VALIDATION IN ACCORDANCE WITH ISO 13849-2

mrlnews

Excerpt from MRL News / Edition 2019.01, page 6 & 7

An important standard which gets too little attention.

In mechanical engineering, it is often necessary to secure machines by incorporating safety-related control functions. ISO 13849 part 1 is a harmonized standard for the construction and design of "safety-related parts of control systems". By contrast, part 2 of this standard, which defines the approach for targeted validation of safety functions, still gets too little attention. In fact, validation is the first evidence of suitability relative to the actual application purpose. Therefore, validation in accordance with ISO 13849 is very important to the overall risk assessment process.

ISO 13849 part 2 defines the validation process for the safety functions incorporated into the machine. The term SRP/CS (safety-related parts of a control system) is also used in this context. The validation process must conclusively demonstrate that the design of the SRP/CS complies with the safety requirements of ISO 13849-1.

The validation process consists of various steps and makes a fundamental distinction between verification and validation. Verification consists of analysis and tests on SRP/CS and parts thereof in order to ascertain whether the results of a design process meet the specifications for this phase, i.e. whether the switching layout corresponds to the design, for example. The key question is whether the Performance Level (PL) achieved at least meets (or exceeds) the Performance Level required (PLr). If this is not the case, the design can be adjusted. Evidence of suitability for the actual application purpose is known as validation. One of the elements at this phase is an error simulation, which aims to demonstrate that the system enters a safe condition in accordance with the specifications and that there are no new hazards as a result.

Independent testers

Verification and validation can be carried out based on analysis or based on a combination of analysis and testing. As a general rule, the whole validation process should be carried out by independent persons, i.e. people that were not directly involved in the design and construction of the SRP/CS. However, testing by a third party is not strictly necessary. The IFA Institute[1] provides recommendations on the principle that the degree of independence should be commensurate with the risk, i.e. the PLr.

The validation process set out in ISO 13849-2 also stipulates that a validation plan should be drawn up. This plan describes the requirements and objectives of all activities to be carried out and the means for validating the defined safety functions, categories and Performance Level, including, for example, specifications for safety functions, a document list, references to applicable testing standards, etc. In order to prepare for the validation process, extensive documentation also needs to be collated, including circuit diagrams, error lists, user information, etc.

The categories classify the SRP/CS with respect to their resistance to faults and their behavior in the event of a fault. They are also the starting point for determining failure probabilities and PL.

Another step in the process is the validation of measures to avoid systematic failures, for example, by means of fault analysis, known as Failure Mode and Effects Analysis (FMEA). In addition, the performance and interference immunity of the SRP/CS to environmental influences such as mechanical strain or temperature fluctuations must be validated.

For the validation of safety-related software, on the one hand, it checks whether the requirements for the safety-related software specification for functional behavior and the performance criteria (e.g. time-related specifications) have been correctly implemented. On the other hand, tests are carried out in order to check how errors are detected and controlled by the software. At the end of the analysis, the correct estimation of the PL is checked, and a validation carried out on the question as to whether a combination of safety-related parts achieves the Performance Level defined in the design process. A validation report is then drawn up.

Benefits of validation in the design process

If the risk reduction is based on using a safety-oriented controller, then achieving a Performance Level is necessary but not sufficient. Only documented validation is sufficient evidence that the defined objective has been achieved to an acceptable extent.

Early consideration of validation in the design process can improve economic viability, as potential errors are discovered at an early stage and there is no further necessity for a subsequent redesign of the SRP/CS.

The validation does not have to be carried out by third parties, but it can be helpful to involve external experts who have an objective view of the situation.

[1)] IFA – Institute for Occupational Safety and Health of the German Social Accident Insurance

SCHMERSAL USA
15 Skyline Drive, Hawthorne NY 10532
Tel: 914-347-4775 Fax: 914-347-1567
salesusa@schmersal.com
www.schmersalusa.com

SCHMERSAL CANADA
29 Centennial Road, Unit 1, Orangeville ON L9W 1R1
Tel: 519-307-7540 Fax: 519-307-7543
salescanada@schmersal.com
www.schmersalcanada.ca