cutting blades that can produce serious injury to workers. In our case study, a special steel blade is used to split various types of stones. The blade is moved orthogonally to the stone, by a hydraulic system that can work up to 200 kN of force, in order to cut them in multiple small pieces.

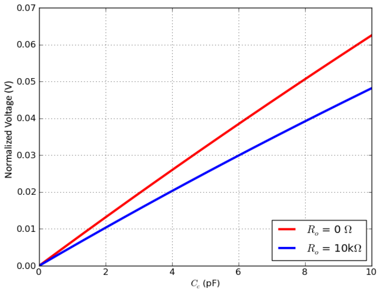


Figure 6. Normalized output voltage

Since 2006, the global European rule for machinery *2006/42/EC* [10] set a new approach to the design procedure of new safety-related systems in industrial machines. In particular, the new rule IEC EN 62061 [14], issued in 2005, replaces the old EN954-1 [11] starting from December 2011. The new rule is the sector transposition of the general rule IEC 61508 [13] that takes into account all the aspects of functional safety issues in industrial processes with complex electrical and programmable system by defining the Safety Integrity Level (SIL). The SIL is a discrete number from 1 to 3 (a level 4 is defined in IEC 61508 but is not applicable to industrial machines) that links the evaluation of likelihood to injury consequences of a hazardous event. In other words, the SIL indicates the "goodness" and the reliability with which a system must perform its safety tasks.

In the absence of a safety-system, any dangerous event related to an industrial process, called *hazard*, can create serious harm to persons and environment. This concept is defined as *risk* [13] and the purpose of every safety systems is to either eliminate it or, at least, mitigate the consequences up to a globally acceptable level.

4.1. IEC EN 62061

Rule IEC 62061 describes the design procedure of safety related systems as an iterative process from functional requirement specification to hardware and software design of the safety function. First, designers have to define a Safety Related Control Function (SRCF) for each hazard of the machinery under control, defining in detail the functionality that has to be implemented to reduce the risk associated with each hazard. Then, the risk related to each hazard has to be evaluated in order to allocate a Safety Integrity Level (SIL) to each SRCF.

The SRCF function has to be designed (Hardware and Software) in a component, called Safety Related Control System (SRECS), in order to satisfy all the requirements of the SIL level, defined by the standards [13],[14]. These requirement are mainly defined in a qualitative way for aspects of the software and architecture system design, while in a statistical way for hardware design. Table 1 reports the latter case, defined in IEC 62061 and IEC 61508 as a function of the probability of dangerous failure per hour for each SIL level.

SIL	Probability of dangerous Failure per Hour
1	$\geq 10^{-6}$ *to* $< 10^{-5}$
2	$\geq 10^{-7}$ *to* $< 10^{-6}$
3	$\geq 10^{-8}$ *to* $< 10^{-7}$

Table 1. Safety Integrity Level values for SRCF

As reported in Annex B of IEC 62061 [14], each SRECS can be decomposed in three main functional blocks (Input, Logic Solving and Output) that can be shared or reused in different SRECS of the system. Each functional block will be chosen or designed to meet the safety integrity requirements of the SIL level associated to the SRECS function. The IEC 62061 standard reports various general architectures that can be used during development of a SRECS to compose individual functional blocks, both in redundant or single mode.

4.2. SIL Evaluation

In our case study the main goal is to design a safety barrier for stone cutting machines. The evaluation of SIL associated with the process was conducted in a semi-quantitative way based on statistical data and design parameters of the machine. The analysis also has taken into account various functional aspects such as speed of moving parts, the tool size, the hydraulic inertia of the machine, etc. In this work, due to lack of space, we must limit our presentation to the results of the classification without providing details on values adopted.

After evaluation, we found only a single safety-related hazard represented by the movement of the blade. The consequences of a hypothetical harm associated with this hazard can be the fracture of one or more limbs, or amputation of limbs or fingers. The classification of the type of hazard was carried out according to rules UNI EN ISO 12100 [16] and IEC 62061. Table 2 reports all parameters used for classification. The result is then applied in Table 3 to determine the SIL level through the SIL assignment matrix derived from rule IEC 62061 [14].

Our case study is classified as a SIL 2 and subsequent phases of the design should take this value into account to ensure compliance with the reliability and safety requirements of the SIL 2 level.

Hazard	*Se*	*Fr*	*Pr*	*Av*	***Cl***
Moving elements	3	5	3	1	**12**

Se: Severity (Irreversible: broken limb(s), losing a finger(s))
Fr: Frequency of occurrence($>$ 1h to $\leq$ 1 day)
Pr: Probability of exposure (Possible)
Av: Avoiding harm (Probable)
Cl: Harm probability class (Cl = Fr + Pr + Av)

Table 2. Hazard classification (*Cl*).

Severity (*Se*)	Class (*Cl*) 3-4	5-7	8-10	**11-13**	14-15
4	SIL 2	SIL 2	SIL 3	SIL 3	SIL 3
3		(OM)	SIL 1	**SIL 2**	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Table 3. Risk evaluation matrix [14]

5. Safety system design

During the early phases of the project, designers must chose a base architecture of the system that can be followed during the later stages. As shown in Figure 7, our system can be conceptually split into four main functional blocks:

1. *Signal generation* is performed on each conductive glove through small battery-powered PCB. The signal shape is a single sinusoidal tone with different frequencies for each glove in order to discriminate, for safety purpose, left and right hand of the operator (i.e. 60 kHz for right and 95 kHz for left).

2. *Signal acquisition and conditioning*. This part consist of a hardware PCB board, without any logical elements, designed for collecting the signal from each sensing element. In this section, each input signal is filtered by analog circuits in order to reduce the noise from 50 $\div$ 60 Hz and their harmonics. The safety integrity level of blocks 1 and 2 are mainly assured by statistical evaluation of failure probability of electronic circuits in terms of MTTF hours.

3. *The FPGA block*, itself subdivided into three main steps, represents the logical signal analysis part. We choose to design this block in a single FPGA chip in order to reduce development and certification costs due to lack of use of operating systems and RAM elements otherwise required in a CPU based development.

4. *Stop System*. This part is already designed and installed on the cutting machine. It consists of various hydraulic valves and solenoids that can stop the blade quickly. The stop command is given by a boolean signal produced by the previous stage when a hazardous event is detected.

The following sections will focus on the design phase of the FPGA safety logical blocks.

5.1. Architectural constraint

As previously introduced, rule IEC 62061 defines four types of architectures which can be chosen depending on the requirements of the application. An important point that must be considered in the architectural choice concerns the reliability of the components that will be used. It can be noted that the reliability requirements of the SIL

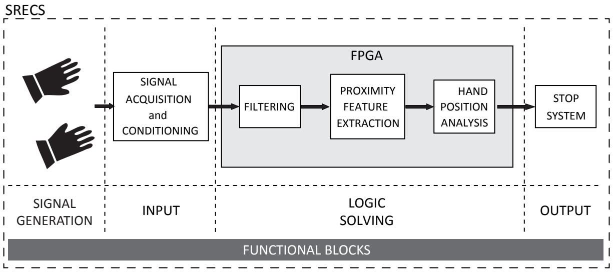


Figure 7. Functional blocks of the system

must be satisfied by the *entire* SRECS. It follows that in a non-redundant architecture the reliability requirements of the individual blocks will have to be stronger than in a redundant case. On the other hand, redundant architectures can tolerate one or more faults and can be implemented using components with lower reliability, but require greater work for design and certification.

Another important aspect at this level concerns the failure modes of components and the system. Each SRECS, block or component can have failures that are classified by the rules [13] [14] in two groups:

- *Dangerous failures* can lead the system to a dangerous state, or inhibit the operation of the safety-related function;
- *Safe failures* are minor faults that are not able to compromise the safety functionality; or they are dangerous failures that can be detected by a diagnostic unit and for which some safety actions may be taken to put the system in a safe state.

Failure classification allows various metrics, such as the Safe Failure Fraction (SFF) and the Diagnostic Converage (DC), to be defined for qualifying reliability and safety of components. The circuit architecture also implicitly defines the fault tolerance of the SRECS.

The SFF, as reported in IEC 62061, is a statistical parameter defined as:

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D} \quad (3)$$

where λ_S is the total probability of safe failure, λ_D is the total probability of dangerous failure and λ_{DD} is the total probability of dangerous failure that can be detected by the diagnostic unit.

The DC instead is a statistical parameter defined as:

$$DC = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} \quad (4)$$

where λ_{DD} is defined as previously and λ_{DU} is the total probability of dangerous failure that cannot be detected by any diagnostic units. A conservative hypothesis that all system failures are dangerous ($\lambda_S = 0$) is often considered [19]. Under this assumption it can be proved from 3 and 4 that:

$$SFF = DC \quad (5)$$

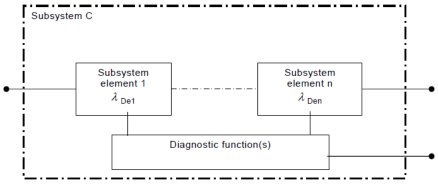


Figure 8. Architecture type "C" [14]

In our case study we chose a type "C" architecture [14], shown in Figure 8, that is a zero fault tolerance system with a diagnostic function. In this case, any undetected fault of the system can lead to a dangerous failure of the SRECS. Our choice of a non-redundant approach is mainly explained to achieve a cost reduction of the system, at the expense of an increased design complexity to meet the SIL 2 requirements, because it is necessary to design a diagnostic system with high performance. As can be noticed from Table 4, for a SIL 2 application with a zero tolerance architecture the system must be designed with a SFF from 90% to < 99%. Those parameters will be kept as a reference and verified during the later stages of design.

Safe Failure Fraction (SFF)	Hardware fault tolerance		
	0	1	2
<60%	N.A.	SIL 1	SIL 2
60% ≤ SFF < 90%	SIL 1	SIL 2	SIL 3
90% ≤ SFF < 99%	SIL 2	SIL 3	SIL 3
≥ 99%	SIL 3	SIL 3	SIL 3

Table 4. Architectural constraints on subsystems [14]

5.2. FPGA design

Our approach to analyzing the signals collected by the capacitive elements uses an FPGA. The main objective of this signal analysis is to evaluate the geometrical distance of the hands from the cutting edge and to verify if the machine is working in safety conditions or acting to prevent harm. This operation can be performed by the following three steps, schematically represented in Figure 9. All FPGA modules are written in VHDL and synthesized on a commercial Xilinx FPGA:

1. *Signal Filtering*. In this section, signals collected by the sensing elements are filtered through two 50-tap FIR filters whose frequency response is shown in Figure 10. Each acquired signal presents, before filtering, the sum of components due to both the left and the right glove. After the filtering stage, we reconstruct two different signals for each sensing bars, whose signal levels are proportional to the distance of each glove from the blade, with a minimum rejection of about 45 dB between the two signals;

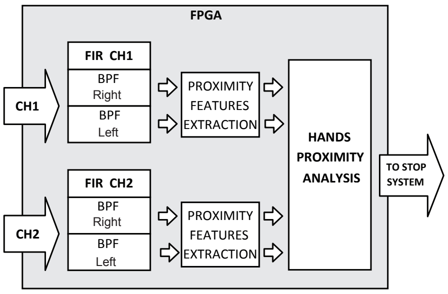


Figure 9. FPGA modules

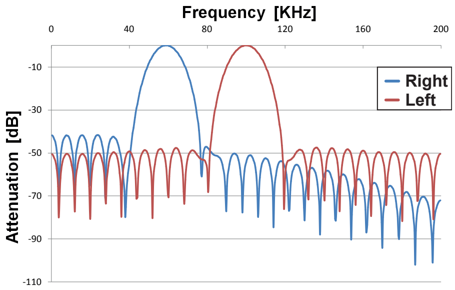


Figure 10. Transfer function of FIR filters

2. *Features Extraction*. This operation associates an estimated distance (glove to blade) to the signal level of each glove through a look-up table (LUT) which was set during calibration phases. Any future mechanical changes to the machine or sensing elements in geometry of the system can be managed by a re-calibration of those values;

3. *Hand Position Analysis*. In this block, all data collected by the feature extraction modules are evaluated with a threshold of 148 mm. Every signal lower than this value indicates a potentially hazardous situation. In this case, a stop command is sent to the machine that will lead to a safe state. Threshold value was calculated by evaluating various parameters of the system (i.e. blade speed and mechanical inertia, positions worst-case of hands and fingers near the blade, electronics and hydraulics response time, etc.) ensuring to meet the safety requirements.

All these blocks are designed to meet both the quantitative and the qualitative safety integrity requirements of SIL 2. The former are handled by statistical analysis of reliability during the design phases of the PCB, the latter instead are mainly handled during FPGA module design. In particular, to ensure compliance with the SFF required by our application, we had to adopt the following design techniques:

- *Stop signal*. A basic solution widely adopted to reduce the number of safety-related failure is to use "negative logic" for stop and command signals. With this simple technique, the stop (or similar) command is automatically activated in case of failures such as the lack of power supply of the control embedded system, and is especially effective when electromechanical components, e.g., relays or oleo dynamics valves, are used. These techniques can increase the SFF of the SRECS because they keep the system in a safe state;

- *Glove signal check*. Another safety-critical point of the system comes from the active gloves. The level of the signal emitted by the on-board logic is directly linked to the distance glove-blade calculated by the FPGA logic. Any failure that can occur on the active gloves, like no signal output due to low battery level, can cause a serious failure in the overall system. For this reason, in our approach we designed a simple input signal check based on a threshold of minimum signal acquired by the system that guarantees the correct glove operation. In addition, on-glove diagnostic and periodical check procedures are required to meet all safety requirements;

- *Diagnostics*. The whole safety system is designed with diagnostic functions to meet the SFF requirements. Output re-reading, analog signal control points and on-line data checks are developed on the FPGA for diagnostic purpose so that any detected fault brings the machine in a safe state.

With these design solutions we achieve a theoretical compliance with the reliability and diagnostics requirements for SIL 2 level. Any future changes or improvements to this diagnostic part will be assessed during the safety certification phases. To improve the safety of the FPGA modules we also used a model checking tool (NuSMV) in order to prove in advance the consistency of state machines and other logical elements synthesized on FPGA.

5.3. SFF and SIL verification

After preliminary hardware design is completed, a verification process is required to check if all safety integrity parameters comply with the SIL level. Moreover, at this stage more data are available both on hardware components reliability and failure modes. The first step of this analysis consists in failure modes classification into a safe and dangerous class, in order to estimate the SFF of the system. In our approach, we chose to perform the analysis according to IEC 61508-6 [13] that is based on Failure Modes and Effects Analysis (FMEA) both for the hardware components used in each subsystem and for the diagnostic circuits.

We obtained a good match to the safety integrity requirements for SIL 2 level, although very close to the limits. In this work, due to the limited space and intellectual property of the PCB design, we present only the results showed in Table 5. It must be noted that our results are

Module	λ_D $\left[h^{-1}\right]$	Safe Failure [%]	Dangerous Failure [%]	λ_{DD} $\left[h^{-1}\right]$	λ_{DU} $\left[h^{-1}\right]$
DC/DC Converter	$5,90 \cdot 10^{-7}$	$97,2$	$2,8$	$5,73 \cdot 10^{-7}$	$1,65 \cdot 10^{-8}$
Input Amplifier	$1,15 \cdot 10^{-8}$	$98,4$	$1,6$	$1,13 \cdot 10^{-8}$	$1,84 \cdot 10^{-10}$
FPGA Board	$1,10 \cdot 10^{-8}$	$96,2$	$3,8$	$1,08 \cdot 10^{-8}$	$4,18 \cdot 10^{-10}$
Output Stage	$8,03 \cdot 10^{-8}$	49	51	$3,93 \cdot 10^{-8}$	$4,10 \cdot 10^{-8}$
Safety Relay	$4,96 \cdot 10^{-8}$	82	18	$4,07 \cdot 10^{-8}$	$8,93 \cdot 10^{-9}$
Active Glove	$2,00 \cdot 10^{-7}$	94	6	$1,88 \cdot 10^{-7}$	$1,20 \cdot 10^{-8}$
TOTAL	$9,43 \cdot 10^{-7}$			$8,64 \cdot 10^{-7}$	$7,90 \cdot 10^{-7}$
SFF [%]	$91,62$				

Table 5. FMEA analysis and SFF calculation of preliminary hardware design

conservative because, as previously introduced, we considered all failures as dangerous ($\lambda_S = 0$) in order to reduce computation complexity. The major limitation that we found in our work is the lack of statistical data on the reliability of some parts of the system, such as conductive gloves, that have been made ad hoc for the system. In these cases we used a conservative estimation that has penalized the overall reliability of the system but allows us to have a good reliability margin for certification.

6. Conclusions

In this paper we have discussed a real industrial application based on a novel safety barrier for stone cutting machinery. First, we presented the capacitive coupling method used in the application. Simulation and measurements show good results for estimating the distance between gloves and blade.

In the second part we mainly focused our attention to design problems of the safety embedded system from hazard analysis to preliminary hardware design. Our case study was a SIL 2 level and we design the safety related system in a non redundant architecture based on an FPGA approach. We prove that the preliminary hardware and software design meets the safety requirements of the SIL level. The main limitation of our safety verification arises from the lack of reliability and failure modes of the components, mitigated by a conservative analysis.

Our project will be shortly submitted to the certification procedure by an independent certification authority in order to verify its compliance to rule IEC 62061 and IEC 61508.

References

[1] W. Anderson. Risk analysis methodology applied to industrial machine development. *Industry Applications, IEEE Transactions on*, 41(1):180 – 187, jan.-feb. 2005.

[2] L. Baxter. *Capacitive Sensors:Design and Applications*. Wiley-IEEE Press, 1997.

[3] A. Bozzoli, M. Frizzi, L. Cristoforetti, and A. Vaccari. Plant for working products. Patent WO 2011/144997 A2, Nov 2011.

[4] M. Catelani, L. Ciani, V. Luongo, and R. Singuaroli. Evaluation of the safe failure fraction for an electromechanical complex system: remarks about the standard IEC61508. In *Instrumentation and Measurement Technology Conference (I2MTC), 2010 IEEE*, pages 949 –953, may 2010.

[5] S. Dalpez, R. Passerone, D. Cancila, and F. Terrier. An industrial case study using an MBE approach: From architecture to safety analysis. In *Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW), 2010 13th IEEE International Symposium on*, pages 116 –122, may 2010.

[6] R. Girardey, M. Hu andbner, and J. Becker. Safety aware place and route for on-chip redundancy in safety critical applications. In *VLSI (ISVLSI), 2010 IEEE Computer Society Annual Symposium on*, pages 74 –79, july 2010.

[7] G. Griessnig, R. Mader, C. Steger, and R. Weiss. A CPLD-based safety concept for industrial applications. In *Industrial Electronics (ISIE), 2010 IEEE International Symposium on*, pages 3027 –3032, july 2010.

[8] J. D. Jackson. *Classical Electrodynamics, third edition*. 1998.

[9] L. P. L.D. Landau, E.M. Lifshitz. *Electrodynamics of Continuous Media, Second Edition*. Elsevier Butterworth-Heinemann, 2004.

[10] 2006/42/EC. Directive on machinery, european community. 17 May 2006.

[11] EN 954-1:1996. Safety-related parts of control systems.

[12] EN ISO 13849-1. Safety-related parts of control systems general principle of design, 2007.

[13] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related system, parts 1-7, 2005.

[14] IEC 62061:2005-01. Safety of machinery functional safety of safety related electrical, electronic and programmable electronic control systems.

[15] UNI EN 999:2000. The positioning of protective equipment in respect of approach speeds of parts of the human body.

[16] UNI EN ISO 12100. Safety of machinery. general principles for design, 2010.

[17] B. Pottier, L. Rasolofondraibe, and D. Nuzillard. A novel capacitive safety device for target localization and identification. *Sensors Journal, IEEE*, 8(10):1640 –1647, oct. 2008.

[18] F. Salewski and A. Taylor. Systematic considerations for the application of FPGAs in industrial applications. In *Industrial Electronics, 2008. ISIE 2008. IEEE International Symposium on*, pages 2009 –2015, 30 2008-july 2 2008.

[19] E. Soressi. Introduction in safety rules EN954-1, EN13849 and EN62061. In *System Safety 2010, 5th IET International Conference on*, pages 1 –6, oct. 2010.