IEC/TR 62061-1

1 - Scope

This Technical Report is intended to explain the application of IEC 62061 and ISO 13849-1 (2) in the design of safety-related control systems for machinery.

(2) This Technical Report considers ISO 13849-1:2006 rather than ISO 13849-1:1999, which has been withdrawn.

2 - General

2.1 -

Both IEC 62061 and ISO 13849-1 specify requirements for the design and implementation of safety-related control systems of machinery (3). The methods developed in both of these standards are different but, when correctly applied, can achieve a comparable level of risk reduction.

3) These standards have been adopted by the European standardization bodies CEN and CENELEC as ISO 13849-1 and EN 62061, respectively, where they are published with the status of transposed harmonized standards under the Machinery Directive (98/37/EC and 2006/42/EC). Under the conditions of their publication, the correct use of either of these standards is presumed to conform to the relevant essential safety requirements of the Machinery Directive (98/37/EC and 2006/42/EC).

2.2 -

These standards classify safety-related control systems that implement safety functions into levels that are defined in terms of their probability of dangerous failure per hour. ISO 13849-1 has five Performance Levels (PLs), a, b, c, d and e, while IEC 62061 has three safety integrity levels (SILs), 1, 2 and 3.

2.3 -

Product standards (type-C) committees specify the safety requirements for safety-related control systems and it is recommended that these committees classify the levels of confidence required for them in terms of PLs and SILs.

2.4 -

Machinery designers may choose to use either IEC 62061 or ISO 13849-1 depending on the specific features of the application.

2.5 -

The selection and use of either standard is likely to be determined by, for example:

- previous knowledge and experience in the design of machinery safety-related control systems based upon the concept of categories described in ISO 13849-1:1999 can mean that the use of ISO 13849-1:2006 is more appropriate;

- safety-related control systems based upon media other than electrical can mean that the use of ISO 13849-1 is more appropriate;

- customer requirements to demonstrate the safety integrity of a machine safety-related control system in terms of a SIL can mean that the use of IEC 62061 is more appropriate;

- safety-related control systems of machinery used in, for example, the process industries, where other safety-related systems (such as safety instrumented systems in accordance with IEC 61511) are characterized in terms of SILs, can mean that the use of IEC 62061 is more appropriate.

3 - Comparison of standards

3.1 -

A comparison of the technical requirements in ISO 13849-1 and IEC 62061 has been carried out in respect of the following aspects:

- terminology;
- risk estimation and performance allocation;
- safety requirements specification;
- systematic integrity requirements;
- diagnostic functions;
- software safety requirements.

3.2 -

Additionally, an evaluation of the use of the simplified mathematical formulae to determine the probability of dangerous failures (PFH_D) and $MTTF_d$ according to both standards has been carried out.

3.3 -

The conclusions from this work are the following.

- Safety-related control systems can be designed to achieve acceptable levels of functional safety using either of the two standards by integrating non-complex (4) SRECS (safetyrelated electrical control system) subsystems or SRP/CS (safety-related parts of a control system) designed in accordance with IEC 62061 and ISO 13849-1, respectively.

- Both standards can also be used to provide design solutions for complex SRECS and SRP/CS by integrating electrical/electronic/programmable electronic subsystems designed in accordance with IEC 61508.

- Both standards currently have value to users in the machinery sector and benefits will be gained from experience in their use. Feedback over a reasonable period on their practical application is essential to support any future initiatives to move towards a standard that merges the contents of both IEC 62061 and ISO 13849-1.

- Differences exist in detail and it is recognized that some concepts (e.g. functional safetymanagement) will need further work to establish equivalence between respective design methodologies and some technical requirements.

3.3 -

(4) Although there is no definition for the term "non-complex" SRECS or SRP/CS this should be considered equivalent to low complexity in the context of IEC 62061:2005, 3.2.7.

4 - Risk estimation and assignment of required performance

4.1 -

A comparison has been carried out on the use of the methods to assign a SIL and/or PL_r to a specific safety function. This has established that there is a good level of correspondence between the respective methods provided in Annex A of each standard.

4.2 -

It is important, regardless of which method is used, that attention be given to ensure that appropriate judgements are made on the risk parameters to determine the SIL and/or PL_r that is likely to apply to a specific safety function. These judgements can often best be made by bringing together a range of personnel (e.g. design, maintenance, operators) to ensure that the hazards that may be present at machinery are properly understood.

4.3 -

Further information on the process of risk estimation and the assignment of performance targets can be found in ISO 14121-1 and IEC 61508-5.

5 - Safety requirements specification

5.1 -

A first stage in the respective methodologies of both ISO 13849-1 and IEC 62061 requires that the safety function(s) to be implemented by the safety-related control system are specified.

5.2 -

An assessment should have been performed relevant to each safety function that is to be implemented by a control circuit by, for example, using ISO 13849-1, Annex A, or IEC 62061, Annex A. This should have determined what risk reduction needs to be provided by each particular safety function at a machine and, in turn, what level of confidence is required for the control circuit that performs this safety function.

5.3 -

The level of confidence specified as a PL and/or a SIL is relevant to a specific safety function.

5.4 -

The following shows the information that should be provided in relation to safety functions by a product (type-C) standard.

Safety function(s) to be implemented by a control circuit:

Name of safety function

Description of the function

Required level of performance according to ISO 13849-1: PL_r a to e

and/or

Required safety integrity according to IEC 62061: SIL 1 to 3

6 - Assignment of performance targets: PL versus SIL

Table 1 gives the relationship between PL and SIL based on the average probability of a dangerous failure per hour. However, both standards have requirements (e.g. systematic safety integrity) additional to these probabilistic targets that are also to be applied to a safetyrelated control system. The rigour of these requirements is related to the respective PL and SIL.

Table 1 - Relationship between PLs and SILs based on the average probability of dangerous failure per hour

7 - System design

7.1 - General requirements for system design using IEC 62061 and ISO 13849-1

The following aspects should be taken into account when designing a SRECS/SRP/CS.

- When applied within the limitations of their respective scopes either of the two standards can be used to design safety-related control systems with acceptable functional safety, as indicated by the achieved SIL or PL.

- Non-complex safety-related parts that are designed to the relevant PL in accordance with ISO 13849-1 can be integrated as subsystems into a safety-related electrical control system (SRECS) designed in accordance with IEC 62061. Any complex safety-related parts that are designed to the relevant PL in accordance with ISO 13849-1 can be integrated into safety-related parts of a control system (SRP/CS) designed in accordance with ISO 13849-1.

- Any non-complex subsystem that is designed in accordance with IEC 62061 to the relevant SIL can be integrated as a safety-related part into a combination of SRP/CS designed in accordance with ISO 13849-1.

- Any complex subsystem that is designed in accordance with IEC 61508 to the relevant SIL can be integrated as a safety-related part into a combination of SRP/CS designed in accordance with ISO 13849-1 or as subsystems into a SRECS designed in accordance with IEC 62061.

7.2 - Estimation of PFHD and MTTFd and the use of fault exclusions

7.2.1 - PFHD and MTTFd

7.2.1.1 -

The value of $MTTF_d$ in the context of ISO 13849-1 relates to a single channel SRP/CS without diagnostics and, only in this case, is the reciprocal of PFH_D in IEC 62061.

7.2.1.2 -

MTTFd is a parameter of a component(s) and/or single channel without any consideration being given to factors such as diagnostics and architecture, while PFHD is a parameter of a subsystem that takes into account the contribution of factors such as diagnostics and architecture depending on the design structure.

7.2.1.3 -

Annex K of ISO 13849-1 describes the relationship between MTTFd and the PFHD of an SRP/CS for different architectures classified in terms of category and diagnostic coverage (DC).

7.2.1.4 -

The estimation of PFHD for a series connected combination of SRP/CS in accordance with ISO 13849-1 can also be performed by adding PFHD values (e.g. derived from Annex K of ISO 13849 1) of each SRP/CS in a similar manner to that used with subsystems in IEC 62061.

7.2.2 - Use of fault exclusions

7.2.2.1 -

Both standards permit the use of fault exclusions, see 6.7.7 of IEC 62061 and 7.3 of ISO 13849-1. IEC 62061 does not permit the use of fault exclusions for a SRECS without hardware fault tolerance required to achieve SIL 3 without hardware fault tolerance.

7.2.2.2 -

It is important that where fault exclusions are used that they be properly justified and valid for the intended lifetime of an SRP/CS or SRECS.

7.2.2.3 -

In general, where PL e or SIL 3 is specified for a safety function to be implemented by an SRP/CS or SRECS, it is not normal to rely upon fault exclusions alone to achieve this level of performance. This is dependent upon the technology used and the intended operating environment. Therefore it is essential that the designer takes additional care in the use of fault exclusions as PL or SIL increases.

7.2.2.4 -

In general the use of fault exclusions is not applicable to the mechanical aspects of electromechanical position switches and manually operated switches (e.g. an emergency stop device) in order to achieve PL e or SIL 3 in the design of an SRP/CS or SRECS. Those fault exclusions that can be applied to specific mechanical fault conditions (e.g. wear/corrosion, fracture) are described in ISO 13849-2.

7.2.2.5 -

For example, a door interlocking system that has to achieve PL e or SIL 3 will need to incorporate a minimum fault tolerance of 1 (e.g. two conventional mechanical position switches) in order to achieve this level of performance since it is not normally justifiable to exclude faults such as broken switch actuators. However, it may be acceptable to exclude faults such as short circuit of wiring within a control panel designed in accordance with relevant standards.

7.2.2.6 -

Further information on the use of fault exclusions is to be provided in the forthcoming revision of ISO 13849-2 currently being developed by ISO/TC 199/WG 8.

7.3 - System design using subsystems or SRP/CS that conform to either IEC 62061 or ISO 13849-1

7.3.1 -

In all cases where subsystems or safety-related parts of control systems are designed to either ISO 13849-1 or IEC 62061, conformance to the system level standard can only be claimed if all the requirements of the system level standard (as relevant) are satisfied.

7.3.2 -

For the design of a subsystem or a part of safety-related parts of control systems either IEC 62061 or ISO 13849-1, respectively, shall be satisfied. It is permissible to satisfy more than one of these standards provided that those standards used are fully complied with.

7.3.3 -

It is not permissible to mix requirements of the standards when designing a subsystem or part of safety-related parts of control systems.

7.4 - System design using subsystems or SRP/CS that have been designed using other IEC or ISO standards

7.4.1 -

It may be possible to select subsystems, for example, electrosensitive protective equipment, that comply with relevant IEC or ISO product standards and either IEC 61508, IEC 62061 or ISO 13849-1 in their design. The vendor(s) of these types of subsystems should provide the necessary information to facilitate their integration into a safety-related control system in accordance with either IEC 62061 or ISO 13849-1.

7.4.2 -

Subsystems, for example, adjustable speed electrical power drive systems, that have been designed using product standards, such as IEC 61800-5-2, that implement the requirements of IEC 61508 can be used in safety-related control systems in accordance with IEC 62061 (see also 6.7.3 of IEC 62061) and ISO 13849-1.

7.4.3 -

In accordance with IEC 62061 other subsystems that have been designed using IEC, ISO or other standard(s) are subject to 6.7.3 of IEC 62061.

8 - Example

8.1 - General

The following example assumes that all the requirements of the standards have been satisfied.
The example is only intended to demonstrate specific aspects of the application of the standards.

8.2 - Simplified example of the design and validation of a safety-related control system implementing a specified safety-related control function

8.2.1 -

This simplified example is intended to demonstrate the use of subsystems or SRP/CS that comply with IEC 62061 and/or ISO 13849-1

8.2.1 -

in a SRECS/SRP/CS. The example is based on the implementation of a safety function described as a safety-related stop function associated with position monitoring of a moveable guard, with a specified safety integrity level of SIL 3/required performance level PL_r e as described in Figure 1.

8.2.2 -

The following information is relevant to the safety requirements specification for this example.

Safety function

- Safety-related stop function, initiated by a protective device: opening of the moveable guard initiates the safety function STO (safe torque off).

Functional description

- Trapping hazards are safeguarded by means of a moveable guard (protective grating). Opening of the interlocked guard is detected by two position switches, B1/B2, employing a break contact/make contact combination, and evaluation by a central safety module, K1. K1 actuates two contactors, Q1 and Q2, dropping out of which interrupts or prevents hazardous movements or states.

- The position switches are monitored for plausibility in K1 for the purpose of fault detection. Faults in Q1 and Q2 are detected by a start-up test in K1. A start command is successful only if Q1 and Q2 had previously dropped out. Start-up testing by opening and closing of the interlocked guard is not required.

- The safety function remains intact in the event of a component failure. Faults are detected during operation or at actuation (opening and closing) of the interlocked guard resulting in the dropping out of Q1 and Q2 and operational disabling.

- An accumulation of more than two faults in the period between two successive actuations can lead to loss of the safety function.

8.2.3 -

The following features should also be provided.

- Basic and well-tried safety principles are observe (e.g. the load current for the contactors Q1 and Q2 is de-rated by a factor of 50 %) and the requirements of Category B are met. Protective circuits (e.g. contact protection) are implemented.

- A stable arrangement of the protective devices is assured for actuation of the position switches.

- Switch B1 is a position switch with direct opening action in accordance with IEC 60947-5- 1:2003, Annex K.

- The supply conductors to position switches B1 and B2 are laid separately or with protection.

8.2.4 -

The following information is available from the manufacturers for each part within the design of SRP/CS.

- The safety module K1 is declared by the manufacturer (5) as satisfying the requirements for Category 4, PL e and SIL CL 3.

- The contactors Q1 and Q2 possess mechanically linked contact elements conforming with IEC 60947-5-1:2003, Annex L.

(5) This module is dealt with as a subsystem and, as such, the MTTFd of its individual channels need not be given (see 7.2.1.1).

8.2.5 -

The following observation can be made on the design of SRP/CS and/or SRECS.

- Category 4 can only be achieved where several mechanical position switches for different protective devices are not connected in a series arrangement (i.e. no cascading). This is necessary, as faults in the switches cannot otherwise be detected.

8.2.6 - Calculation of the probability of failure in accordance with ISO 13849-1

Figure 2 shows a logic subsystem (safety module K1) to which two-channel input and output elements are connected. Since an abstraction of the hardware level is already performed in the safety-related block diagram, the sequence of the subsystems is in principle interchangeable. It is therefore recommended that subsystems sharing the same structure be grouped together, as shown in Figure 3. This makes calculation of the PL simpler by reducing the number of times limitation of the $MTTF_d$ of a channel to 100 years is performed in the estimation.

8.2.7 - Calculation of the probability of failure in accordance with IEC 62061

8.2.7.1 -

In accordance with 6.6.2 of IEC 62061, the circuit arrangement can be divided into three subsystems: B1/B2, K and Q1/Q2 as shown in the safety-related block diagram.

8.2.7.2 -

For subsystem K, the probability of failure of 2,31×10(exp-9) per hour and a SIL claim limit of 3 for the safety module K1 is declared by the manufacturer.

8.2.7.3 -

For the remaining subsystems, the probability of failure can be estimated as follows.

- Subsystem B1/B2: the $B10_d$ value of 1 000 000 cycles [manufacturer's value] is stated for the mechanical part of B1. For the position switch B2, the $B10_d$ value is 500 000 cycles [manufacturer's value]. At 365 working days per year, 24 working hours per day and a cycle time of 15 min, C is 4 cycles per hour for these components. The failure rate is calculated as $0,1 \times C/B10_d = 4$,

8.2.7.3 -

00×10(exp-7)/h. For B2 this gives a failure rate of 8,00 × 10(exp-7)/h.

NOTE The number of operating cycles, C, of the application according to IEC 62061 corresponds to the mean number of annual operations, nop, according to ISO 13849-1. Since C is stated in cycles per hour and nop in cycles per year, the following relation applies:

Thus the mean operation in hours per day and days per year has influence on the value of C as well as of nop.

- The logical architecture of this subsystem equates to diagram D from 6.7.8.2.5 of IEC 62061 as shown in Figure 4.

8.2.7.4 -

The data above is entered into the formula to give a PFHD of 3,04×10(exp−8).

8.2.7.5 -

Similarly, for subsystem Q1/Q2: contactors Q1 and Q2 have a B10 value that corresponds under inductive load (AC 3) to an electrical lifetime of 10(exp6) cycles (manufacturer's value). If 50 % of failures are assumed to be dangerous, the B10d value is produced by doubling the B10 value. The value assumed above for C results in a failure rate of 2,00×10(exp−7)/h for each contactor.

8.2.7.6 -

The logical architecture of subsystem Q1/Q2 equates to diagram D from 6.7.8.2.5 of IEC 62061. The subsystem elements (contactors Q1 and Q2) are of the same design, therefore Equation (D.1) is used to determine the PFHD of the subsystem:

8.2.7.7 -

The subsystems B1/B2 and Q1/Q2 are then subjected to the architectural constraints given in Table 5 of IEC 62061.

See Table 2.

Table 2 - Architectural constraints on subsystems' maximum SIL CL that can be claimed for an SRCF using this subsystem

8.2.7.8 -

Each subsystem has a safe failure fraction of 99% (based on their DC) and a hardware fault tolerance of 1. That produces a SIL CL (SIL claim limit) of 3 for each subsystem.

8.2.7.9 -

For subsystem K1 the PFHD of 2,31 × 10(exp−9) per hour and SIL CL 3 have been declared by the manufacture (see above).

8.2.7.10 -

The maximum SIL that can be claimed based on the lowest SIL CL is therefore 3.

8.2.7.11 -

The PFHD of each subsystem is added together:

3,04 × 10(exp−8) (subsystem B1/B2) + 2,31 × 10(exp−9) (subsystem K) + 1,01 × 10(exp−8) (subsystem Q1/Q2) = 4,28 × 10(exp−8).

This satisfies the range W 10(exp−8) to < 10(exp−7) as given in IEC 62061, Table 3. Therefore if all other requirements of IEC 62061 are fulfilled this safety function achieves SIL 3.

8.3 - Conclusion

8.3.1 -

The results of the above calculation for this simple example using the method from ISO 13849-1 gives the average probability of dangerous failure as 2,70 × 10(exp−8) per hour (i.e. corresponding to PL e), while use of the method from IEC 62061 gives a probability of dangerous failure as 4,28 × 10(exp−8) per hour (i.e. corresponding to SIL 3). The difference between these results is within expected error bounds and therefore shows an acceptable level of correspondence between both standards.

8.3.2 -

It should be noted that there is some variation between the two standards in the way that β (the susceptibility to common cause failures) is handled for redundant systems. This can cause a small but acceptable deviation (as shown in this example) between the PFHD achieved according to the two standards. The methodology in ISO 13849-1 assumes a β factor of 2% if sufficient measures from Table F.1 of the standard are fulfilled. IEC 62061 uses a differently structured table in Annex F. The use of this table produces a β factor that can range from 1 to 10%. Each method for determination of the β factor is intended to be used only within the context of the subsystem design methodology of its respective standard.