Safety first: safety system plants for rolling mills

Safety first: this is the rule that should guide the design of every industrial plant. AIC, with a fully integrated view of safety automation, has developed an architecture already implemented in a number of steel plants. This involves a way to determine the residual risk by the designer. The first and preferred method for reducing the risk must be through the mechanical design of the machine, with measures to increase the intrinsic safety of the equipment through use of safety circuits.

Authors: Riccardo Albertini, Fabio Tamburini and Stefano Arondi
Automazioni Industriali Capitanio

AIC is a global system integrator that designs, manufactures and markets automation systems for many different industries, although its main business for more than 30 years has been steel industry process automation and control. AIC's international customers include Tata Corus, Sandvik Materials Technology, Gerdau Ameristeel, Riva Acciaio and Lucchini–Severstal Group.

Over the years we have moved from pure electronics to programmable electronics, and developments in technology now enable us also to use the software for safety circuits. The new standard UNI EN ISO 13849-1 requires management and implemention of the rules and design criteria of electrical circuits to achieve the required performance level (PL_R).

The key to this is the PL_R index, which is derived on the basis of this mechanical component and the relationships it has with the process and maintenance operators. The PL_R is, therefore, used to prescribe the degree of reliability of the emergency system; reliability that, for obvious reasons, can never be equal to 100%. PL_R is, therefore, the result of risk assessment according to Annex A of the Directive, which defines a pyramid of risk on the basis of three factors (incorporating the concepts of EN 954-1– see *Figure 1*).

The method presented shows a way to determine the residual risk by the designer. The first and preferred method for reducing the risk must be through the mechanical design of the machine, with measures to increase the intrinsic safety of the equipment. From the point of view of the systems analyst, the rule indicates three discriminants to determine the PL_R:

- S: This estimate covers the possible injury to operators
- F: Combination of frequency of dangerous situation and exposure time
- P: Possibility of avoiding the danger

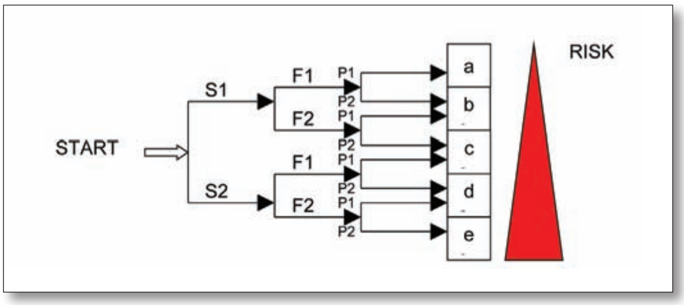

Fig 1 **Determination of risk**

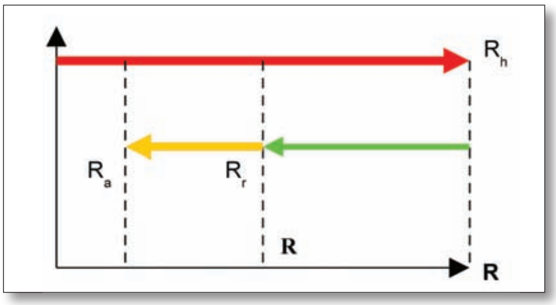

Fig 2 **Risk reduction measures with mechanical (green) and with the safety circuit (yellow)**

The process of reducing the risk is represented in *Figure 2*, in which the residual risk is highlighted.

where:

- For a specific situation of danger, R_h is the risk before protective measures are applied
- R_r is the risk reduction measures carried out with mechanical protection
- R_a is the residual risk mitigated by the safety circuit

Where the mechanical measures are not sufficient to mitigate the risk to operators, it is necessary to implement ▷

Fig 3 **Emergency system flow diagram**

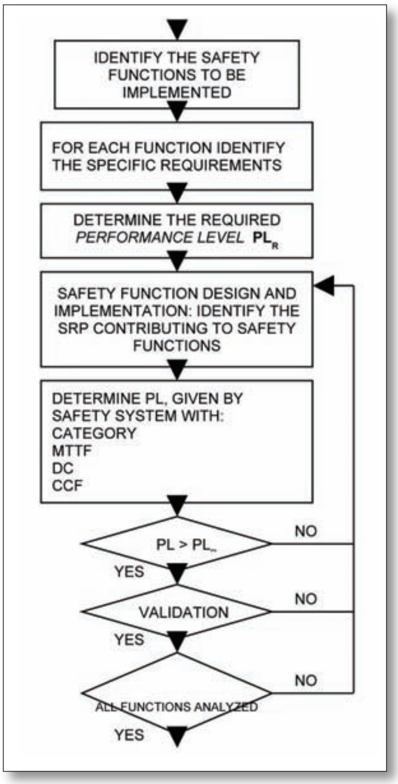

Fig 4 **CPU and distributed I/O signals**

Fig 5 **Safety network interfaces**

Fig 6 **Typical safety box**

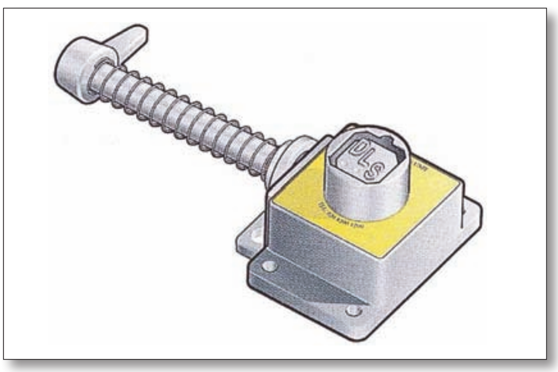

Fig 7 **Single key access lock**

an iterative process that, through safety related parts of a control system, mitigates these risks by introducing a circuit to reduce the possible damage following a situation of danger. The flow diagram given in *Figure 3* represents this process.

The joint efforts of the customer and the manufacturer of mechanical and electrical components lead both individual applications and the whole plant to meet the most stringent safety criteria.

This type of intervention, made when implementing new systems, is also applicable to existing plants, taking advantage of the modular safety PLCs that are not restricted to the amount of I/O handled. An example of such an application is the revamping of the safety system of IRO SpA, Italy.

AIC SAFETY SYSTEM

AIC, with a fully integrated view of safety automation, has developed an architecture already implemented in some steel plants, including at Corus UK, Feralpi Siderurgica and Ferriera Valsabbia, Brescia, Italy.

This new design introduces some special features:

- The safety system is not hardware cabled but realised in programmable logic. The safety PLC provides a range of certified software blocks that implement all the safety functions normally done using hardware.

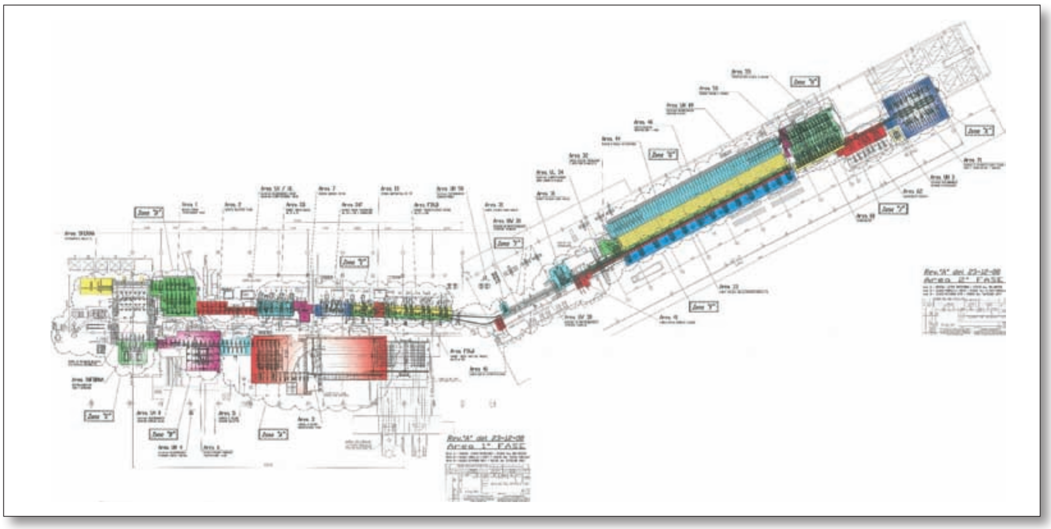

Fig 8 **Hardware architecture of safety system for a complete plant**

- The software architecture for implementing the logic allows splitting of the emergency system into simple macro areas in order to implement a safety system that can reduce plant downtime during the intervention.
- The extreme flexibility of the programming system allows a capillary distribution of the emergency functions that allows the safe shutdown of individual machines.

Examples of safety PLCs used by AIC are Pilz, Siemens and Rockwell. These top-of-the-range products are made with multi-channel architecture whereby the information is processed and compared in parallel by different processors. If the result is the same, then the instructions are transferred to the actuators.

The CPU is equipped with safety network interfaces in order to create the necessary channel of communication for diagnostics of the safety system between automation and safety PLCs (see *Figure 5*). The system supports the major fieldbuses and data exchange via ethernet. The safety bus can handle more than 8,000 points of I/O and the network can have an extension of up to 7,000m.

The possibility of distributing and de-localising safety commands and functions by means of safety BUS networks allows remoting I/O to the single zone to be controlled.

The safety box (see *Figure 6*) can handle an emergency in a single macro area. This, together with the traditional mushroom push button, means that other functions such as a 'gate open' request and 'safe area' lamp, can be implemented, The yellow colour identifies the role played by this device.

The safety system can be activated not only by mushroom push buttons, but also by devices such as safety switches that offer the ability to control access to unsafe areas of the plant (see *Figure 7*). Interlocks can also be implemented, with electric locks to prevent access to danger zones.

Fig 9 **Example of plant protected by AIC safety system**

Figure 8 illustrates hardware architecture of a safety system for a complete plant with the different zones identified.

Figure 9 illustrates an example of plant protected by an AIC safety system.

CONCLUDING REMARKS

Safety has to be the prime driver for equipment designers and plant operators. This involves scientifically assessing the risks and consequences of failure, designing out failure modes and introducing safety circuits so that the residual risks are minimised. AIC has a fully integrated view of safety automation, and has an architecture already implemented in some steel plants. MS

Riccardo Albertini is Senior Project Manager, Fabio Tamburini is Hardware Engineer and Stefano Arondi is Senior Software Engineer, all with AIC Srl, Odolo, Italy.

CONTACT: roberto.migliorati@aicnet.it