SEPTEMBER 2018

Safety and reliability of control systems of machinery

In the risk assessment required by the Machinery Directive 2006/42/EC, the analysis of the safety and reliability of control systems of the machine is primary as different hazardous conditions could arise from a wrong design of the control system or from a level of system reliability not congruent to the risks present on the machine. In this regard, the Machinery Directive 2006/42/EC defines specific design criteria for the control systems and collects them within the related essential safety requirements.

MTM Consulting s.r.l. is able to follow the manufacturers of machines in the drafting of the technical file and, in particular, the risk assessment, providing the most appropriate indications for the design of the control system of the machine so that it is safe and reliable according to the risks actually present on the machine. This study is carried out with the aid and methodologies provided by the reference technical standard: UNI EN ISO 13849-1: 2016.

Safety and reliability of control systems

The Machinery Directive 2006/42/CE contains, in Annex I, the essential health and safety requirements that the machine must meet before being put on the market and / or put into service by the manufacturer. The risk assessment required by the Machinery Directive must be functional to demonstrate the fulfillment of all the safety requirements applicable to the machine. In fact, the design choices made by the manufacturer must be the direct result of the risk assessment so that the operators, who will have to deal with the machine at all life stages, are exposed only to those residual risks that emerged from the assessment itself.

The risk assessment must also cover the design choices related to the equipment (electric, pneumatic and / or hydraulic) of the machine's control system, in particular as regards those parts of the safety-related parts of control systems.

In particular, the essential health and safety requirement 1.2.1 of Annex I - "Safety and reliability of control systems" - defines the requirements that the machine's control system must meet in order to avoid the occurrence of hazardous situations related to a wrong design or to a potential failure of the same system. For example, some evaluations that need to be made:

- The control systems must not be influenced externally by the work environment in which the machine operates: if the machine is designed for outdoor use, the control systems must be designed in compliance with this environment.
- The control systems must withstand the foreseeable stresses: for example, continuous operation on a control device (a button, for example) must not cause it to break quickly, with potential additional hazards for the operator.
- If the management and control system of the machine is damaged or faulty, there must never be any situations of hazard for the operator: the operating logic of the machine must remain

separate from the safety logic, always ensuring that this last is able to monitor the correct operation of the first. In fact, the machine must not have unexpected start-ups, no stops when required (in particular if emergency), changes to the process parameters that lead to unexpected hazardous situations, unexpected behavior, etc.

- Predictable human errors, related to human-machine interaction, must not lead to the creation of hazardous situations: for example, the operator intervention on a management software must not entail hazardous conditions for the operator except by voluntary intervention by the operator himself so that he is effectively aware of what he is about to enable.

The requirements set out in point 1.2.1 of Annex I apply to all parts of the control system which, in the event of a breakdown, may involve hazards due to unsolicited or unforeseen machine behavior. The parts of the control system most involved are the parts of the control system linked to the safety functions (start, stop, emergency stop, etc.). Failure of these safety features would result in a failure of the corresponding safety function and, consequently, a potentially dangerous situation for the operator.

UNI EN ISO 13849-1: 2016 standard

All the components of the control system are subject to faults and / or breakages, therefore it is unthinkable to imagine designing a control system that will never fail. It is reasonable, however, to select the safety-related parts of the control system so as to create a control system that is sufficiently safe and reliable compared to the result that emerged from the risk assessment. The design choices (both as components adopted and as architecture) of the safety-related parts of the control system must be such as to guarantee a level of reliability (Perfomance Level) appropriate to the result of the risk assessment and therefore to the level of risk actually present on the machine.

The UNI EN ISO 13849-1: 2016 standard presents the probabilistic approach now enunciated.

The contents of the standard can be enclosed in these four sequential steps:

- Exclusion or reduction of the probability of failures by adopting reliable components and proven safety principles.
- Use of standardized components with verification of the safety functions by the control system at regular intervals.
- Redundancy of the elements of the control system so as not to lose the safety function in case of failure or breakdown.
- Automatic control for continuous detection of faults and failures.

These concepts are normally applied in combination with each other.

The risk assessment carried out according to the methodology established by the standard thus allows to identify a level of reliability of the control system that is adequate to the risks present on the machine and to choose the correct components to create a control system with the required level of reliability.