Design of safety systems with Programmable Logic

A. Dr. Jorge Marcos – B. Dr. Jacobo Álvarez – C. Dr. Santiago Fernández

A, B: E.T.S.I.Industriales.University of Vigo.
Lagoas-Marcosende s/n.
36280 - Vigo. SPAIN.
Fax: +34-986-811987.
A: Phone: +34-986-812095.
E-mail: acevedo@uvigo.es
B: Phone: +34-986-812090.
E-mail: jalvarez@uvigo.es

C: ATI Research Silicon Valley
2085 Bowers Avenue
Santa Clara, CA 95051, USA
Phone: (408) 572 6327
Fax: (408) 572 6301
E-mail: sfdez@ati.com

Abstract
In many industrial processes, an incorrect operation can lead to irreparable damage to people, equipment, or the environment. In order to reduce risks, the electronic control systems used in this kind of processes must comply with international standard safety requirements.
The solutions proposed in this article are based on the implementation of safety redundant control systems in Programmable Logic Devices (PLDs and FPGAs), now a widely used and low cost technology. The proposed methodology for safe controllers design is based on the combination of dynamic logic and redundant circuits with voting capabilities. This methodology leads to low cost PLD based control, diagnosis, and supervision systems that allow to achieve the different safety levels established in international safety standards.
The use of Programmable Logic Devices (PLDs) instead of high-end Programmable Logic Controllers (PLCs) adds flexibility to the design of safety-related control systems and reduces costs, while maintaining high reliability and a good degree of failure detection.

1.- INTRODUCTION

Advances in technology over the past decades have enabled the rapid evolution of industrial processes that support an increasingly large portion of the modern society way of life. From medical facilities, to flight control systems, we are surrounded by advances involving the use of equipment that, in the event of a failure, can cause serious damage to people, installations, or the environment. Safety has emerged then as a primary requirement for the design and operation of new equipment.

The concern of modern society about safety has motivated, on one hand, the creation of health and human safety-organizations and institutions, like the Occupational Safety and Health Administration (OSHA). It has also impulsed the important efforts that some international standardization organizations, like the International Electrical Commission (IEC) and the American National Standards Institute (ANSI), are dedicating to elaborate new specific standards that regulate the safety of industrial applications [1]-[8] [11]-[12]. The main goal of this standards is to clarify

the requirements for different applications and systems, in order to elevate their safety to an acceptable level.

There is a large number of industrial processes where an erroneous operation can lead to important damage to their environment, and economical losses. That is why these processes, and the machines involved, must be designed to operate safely. However, the high automation and management levels required nowadays make necessary to use electronic systems for the process control and supervision tasks. These electronic systems must assume the responsibility of halting the process or taking it to a safe state to guarantee the installation operational safety in the presence of a possible risky situation. This need has originated, several years ago, the interest in developing both hardware and software, related to electronic systems safety, and specially to microprocessor-based control systems, which has lead to numerous research works [24][26][27]. The following fields have higher safety requirements for the design and operation of electronic systems:

- Emergency systems: fire detection, human detection in hazardous areas, etc.
- Signalling systems: traffic signals, railway signals and control, airport signals, etc.
- Train control systems: forward and backward control, door locking systems, etc.
- Automotive applications: anti-lock brake systems, etc.
- Aeronautical applications: aircraft control systems, etc.
- Nuclear power stations.
- Chemical and petroleum plants.
- Electric power stations and electric distributing plants.
- Mining.
- Oil and gas pipelines.
- Submarine drilling rigs.
- Food factories.
- Waterworks.
- People transportation.
- Tunnel ventilation.
- Environmental plants: garbage incineration plants, etc.

According to different international standards [1][2], electronic systems capable of leading an installation into a safe state, in the presence of a dangerous event, are named Safety Instrumented Systems (SIS, see fig. 1) and, following those standards, these systems must comply with several requirements to reach the safety level needed for each particular application.

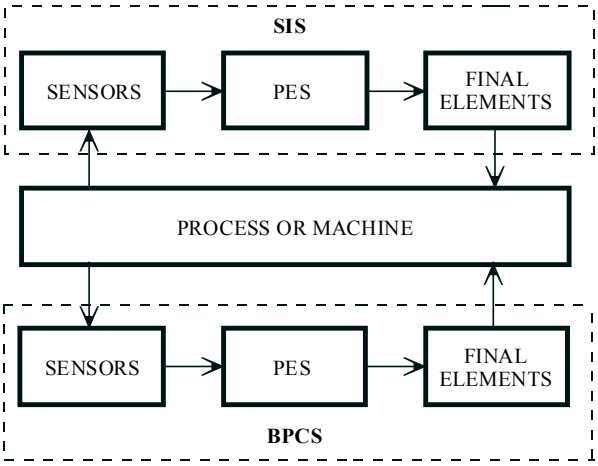

Fig. 1. The BPCS and the SIS as independent systems.

Usually, these safety systems are distinguished by the use of highly reliable components in redundant configurations. This allows them to guarantee that the installation reaches the safe state when the value of any of the process variables goes outside of the permitted range. Though these safety systems are designated as Safety Instrumented Systems (SIS), as mentioned before, it is usual to find other denominations like Emergency Shutdown (ESD), Emergency Shutdown Systems (ESS), Safety Shutdown Systems (SSD) or Safety Interlock Systems (also SIS). There is a lot of such systems in the market, specially for machine-tools (presses, etc.)

Nowadays, one of the most employed type of control system for process and machine automation is the Programmable Logic Controller (PLC), which constitutes together with its sensors, its final actuators, and its interface circuits, the so-called Basic Process Control System (BPCS, see fig. 1).

In safety applications the inclusion of a SIS is needed to implement the safety function. Ideally, the SIS should be an independent system, different from the BPCS [25]. However, many PLC manufacturers only offer systems that include both, control and safety functions, in their product lines [9][10]. Usually, such PLCs are high-end systems, with a great number of

inputs and outputs, that lead to expensive installations because of their redundant architectures. These PLCs are adequate to control big and complex plants or processes, but they result an expensive solution for simple processes, with a few number of safety-critical variables.

Bearing in mind that, for a given installation, not all the variables are critical from the safety point of view, and that the critical variables are usually binary, that is, they only have two states, All or Nothing (On and Off), in this article we propose several solutions based on the implementation of the electronic control system for the SIS on Programmable Logic Devices (PLDs or FPGAs) [14]-[18]. These programmable devices constitute a widely-tested, low-cost technology that allows to implement, in an easy way, electronic control systems both for independent BPCS and SIS and offers great possibilities due to the new PLD design and development tools, provided by the manufacturers at low cost.

The use of Programmable Logic Devices instead of Programmable Logic Controllers (PLCs), adds flexibility to the design of safety-related control systems and reduces costs, while maintaining high reliability and a good degree of failure detection.

It is also possible, for some applications, to combine control and safety functions within the system. Actually, it is possible to implement a low cost PLC-based BPCS to carry out the main control function, and an independent Programmable Logic based SIS, to carry out the safety function. This versatility is achieved through the combination of diagnosis and voting circuits.

This article is structured in the following sections. Section 1 is this introduction. Section 2 introduces several concepts related to SIS, and presents SIS architectures. In section 3 we discuss the basic proposed strategy to implement SIS on programmable logic. We also present specific techniques to address the addition of safety logic to inputs, outputs, and control logic (CPU). Finally, Section 4 concludes the paper.

2.- SAFETY INSTRUMENTED SYSTEMS

The need for Safety Instrumented Systems (SIS) in the industry has impulsed the development of standards that define their scope and requirements. The most recent standard, establishes that Safety Instrumented Systems are composed of the following components:

- Sensors
- Logic solver
- Power supply
- Field wiring
- Output control elements
- Communication interface

3. - DESIGN OF SAFETY INSTRUMENTED SYSTEMS BASED ON PROGRAMMABLE LOGIC DEVICES

In this section, we describe a methodology to increase the safety and the reliability of any industrial electronic control system, by adding a SIS, implemented using Programmable Logic Devices (PLDs and FPGAs). The main goal of this methodology is to develop simple, cost-effective, hardware implementations that can be used in industrial installations to achieve a target level of safety, as described by international standards.

Fig. 2 shows the block diagram of a typical programmable electronic control system. It has input and output interfaces to communicate with its environment, and a main control unit. To increase the safety and availability of the control system, these three blocks may need modifications. In an industrial environment, there are several design considerations to take into account.:

- In most industrial control systems, only a few input and output variables can be considered critical, from the safety point of view.
- Critical variables are usually binary, that is, all-nothing (On-Off), or they can be reduced to binary ones.
- The manufacturers and technicians experience shows that 90% of the failures in a control system are caused by malfunction at the input or output interface, while only 10% is due to a CPU or power source failure.
- The CPU or logic solver is usually based on a Programmable Logic Controller or an Industrial Computer Unit.

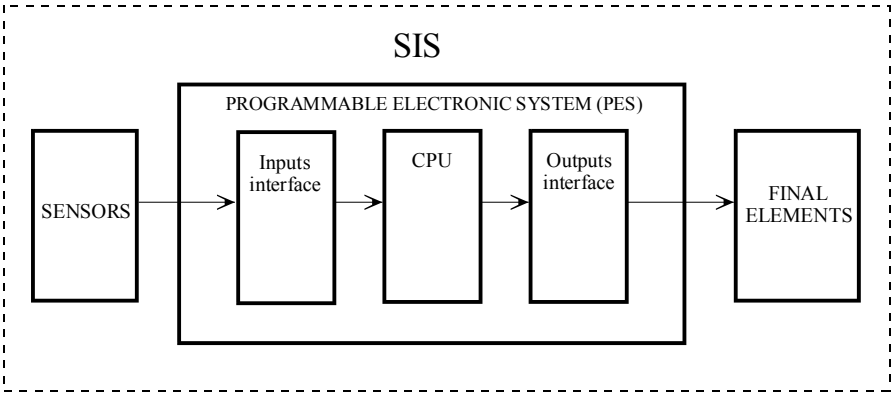

Fig. 2. Block diagram of a Programmable Electronic Control System.

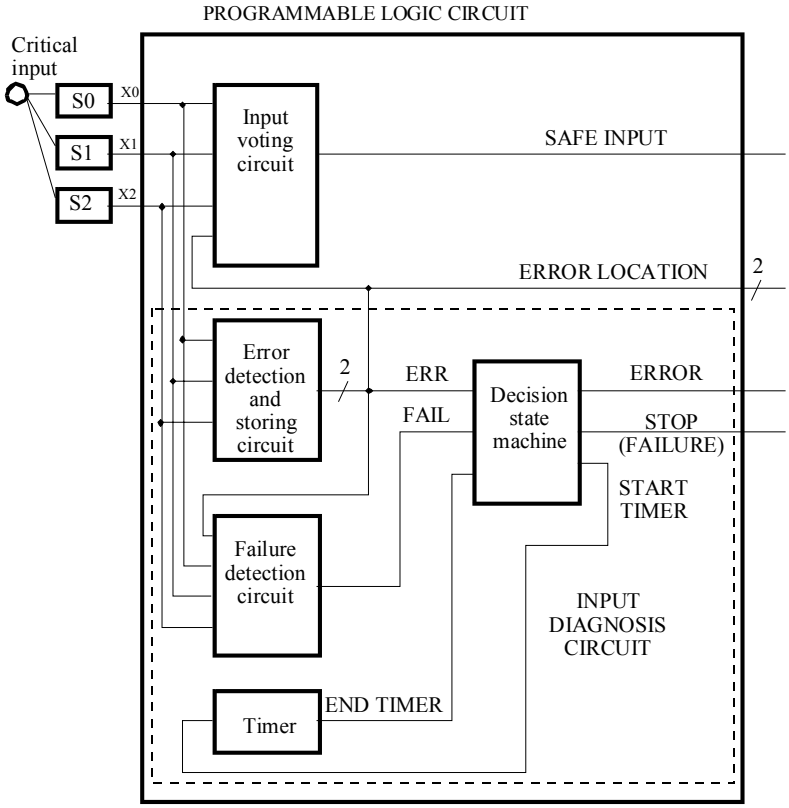

Fig. 3. Block diagram of the Safe Input Cell.

The previously described design considerations lead to a Programmable Logic based SIS design methodology, composed of the following steps:

1) Increase the safety at the input stage, focusing only on critical binary inputs.

2) Increase the safety at the output stage, focusing only on critical binary outputs.

3) If the safety increase achieved with the previous two steps is not enough, then increase the safety of the CPU stage.

3.1- Inputs safety

To achieve a high safety level at the input stage (fig. 2), each critical input is tripled and connected to a Safe Input Cell [21]–[23] (fig. 3).

3.2- Outputs safety

The digital output circuits of the logic solvers (specially PLCs) can be of various types (relay, transistor, TRIAC). PNP or NPN transistor outputs are very common. The most usual output failure occurs at the output transistor (short-circuit or open circuit) or its associated circuit. To solve this problem, redundancy of the outputs must be combined with other techniques as described below.

Our proposed solution to increase the plant safety at the output stage (fig. 2), is based on dynamic outputs [13], [28], in which the activation of an output (level "1") leads to the output oscillation at a given frequency, instead of a fixed value. A Safe Output Cell (fig. 4), used in every critical output, generates the dynamic signal described before.

3.3- CPU safety

As mentioned before, if the safety level reached with the previous two steps (inputs and outputs) is not enough, then it is necessary to increase the safety of the CPU stage. The first two steps have led to a high increment in the installation safety, but if a SIS is required, they have to be combined with a safe CPU (logic solver) to achieve the required SIL.

In fig. 5 it is shown the block diagram of a PLC based BPCS and a PLD based SIS, that work in parallel [19]-[23]. The SIS only deals with critical inputs and outputs. In fig. 5, the architecture of the SIS is 1oo1, according to the IEC61508 standard.

In fig. 6 it is shown the block diagram of a PLD based SIS with a 2oo3D architecture, where the CPU is tripled. This guarantees that if one CPU fails, the safety function is not affected. In this case, the voting circuit is implemented through the outputs. For each critical output, each one of the three CPUs (CPU_A, CPU_B y CPU_C) generates its own output (R_A, R_B y R_C). These three outputs are combined in a relay-based output voting circuit, so the critical output is active only if two of the three outputs are active. When CPU redundancy is combined with input redundancy (through Safe Input Cells) and dynamic outputs, as shown in fig. 6, it is possible to detect the failure of any of the three relays, when multiple contact relays are used, in a similar way as it is described in the previous section for the output interface. Besides CPU redundancy, it has been added a PLD based CPU diagnosis circuit that detects if the outputs of the three CPUs coincide.

The three CPUs of fig. 6 are based on Programmable Logic. This has the following advantages:

- Very low cost, compared to other solutions.
- Application adaptability, due to the versatility and programmability of Programmable Logic Devices (PLDs and FPGAs).
- Integration, since the Safe Input Cells, the SIS CPU, and the Safe Output Cells, can be included in each one of the three programmable circuits needed for the tripled architecture, as shown in fig. 6.

4.- CONCLUSIONS

The solutions proposed in this article allow to design low cost, Programmable Logic based, Safety Instrumented Systems (SIS) with the required safety levels, as well as better maintainability characteristics. These solutions can be adapted to the different specifications of any industrial application. The proposed PLD-based SIS design method is specially suitable to control processes with a reduced number of critical inputs and outputs.

Any failure, either in the inputs, the CPU or the outputs, can be detected by the proposed diagnosis circuits, which can be implemented using Programmable Logic at a very low cost. These solutions only have the drawback of the knowledge needed to design with Programmable Logic, but this difficulty can be reduced to a minimum with the new high level, language-based, software tools and the adequate libraries, that may include the Safe Input Cells, the Safe Output Cells and the CPU diagnosis circuit.

The application of some of these solutions, like the Safe Input Cells, allows to identify the location of the errors (discrepancies) while the control system keeps working properly, so the corrective maintenance tasks are simplified, and the maintainability and the plant availability are increased.

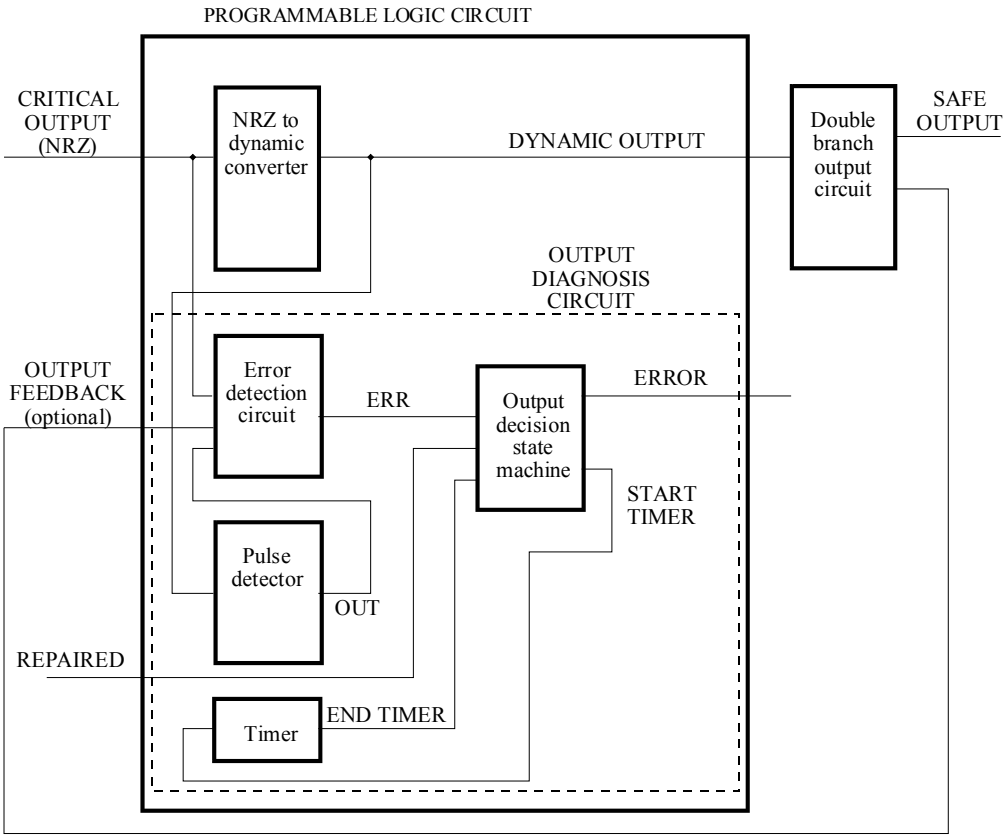

Fig. 4. Block diagram of the Safe Output Cell and the external output circuitry.

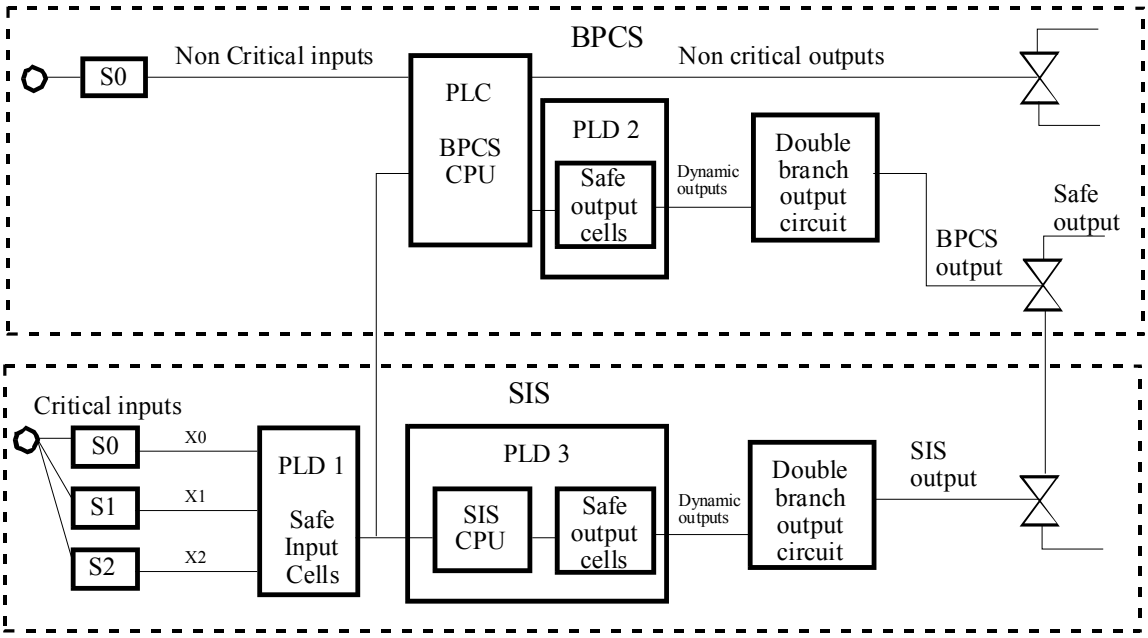

Fig. 5. Block diagram of a PLC based BPCS and a PLD based SIS working in parallel. The architecture of the SIS is 1oo1.

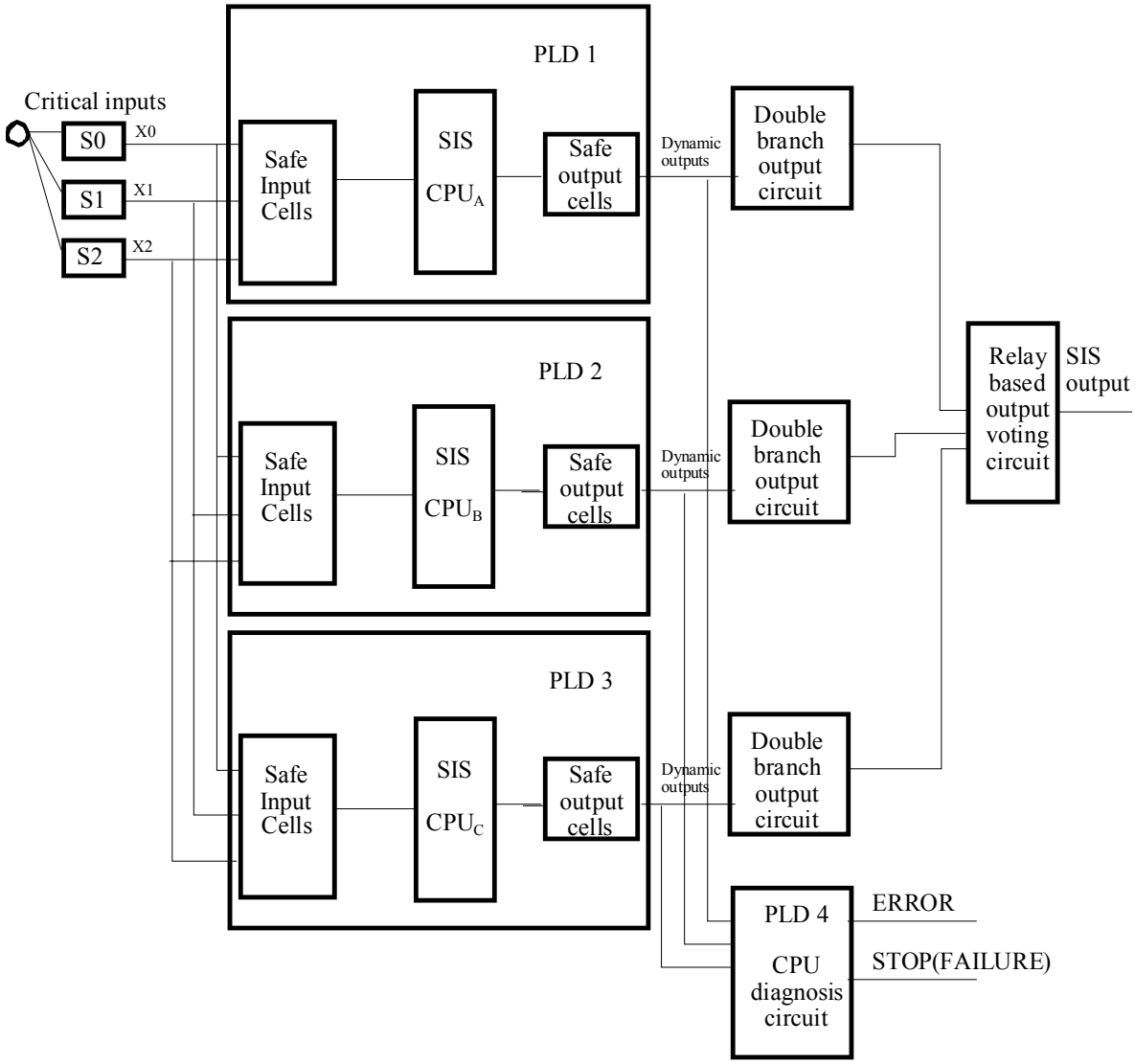

Fig. 6. Block diagram of a SIS with 2oo3D architecture, implemented with Programmable Logic Devices (PLDs).

The methods given in this article are modular, both, in the sense of being applicable to the inputs and the outputs considered critical, and in the sense of being complementary to conventional control systems like Programmable Logic Controllers (PLCs), including low cost ones.

There are now Programmable Logic Devices in the market with up to 200,000 equivalent logic gates and 173 I/O pins for less than 20 $ per device (less price in greater quantities) [18]. This kind of devices are specially suited for the application of the proposed methodology to simple processes or plants.

Moreover, the easy development of standard IP libraries for the different blocks involved in the design of safety systems (like the safe input cell, the safe CPU cell and the safe output cell) can simplify and shorten the design process to a great extent.

The only lack of these PLD based SIS, as described here, is the absence of a communications interface that allows them to be integrated in an industrial net. Nevertheless, there are many standard communication interface cores available in the market, that can be easily integrated in a Programmable Logic Device.

5. - REFERENCES

[1] ANSI/ISA S84.01-1996. Application of Safety Instrumented Systems for the Process Industries.

[2] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems. CEI-IEC, 1998.

[3] EN 954-1. Safety of machinery. Safety-related parts of control systems. Part 1: General principles for design.

[4] DIN V VDE 0801, Principles for computers in safety-related systems.

[5] DIN IEC 65A/255/CDV, Functional safety of electrical/electronic programmable electronic safety-related systems.

[6] DIN V 19250, Control technology; fundamental safety aspects to be considered for measurement and control equipment.

[7] EN 50126, Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

[8] IEC 61511-1, Functional safety - Safety Instrumented Systems for the process industry sector.

[9] Siemens. Safety Integrated: Application Manual, Safety Technology. Siemens AG. Berlin, 1999. http://www.siemens.com

[10] Pilz. PSS, Compact Safety Systems. http://www.pilz.com

[11] ISA-dTR 84.02-1996. Electrical (E) / Electronics(E) / Programmable Electronic Systems (PES) for use in Safety Applications-Safety Integrity Evaluation Techniques.

[12] IEEE.Standard for Software Verification & Validation. New York, 1986.

[13] J.P.Vautrin, M.Collier. Application of dynamic and self-checking functions in the improvement of the safety of logic systems. Electronique Industrielle Nº 60, pp. 89-98, Nov. 1983.

[14] Chan, Pak K., Mourad, Samiha. Digital design using Field Programmable Gate Arrays. Prentice Hall, New Jersey, 1994.

[15] Jenkins, Jesse H. Designing with FPGAs and CPLDs. Prentice Hall, New Jersey, 1994.

[16] Oldfield, J.V., Dorf, R.C. Field Programmable Gate Arrays: Reconfigurable logic for rapid prototyping and Implementation of Digital Systems. John Wiley & Sons, 1995.

[17] Pellerin, D., Holley, M. Practical design using programmable logic. Prentice Hall, London, 1991.

[18] Xilinx web site, http://www.xilinx.com, Xilinx.

[19] J. Marcos, E. Mandado and C.M. Peñalver Implementation of fail-safe control systems using PLCs. IEEE/IAS International conference on industrial automation and control, pp. 395-400. Hyderabad (India). January 5-7, 1995.

[20] J. Marcos, V. Vázquez, E. Mandado, C.M. Peñalver and J.J. Rodríguez. Fail-safe output modules for electronic control systems. ISIE '97/IEEE International Symposium on Industrial Electronics, Vol. II, pp.493-496. Guimares-Portugal, July 7-11, 1997.

[21] J. Marcos, A. Gómez, E. Mandado, C. M. Peñalver and A. Lago. Fail-safe and test for electronic control system using PLCs. 1st IEEE Latin-American Test Workshop, pp.140-145. Río de Janeiro-Brasil, March 13-15, 2000.

[22] J. Marcos, J. Álvarez, E. Mandado and A. Nogueiras. Failure safe PLD based control system 2st IEEE Latin-American Test Workshop, pp.174-179. Cancún-México, February 11-14, 2001.

[23] J. Marcos and J. Álvarez. Easy maintainable failure-safe electronic control systems. ESReDA 22nd Seminar on maintenance management & optimization. EUROPEAN SAFETY, RELIABILITY & DATA ASSOCIATION, pp.1-7. Madrid-Spain, May 27-28, 2002.

[24] J.P Gérardin, C. Vigneron, P. Charpentier. Eléments de réponse au probléme de la securité des dispositifs industriels à microprocesseur. Cahiers de notes documentaires, Nº 135, pp. 289-294, 1989.

[25] D. Dei-Svaldi, J.P. Vautrin. Les automates programmables. Nouvelles technologies, nouveaux risques, principes de sécurité à appliquer. Cahiers de notes documentaires, Nº 117, pp. 467-473, 1984.

[26] P.Bremer, A. Halldén, J. Jacobson. Microcomputer-Based Protective Functions in Industrial Production Systems. Assessment Method. Swedish National Testing and Research Institute,1993.

[27] S. Bologna. G. Dahll, G. Picciolo, R. Taylor. Safety Applications of Computer Based Systems for the Process Industry. ENEA, Italy, 1997.

[28] J. Marcos, A. Gómez. Oscillating output improves system security. EDN, February 2003.