IEC 62061

(First edition – 2005)

Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

CORRIGENDUM 2

Page 39

3.2 Terms and definitions

Delete the Note to definition 3.2.41: safe failure.

Page 83

Replace Table 5 with the following:

Table 5 – Architectural constraints on subsystems: maximum SIL that can be claimed for a SRCF using this subsystem

Safe failure fraction	Hardware fault tolerance (see Note 1)		
	0	1	2
< 60 %	Not allowed (for exceptions see Note 3)	SIL1	SIL2
60 % – < 90 %	SIL1	SIL2	SIL3
90 % – < 99 %	SIL2	SIL3	SIL3 (see Note 2)
≥ 99 %	SIL3	SIL3 (see Note 2)	SIL3 (see Note 2)

NOTE 1 A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety-related control function.

NOTE 2 A SIL 4 claim limit is not considered in this standard. For SIL 4 see IEC 61508-1.

NOTE 3 See 6.7.6.4 or for subsystems where fault exclusions have been applied to faults that could lead to a dangerous failure, see 6.7.7.

Page 83

Clause 6, add a new subclause 6.7.6.4 as follows:

6.7.6.4 Electromechanical subsystems, which have a safe failure fraction of less than 60 % and zero hardware fault tolerance, that use well-tried components (see Note) in accordance with ISO 13849-1:2006 Category 1 PLC shall be considered to achieve a SILCL of SIL1.

NOTE A well-tried component for a safety-related application is a component which has been:
a) widely used in the past with successful results in similar applications, or
b) made and verified using principles which demonstrate its suitability and reliability for safety-related applications.

Renumber subclause 6.7.6.4 as:

6.7.6.5 Where a subsystem is designed according to ISO 13849-1:1999 and validated according to ISO 13849-2:2003, the following relationship in the context of architectural constraints alone can be applied in accordance with Table 6. It is assumed that a subsystem with a particular category complying with ISO 13849-1:1999 has the associated hardware fault tolerance and safe failure fraction as indicated in Table 6.

NOTE To achieve a required SIL, it is also necessary to fulfil the requirements according to probability of dangerous failure and systematic safety integrity.