Introduction

The structure of safety standards in the field of machinery is as follows.

a) Type-A standards (basis standards) give basic concepts, principles for design and general aspects that can be applied to machinery.

b) Type-B standards (generic safety standards) deal with one or more safety aspect(s), or one or more type(s) of safeguards that can be used across a wide range of machinery:
   - type-B1 standards on particular safety aspects (e.g. safety distances, surface temperature, noise);
   - type-B2 standards on safeguards (e.g. two-hands controls, interlocking devices, pressure sensitive devices, guards).

c) Type-C standards (machinery safety standards) deal with detailed safety requirements for a particular machine or group of machines.

This part of ISO 13849 is a type-B-1 standard as stated in ISO 12100-1.

When provisions of a type-C standard are different from those which are stated in type-A or type-B standards, the provisions of the type-C standard take precedence over the provisions of the other standards for machines that have been designed and built according to the provisions of the type-C standard.

This part of ISO 13849 is intended to give guidance to those involved in the design and assessment of control systems, and to Technical Committees preparing Type-B2 or Type-C standards which are presumed to comply with the Essential Safety Requirements of Annex I of the Council Directive 98/37/EC, The Machinery Directive. It does not give specific guidance for compliance with other EC directives.

As part of the overall risk reduction strategy at a machine, a designer will often choose to achieve some measure of risk reduction through the application of safeguards employing one or more safety functions.

Parts of machinery control systems that are assigned to provide safety functions are called safety-related parts of control systems (SRP/CS) and these can consist of hardware and software and can either be separate from the machine control system or an integral part of it. In addition to providing safety functions, SRP/CS can also provide operational functions (e.g. two-handed controls as a means of process initiation).

The ability of safety-related parts of control systems to perform a safety function under foreseeable conditions is allocated one of five levels, called performance levels (PL). These performance levels are defined in terms of probability of dangerous failure per hour (see Table 3).

The probability of dangerous failure of the safety function depends on several factors, including hardware and software structure, the extent of fault detection mechanisms [diagnostic coverage (DC)], reliability of components [mean time to dangerous failure (MTTF_d), common cause failure (CCF)], design process, operating stress, environmental conditions and operation procedures.

In order to assist the designer and help facilitate the assessment of achieved PL, this document employs a methodology based on the categorization of structures according to specific design criteria and specified behaviours under fault conditions. These categories are allocated one of five levels, termed Categories B, 1, 2, 3 and 4.
The performance levels and categories can be applied to safety-related parts of control systems, such as

— protective devices (e.g. two-hand control devices, interlocking devices), electro-sensitive protective devices (e.g. photoelectric barriers), pressure sensitive devices,

— control units (e.g. a logic unit for control functions, data processing, monitoring, etc.), and

— power control elements (e.g. relays, valves, etc),

as well as to control systems carrying out safety functions at all kinds of machinery — from simple (e.g. small kitchen machines, or automatic doors and gates) to manufacturing installations (e.g. packaging machines, printing machines, presses).

This part of ISO 13849 is intended to provide a clear basis upon which the design and performance of any application of the SRP/CS (and the machine) can be assessed, for example, by a third party, in-house or by an independent test house.

**Information on the recommended application of IEC 62061 and this part of ISO 13849**

IEC 62061 and this part of ISO 13849 specify requirements for the design and implementation of safety-related control systems of machinery. The use of either of these International Standards, in accordance with their scopes, can be presumed to fulfil the relevant essential safety requirements. The following table summarizes the scopes of IEC 62061 and this part of ISO 13849.

<table>
<thead>
<tr>
<th>Technology implementing the safety-related control function(s)</th>
<th>ISO 13849-1</th>
<th>IEC 62061</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Non-electrical, e.g. hydraulics</td>
<td>X</td>
<td>Not covered</td>
</tr>
<tr>
<td>B Electromechanical, e.g. relays, and/or non complex electronics</td>
<td>Restricted to designated architectures (^{a}) and up to PL = e</td>
<td>All architectures and up to SIL 3</td>
</tr>
<tr>
<td>C Complex electronics, e.g. programmable</td>
<td>Restricted to designated architectures (^{a}) and up to PL = d</td>
<td>All architectures and up to SIL 3</td>
</tr>
<tr>
<td>D A combined with B</td>
<td>Restricted to designated architectures (^{a}) and up to PL = e</td>
<td>(X^{c})</td>
</tr>
<tr>
<td>E C combined with B</td>
<td>Restricted to designated architectures (see Note 1) and up to PL = d</td>
<td>All architectures and up to SIL 3</td>
</tr>
<tr>
<td>F C combined with A, or C combined with A and B</td>
<td>(X^{b})</td>
<td>(X^{c})</td>
</tr>
</tbody>
</table>

\(X\) indicates that this item is dealt with by the International Standard shown in the column heading.

\(^{a}\) Designated architectures are defined in 6.2 in order to give a simplified approach for quantification of performance level.

\(^{b}\) For complex electronics: use designated architectures according to this part of ISO 13849 up to PL = d or any architecture according to IEC 62061.

\(^{c}\) For non-electrical technology, use parts in accordance with this part of ISO 13849 as subsystems.