

## EN ISO 13849-1:2008 Validation Service

### Independent validation of your Machinery safety systems

**“Validation should be carried out by persons who are independent of the design of the safety-related part(s).”**

EN ISO 13849-2:2008 Clause 3.1

#### EN ISO 13849

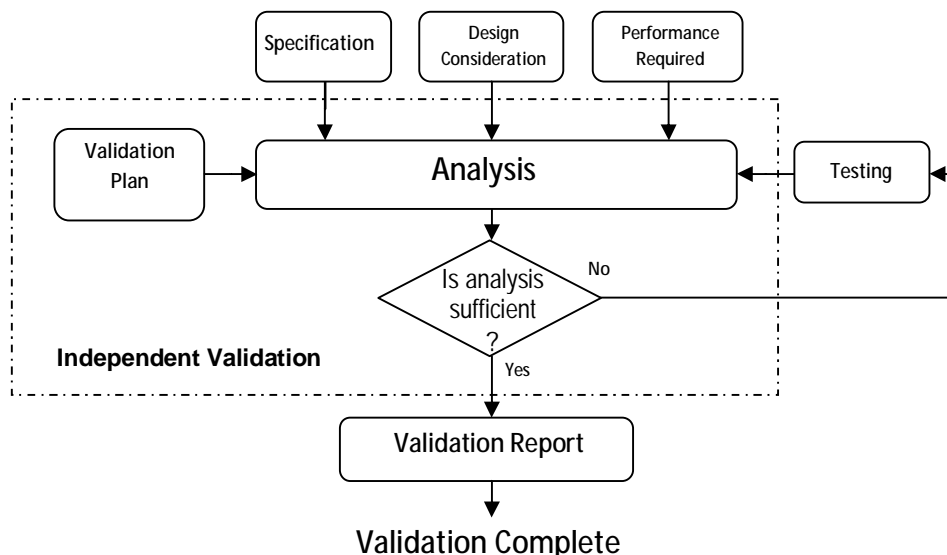
The new European Harmonised Standard, EN ISO 13849-1:2008 “*Safety of machinery — Safety-related parts of control systems*” replaces EN 954-1. In comparison with an EN 954-1 assessment, EN ISO 13849-1 is complicated and time-consuming. It requires a risk assessment process to establish a system performance level, followed by a number of calculations involving mean time to dangerous failure, diagnostic coverage, architecture and common-cause failures to validate that the performance level has been achieved.

Health & Safety Compliance Engineering, having been actively involved in the development of this and other standards for machinery safety, offers independent validation and analysis of your safety control system designs for machinery.

#### Validation process

The purpose of the validation process is to confirm the conformity of the design of the safety related parts of the control system within the overall safety requirements of the machinery and demonstrate that each safety-related part meets the requirements of EN ISO 13849-1.

EN ISO 13849 requires that validation should be carried out by persons who are independent of the design of the safety-related systems:-



This validation process should be started as early as possible and in parallel with the design, so that problems can be corrected early whilst they are still relatively easy to correct.

## Validation plan

The validation and analysis carried out by Health & Safety Compliance Engineering is based on a validation plan which includes:

- Examination of the specification requirements;
- The operational and environmental conditions;
- The Performance Levels required of the safety-related systems;
- The architecture used in the design of the safety-related systems;
- The safety principles applied in the design of the safety-related systems;
- The components used in the safety-related systems;
- The fault assumptions and fault exclusions to be considered;
- The methods of analysis;
- The tests to be applied.

## Information required for validation

The information required for validation will vary with the technology used, the design rationale of the system and the contribution of the safety-related parts of control systems to the reduction of the risk. Documents containing sufficient information will be required for the validation process and these could include:

- Description, specification and requirements of the machinery and safety systems;
- The expected performance of the safety functions;
- Block diagrams with functional description of the blocks;
- The drawings and control schematics, e.g. Electrical, pneumatic, hydraulic and mechanical
- Functional description of the control schematics;
- Component specifications, including manufactures claim limits;
- Time sequence diagrams relevant to safety;
- Description of the relevant characteristics of components previously validated;
- Analysis of all relevant faults including the justification of any excluded faults;
- Analysis of the influence of processed materials;

Where software is relevant to the safety function(s), the software documentation must include:

- Evidence including approvals and certification proving compliance of the hardware and software to the requirements of EN61508;
- Evidence that the software is capable of achieving the required safety performance, including manufactures claim limits;
- Functional programme diagrams with description of firmware blocks and their interconnection;
- A specification which is clear and unambiguous and states how the safety performance of the software has been achieved;
- Details of any tests carried out to prove that the required safety performance is achieved.

## Analysis

Analysis of the design of the safety related control system is based on the information provided including the specification, the design considerations related to the machine and control systems and the level of performance required of the system.

Comprehensive analysis, in accordance with the Validation Plan, enables us to model the structure of your safety related control system based upon the components used and the designated architectures, thereby permitting calculation of the reliability values in detail, including relevant parameters such as the overall component reliability ( $MTTF_d$ ), the average test quality ( $DC_{avg}$ ) of components and blocks and probable common-cause failures (CCF), to determine Performance Level achieved (PL). This is in turn compared to the Performance Level required ( $PL_r$ ) for the level of risk posed by the machine.

The results of the validation are fully recorded in a comprehensive report and, if found necessary, practical recommendations are made to help achieve and/or maintain conformity and system integrity.

