TK282, 200624

# Bakgrund, koppling till EN 62061 samt kort om förändringar

Anette Wester Odbratt

# Historik

## EN 954-1 och EN ISO 13849-1

- EN 954-1:1996 (kvalitativa krav)
- EN ISO 13849-1:2006 (kvalitativa och kvantitativa krav)
- EN ISO 13849-1:2008
- EN ISO 13849-1:2015
- EN ISO 13849-1:2020?

# ISO/DIS 13849-1

O´Tooles lag
Murphy var en optimist!

**3.1.22**

**safety function**

function of the machine whose failure can result in an immediate increase of the risk(s)

©ABB

# Allmänt

- Revidering av EN ISO 13849-1 pågår parallellt med revideringen av EN 62061
- Ansvarig arbetsgrupp för EN ISO 13849-1; TC199/WG8
- Ingen samordning mellan EN ISO 13849-1 och EN 62061
- Tanken var att använda kapitlet om krav för mjukvara i båda standarderna – ett resultat från arbetet med att slå samman standarderna (JWG1). Resultatet blev att endast IEC 62061 behöll det, medan EN ISO 13849-1 återgick till krav för mjukvara enligt befintlig standard (med modifiering).
- Diskussioner från arbetet i JWG1 fortsatte i WG8, dvs spännvidd från de som allra helst vill ha EN 954-1 tillbaka till de som vill ha fler krav och en tillnärmning till EN/IEC 61508

©ABB

# Ändringar och diskussioner i korthet

- Ändrat flöde i standarden – tanken är att mer följa designprocessen.
- Förslag om hur ”electronic components” skulle kunna anses vara ”well tried components” – ständigt återkommande förslag under revideringen. Ej accepterat.
- I gällande standard finns möjlighet att utvärdera ett Output subsystem om applikationsspecifika tillförlitlighetsdata saknas. Denna möjlighet utökas nu även till Input och Logik.
- Kapitel om Validering är taget från del 2 och nu inkluderat.
- Metoden för att bestämma PL har varit under stor debatt. Många och långa diskussioner om parametern O - Probablity of occurence of hazardous event, som inte finns med i DISen. Däremot finns nytt förslag för bestämning av P. OBS! Annex A är informativt (som i gällande utgåva).
- Mjukvara – paragraf 4.6 behålls (modifierat), blir kapitel 7.
- Nya definitioner; 56 st i DISen, 39 st i gällande standard. Nya def., exempel; subsystem (3.1.44), subsystem element (3.1.45), well-tried component (3.1.47) skilled person (3.1.56).
- Proven in Use (3.1.39) finns i gällande utgåva – dock utan förklaringar och krav (finns tydligt angivet vad som är ”Proven in Use” i EN 61508). Definitionen Proven in Use är borttagen från DISen.
- Vad händer när Mission time är uppnådd?
- Förändringar i kraven på manual reset function
- Eget kapitel för ergonomi

# EN ISO 13949-2

- Vid en kontroll med flera länders standardiseringsorgan framkom att många fler exemplar av del 1 jämfört med del 2, hade sålts.
- WG8 kom fram till att vi därför vill ha en standard
- Från mötesprotokoll N374 (181219)

"For the integration of the annexes from ISO 13849-2, WG 8 decides to start after the publication of ISO 13849-1 the revision of ISO 13849-2 and integrate the Annexes of ISO 13849-2 as an Amendment to ISO 13849-1. As result the published ISO 13849-2 will be withdrawn."

# EN ISO 13849-1

## Innehållsförteckning


**European foreword** ..... v
**Introduction** ..... vi
**1 Scope** ..... 1
**2 Normative references** ..... 1
**3 Terms, definitions, symbols and abbreviated terms** ..... 2
3.1 Terms and definitions ..... 2
3.2 Symbols and abbreviated terms ..... 7
**4 Design considerations** ..... 9
4.1 Safety objectives in design ..... 9
4.2 Strategy for risk reduction ..... 11
4.2.1 General ..... 11
4.2.2 Contribution to the risk reduction by the control system ..... 11
4.3 Determination of required performance level ($PL_r$) ..... 13
4.4 Design of SRP/CS ..... 14
4.5 Evaluation of the achieved performance level PL and relationship with SIL ..... 15
4.5.1 Performance level PL ..... 15
4.5.2 Mean time to dangerous failure of each channel ($MTTF_D$) ..... 16
4.5.3 Diagnostic coverage (DC) ..... 17
4.5.4 Simplified procedure for estimating the quantifiable aspects of PL ..... 17
4.5.5 Description of the output part of the SRP/CS by category ..... 19
4.6 Software safety requirements ..... 20
4.6.1 General ..... 20
4.6.2 Safety-related embedded software (SRESW) ..... 21
4.6.3 Safety-related application software (SRASW) ..... 22
4.6.4 Software-based parameterization ..... 24
4.7 Verification that achieved PL meets $PL_r$ ..... 25
4.8 Ergonomic aspects of design ..... 26
**5 Safety functions** ..... 26
5.1 Specification of safety functions ..... 26
5.2 Details of safety functions ..... 28
5.2.1 Safety-related stop function ..... 28
5.2.2 Manual reset function ..... 29
5.2.3 Start/restart function ..... 29
5.2.4 Local control function ..... 30
5.2.5 Muting function ..... 30
5.2.6 Response time ..... 30
5.2.7 Safety–related parameters ..... 30
5.2.8 Fluctuations, loss and restoration of power sources ..... 30
**6 Categories and their relation to $MTTF_D$ of each channel, $DC_{avg}$ and CCF** ..... 31
6.1 General ..... 31
6.2 Specifications of categories ..... 31
6.2.1 General ..... 31
6.2.2 Designated architectures ..... 32
6.2.3 Category B ..... 32
6.2.4 Category 1 ..... 33
6.2.5 Category 2 ..... 34
6.2.6 Category 3 ..... 35
6.2.7 Category 4 ..... 36
6.3 Combination of SRP/CS to achieve overall PL ..... 38
**7 Fault consideration, fault exclusion** ..... 40
7.1 General ..... 40
7.2 Fault consideration ..... 40
7.3 Fault exclusion ..... 40
**8 Validation** ..... 40
**9 Maintenance** ..... 40
**10 Technical documentation** ..... 41
**11 Information for use** ..... 41
**Annex A** (informative) **Determination of required performance level ($PL_r$)** ..... 43
**Annex B** (informative) **Block method and safety-related block diagram** ..... 47
**Annex C** (informative) **Calculating or evaluating $MTTF_D$ values for single components** ..... 49
**Annex D** (informative) **Simplified method for estimating $MTTF_D$ for each channel** ..... 56
**Annex E** (informative) **Estimates for diagnostic coverage (DC) for functions and modules** ..... 58
**Annex F** (informative) **Estimates for common cause failure (CCF)** ..... 61
**Annex G** (informative) **Systematic failure** ..... 63
**Annex H** (informative) **Example of combination of several safety-related partsof the control system** ..... 66
**Annex I** (informative) **Examples** ..... 69
**Annex J** (informative) **Software** ..... 76
**Annex K** (informative) **Numerical representation of Figure 5** ..... 79
**Annex ZA (informative) Relationship between this European Standard and the Essential Requirements of EU Directive 2006/42/EC** ..... 84
**Bibliography** ..... 85

# ISO/DIS 13849-1

## Innehållsförteckning


Foreword ... vii
Introduction ... viii
1 Scope ... 1
2 Normative references ... 1
3 Terms and definitions ... 2
3.1 Terms and definitions ... 2
3.2 Symbols and abbreviated terms ... 11
4 Overview ... 12
4.1 Requirements for risk assessment and risk reductions ... 12
4.2 Contribution to the risk reduction by the safety function ... 14
4.3 Risk reduction using an SRP/CS ... 15
4.4 Methodology ... 16
4.5 Required Information ... 17
4.6 Safety function realization by using subsystems ... 17
5 Specification of safety functions ... 17
5.1 General ... 17
5.2 Safety requirements specification (SRS) ... 18
5.2.1 General requirements ... 18
5.2.2 Decomposition of SRP/CS into subsystems ... 21
5.2.3 Requirements for specific safety functions ... 23
5.3 Determination of required performance level ($PL_r$) for each safety function ... 27
5.4 Review of the safety requirement specification ... 27
6 Design considerations ... 28
6.1 Evaluation of the achieved performance level PL ... 28
6.1.1 General overview of Performance level PL ... 28
6.1.2 Correlation between PL and SIL ... 29
6.1.3 Architecture – Categories and their relation to $MTTF_D$ of each channel, $DC_{avg}$ and CCF ... 30
6.1.4 Mean time to dangerous failure ($MTTF_D$) ... 37
6.1.5 Diagnostic coverage (DC) ... 38
6.1.6 Common cause failures (CCF) ... 39
6.1.7 Systematic failures ... 39
6.1.8 Simplified procedure for estimating the PL ... 40
6.1.9 Alternative procedure to determine the PL and $PFH_D$ without $MTTF_D$ ... 41
6.1.10 Fault consideration and fault exclusion ... 43
6.2 Combination of subsystems to achieve an overall PL of the safety function ... 44
6.2.1 General ... 44
6.2.2 Known $PFH_D$ values ... 45
6.2.3 Unknown $PFH_D$ values ... 45
7 Software safety requirements ... 46
7.1 General ... 46
7.2 Safety-related embedded software (SRESW) ... 47
7.3 Safety-related application software (SRASW) ... 48
7.4 Limited variability language (LVL) ... 51
7.4.1 General ... 51
7.4.2 Full variability language (FVL) ... 52
7.4.3 Decision for LVL or FVL ... 52
7.5 Software-based parameterization ... 54
7.5.1 General ... 54
7.5.2 Influences on safety-related parameters ... 54
7.5.3 Requirements for software based manual parameterization ... 55
7.5.4 Verification of the parameterization tool ... 56
7.5.5 Performance of software based manual parameterization ... 57
8 Verification that achieved PL meets $PL_r$ ... 57
9 Ergonomic aspects of design ... 57
10 Validation ... 57
10.1 Validation principles ... 57
10.1.1 General ... 57
10.1.2 Validation plan ... 59
10.1.3 Generic fault lists ... 60
10.1.4 Specific fault lists ... 60
10.1.5 Information for validation ... 60
10.2 Validation by analysis ... 61
10.2.1 General ... 61
10.2.2 Analysis techniques ... 62
10.3 Validation by testing ... 62
10.3.1 General ... 62
10.3.2 Measurement accuracy ... 63
10.3.3 Additional requirements for testing ... 63
10.3.4 Number of test samples ... 64
10.3.5 Testing methods ... 64
10.4 Validation of the Safety Requirements Specification (SRS) ... 65
10.5 Validation of the safety function ... 65
10.6 Validation of the safety integrity of the SRP/CS ... 66
10.6.1 Validation of subsystem(s) ... 66
10.6.2 Validation of measures against systematic failures ... 67
10.6.3 Validation of safety-related software ... 67
10.6.4 Validation of combination of subsystems ... 68
10.6.5 Checking/verification of safety integrity ... 69
11 Maintenance ... 69
12 Technical documentation ... 69
13 Information for use ... 70
13.1 General ... 70
13.2 Information for SRP/CS integrator ... 70
13.3 Information for user ... 71
Annex A (informative) Determination of required performance level ($PL_r$) ... 73
A.1 Selection of $PL_r$ ... 73
A.2 Guidance for selecting parameters S, F and P for the risk estimation ... 74
A.2.1 Severity of injury S1 and S2 ... 74
A.2.2 Frequency and/or exposure times to hazard, F1 and F2 ... 74
A.2.3 Possibility of avoiding the harm ... 75
A.3 Overlapping hazards ... 76
Annex B (informative) Block method and safety-related block diagram ... 78
B.1 Block method ... 78


©ABB

# ISO/DIS 13849-1

## Innehållsförteckning


B.2 Safety-related block diagram ... 78
Annex C (informative) Calculating or evaluating $MTTF_D$ values for single components ... 80
C.1 General ... 80
C.2 Good engineering practices method ... 80
C.3 Hydraulic components ... 80
C.4 MTTFD of pneumatic, mechanical and electromechanical components ... 82
C.4.1 General ... 82
C.4.2 Calculation of $MTTF_D$ for components from $B_{10D}$ ... 83
C.4.3 Explanation of the equations ... 84
C.4.4 Example ... 84
C.5 $MTTF_D$ data of electrical components ... 85
C.5.1 General ... 85
C.5.2 Semiconductors ... 85
C.5.3 Passive components ... 86
Annex D (informative) Simplified method for estimating MTTFD for each channel ... 88
D.1 Parts count method ... 88
D.2 $MTTF_D$ for different channels, symmetrisation of $MTTF_D$ for each channel ... 89
Annex E (informative) Estimates for diagnostic coverage (DC) for functions and modules ... 90
E.1 Examples of diagnostic coverage (DC) ... 90
E.2 Estimation of average DC ($DC_{avg}$) ... 93
Annex F (informative) Measures against common cause failures (CCF) ... 94
F.1 General ... 94
F.2 Estimation of effect of CCF ... 94
F.3 Description of the measures against CCF in Table F.1 ... 95
F.4 Measures against CCF and other relevant standards ... 97
Annex G (informative) Systematic failure ... 98
G.1 General ... 98
G.2 Measures for the control of systematic failures ... 98
G.3 Measures for avoidance of systematic failures ... 99
G.4 Measures for avoidance of systematic failures during SRP/CS integration ... 100
Annex H (informative) Example of combination of several subsystems ... 101
Annex I (informative) Examples ... 103
I.1 General ... 103
I.2 Safety function and required performance level ($PL_r$) ... 103
I.3 Example A, single-channel system ... 104
I.3.1 Identification of safety-related parts ... 104
I.3.2 Quantification of $MTTF_D$, $DC_{avg}$, measures against CCF, category, PL ... 105
I.4 Example B, redundant system ... 106
I.4.1 Identification of safety-related parts ... 106
I.4.2 Quantification of $MTTF_D$ for each channel, $DC_{avg}$, measures against CCF, category and PL ... 107
Annex J (informative) Software ... 111
J.1 Description of example ... 111
J.2 Application of V-model of software safety lifecycle ... 111
J.3 Verification of software specification ... 112
J.4 Example of programming rules ... 112
Annex K (informative) Numerical representation of Figure 12 ... 114
Annex L (informative) EMC immunity requirements ... 118
Annex M (informative) Additional Information for Safety Requirements Specification ... 121
Annex N (informative) Avoiding of systematic failure in software-design ... 123
N.1 Selection of fault avoiding measures for the design of safety-related software ... 123
Anhang ZA (informative) Relationship between this European Standard and the essential requirements of EU Directive 2006/42/EC aimed to be covered ... 130
Bibliography ... 131

# Koppling till EN 62061

ISO/TR 23849 – beslut taget att denna ska dras tillbaka

**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.

# IEC 62061:2005 och IEC 62061 (CDV)

Scope

**1 Scope**

This International Standard specifies requirements and makes recommendations for the design, integration and validation of safety-related electrical, electronic and programmable electronic control systems (SRECS) for machines (see Notes 1 and 2). It is applicable to control systems used, either singly or in combination, to carry out safety-related control functions on machines that are not portable by hand while working, including a group of machines working together in a co-ordinated manner.

**1 Scope**

This International Standard specifies requirements and makes recommendations for the design, integration and validation of safety-related control systems (SCS) for machines. It is applicable to control systems used, either singly or in combination, to carry out safety functions on machines that are not portable by hand while working, including a group of machines working together in a co-ordinated manner.

Nytt förslag till IEC 62061 begränsas inte till SRECS utan omfattar samma som EN ISO 13849-1.

# Korrelation till PL – enligt IEC 62061 (CDV)

Ensidig begränsning av pre-designed subsystems

**Table 2 – Required SIL and PFH of pre-designed subsystem**

| IEC 62061 (IEC 61508) | IEC 62061 | IEC 61508 Type B subsystem (see also NOTE 1) | ISO 13849 (see also NOTE 2) | IEC 61496 |
|---|---|---|---|---|
| **PFH** | **SIL** | **at least ...** | **at least ...** | **at least ...** |
| $< 10^{-5}$ | SIL 1 | SIL 1 | PL c | Type 2 |
| $< 10^{-6}$ | SIL 2 | SIL 2 | PL d | Type 3 |
| $< 10^{-7}$ | SIL 3 | SIL 3 | PL e | Type 4 |

NOTE 1 This column includes SIL-based standards that fulfil the architectural constraints of the IEC 61508, such as IEC 61800-5-2 and IEC 60947-5-3.

NOTE 2 Does not apply to subsystems using complex components.

NOTE 3 A relation between IEC 62061 and IEC 61511 or ISO 26262 cannot be assumed within this table.

# Korrelation till SIL - enligt EN ISO 13849-1

**Table 3 — Correlation between performance level (PL) and safety integrity level (SIL)**

| PL | SIL<br>(IEC 62061, for information) high/continuous mode of operation |
|---|---|
| a | No correlation |
| b | 1 |
| c | 1 |
| d | 2 |
| e | 3 |

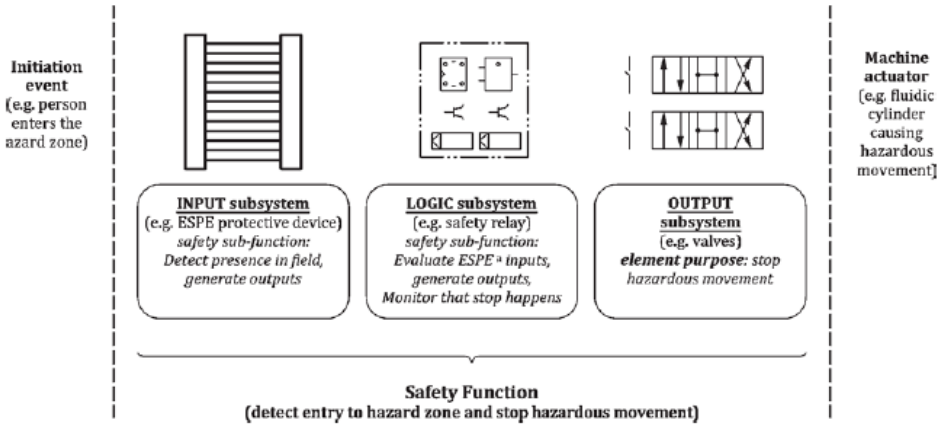
PL a has no correlation on the SIL scale and is mainly used to reduce the risk of slight, normally reversible, injury.

# 20 års Mission Time – och sen?

- Frågan om vad man gör med komponenter/säkerhetskomponenter i en skyddsfunktion efter de 20 årens mission time har vi haft uppe flera gånger i TK282
- I DISen blev lösningen att lägga till en Note under definitionen av mission time

**3.1.33**
**mission time**
$T_M$
period of time covering the intended use of an SRP/CS
Note 1 to entry: to entry: Typically, by reaching the mission time the SRP/CS is replaced.

# Subsystem

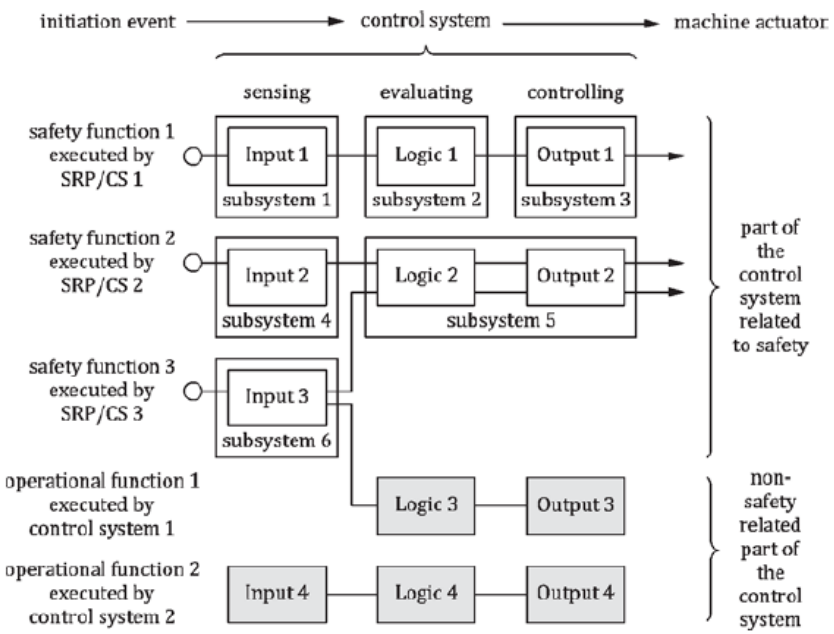



**3.1.44**
**subsystem**
entity which results from a first-level decomposition of an SRP/CS and whose dangerous failure results in a dangerous failure of a safety function

Note 1 to entry: The subsystem specification includes its role in the safety function and its interface with the other subsystems of the SRP/CS.

Note 2 to entry: One subsystem can be part of one or several SRP/CS, e.g. the same combination of contactors can be used for de-energise a motor in case of detection of a person in a danger zone and also in case of opening a safe guard.

# Skyddsfunktioner och subsystem




**Key**

a) Safety function 1 is decomposed into sub-function 1, sub-function 2 and sub-function 3. Sub-function 1 is executed by subsystem 1, etc.

b) Safety function 2 is decomposed into sub-function 4 and sub-function 5. Sub-function 4 is executed by subsystem 4, etc.

c) Safety function 3 is decomposed into sub-function 6 and sub-function 5. Sub-function 6 is executed by subsystem 6, etc.

# Avsaknad av applikationsspecifik data

EN ISO 13849-1:2015

**4.5.5 Description of the output part of the SRP/CS by category**

If for mechanical, hydraulic or pneumatic components (or components comprising a mixture of technologies) no application–specific reliability data are available, the machine manufacturer may evaluate the quantifiable aspects of the PL without any $MTTF_D$-calculation. For such cases, the safety-related performance level (PL) is implemented by the architecture, the diagnostic and the measures against CCF.

…

**Table 7 — PL and $PFH_D$ as worst case estimation based on category, $DC_{avg}$, and use of well-tried components**

| | $PFH_D$ (1/h) | Cat. B | Cat. 1 | Cat. 2 | Cat. 3 | Cat. 4 |
|---|---|---|---|---|---|---|
| PL a | 2*10–5 | • | O | O | O | O |
| PL b | 5*10–6 | • | O | O | O | O |
| PL c | 1,7*10–6 | - | •2* | •1* | O | O |
| PL d | 2,9*10–7 | - | - | - | •1* | O |
| PL e | 4,7*10–8 | - | - | - | - | •1* |

• Applied category is recommended.

O Applied category is optional.

- Category is not allowed.

1* Proven in use (see 3.1.39) or well-tried (confirmed by the component manufacturer to be suitable for the particular application) components and well-tried safety principles must be used.

2* Well-tried components and well-tried safety principles must be used.

For safety-related components that are not monitored in the process, the T10d value can be determined based on proven in use data by the machine manufacturer.

# Avsaknad av applikationsspecifik data

## ISO/DIS 13849-1

**6.1.9 Alternative procedure to determine the PL and $PFH_D$ without $MTTF_D$**

**6.1.9.1 General**

The alternative procedure to determine the PL without $MTTF_D$ is limited to subsystems incorporating mechanical, hydraulic, pneumatic, electrohydraulic or electropneumatic components where no reliability data is available. This method can also be used when the good engineering practice method given in Annex C.2 is not applicable. In these two cases, the machine manufacturer may use the alternative procedure described in 6.1.9 to evaluate the PL without any $MTTF_D$ calculation.

The combination of several subsystems with different PL is considered in 6.2.

**6.1.9.2 Preconditions**

If for mechanical, hydraulic or pneumatic components (or components comprising a mixture of technologies) no application–specific or component manufacturer reliability data are available or the good engineering practice method of Annex C.2 is not applicable, the machine manufacturer may evaluate the quantifiable aspects of the PL without any $MTTF_D$-calculation.

Where no $MTTF_D$ data is available, the safety-related performance level (PL) can be implemented by the architecture, the diagnostic and the measures against CCF.

As a worst case assumption the $T_{10D}$ value is limited to 10 years. In this case the calculation of the $DC_{avg}$ is reduced to the arithmetic mean value of all individual component DC values in the functional channel.

For well-tried components an assumption for $T_{10D}$ for 20 years may be accepted.

# Avsaknad av applikationsspecifik data

ISO/DIS 13849-1

**6.1.9.3 Inputs and outputs**

The mission time (TM) is assumed to be 20 years. For category 2 a sufficient test rate and reliability of the test channel (see 6.1.3.2.4) are required. The requirements, e.g. according to $DC_{avg}$ and CCF and systematic issues, for each category (see 6.1.3) shall be fulfilled.

Table 7 shows the relationship between achievable PL (corresponding to Figure 12) and categories. PL a and PL b can be implemented with Cat. B if basic safety principles are followed. PL c can be implemented with Cat. 1 or Cat. 2, if well-tried components and well-tried safety principles are used.

PL d can be implemented with Cat. 3, respectively PL e with Cat. 4, if well-tried components, basic and well-tried safety principles are used.

Table 7 — PL and $PFH_D$ estimation based on category, and component selection

| | $PFH_D$ (1/h) | Cat. B | Cat. 1 | Cat. 2 | Cat. 3 | Cat. 4 |
|---|---|---|---|---|---|---|
| PL b | $5\times10^{-6}$ | • | O | O | O | O |
| PL c | $1{,}7\times10^{-6}$ | — | •1* | •1* | O | O |
| PL d | $2{,}9\times10^{-7}$ | — | — | — | •1* | O |
| PL e | $4{,}7\times10^{-8}$ | — | — | — | — | •1* |

• Applied category is recommended.

O Applied category is optional.

— Category is not allowed.

1* Well-tried components, basic and well-tried safety principles shall be used.

# Avsaknad av applikationsspecifik data

ISO/DIS 13849-1

**6.1.9.4 Logic**

Where no $MTTF_D$ data is available a conservative approach using $MTTF_D$ can be assumed

— for category B, 2 and 3 is 10 years for each channel.

— for category 1 a $MTTF_D$ of the channel of 30 years can be assumed and well-tried components have to be used. The maximum PL that can be achieved is PL c (see Annex K).

For category 2 and category 3 common-cause failures (CCF) and diagnostic coverage (DC) shall be considered. The $DC_{avg}$ shall match at least 60 % for category 2 and category 3.

Category 4 is excluded in this method.

With the category, the $MTTF_D$ and the $DC_{avg}$, the PL and the $PFH_D$ of the subsystem can be determined with Table K.1.

# Manual reset function

## EN ISO 13849-1

**5.2.2 Manual reset function**

The following applies in addition to the requirements of Table 8.

After a stop command has been initiated by a safeguard, the stop condition shall be maintained until safe conditions for restarting exist.

The re-establishment of the safety function by resetting of the safeguard cancels the stop command. If indicated by the risk assessment, this cancellation of the stop command shall be confirmed by a manual, separate and deliberate action (manual reset).

The manual reset function shall

— be provided through a separate and manually operated device within the SRP/CS,

— only be achieved if all safety functions and safeguards are operative,

— not initiate motion or a hazardous situation by itself,

— be by deliberate action,

— enable the control system for accepting a separate start command,

— only be accepted by disengaging the actuator from its energized (on) position.

The performance level of safety-related parts providing the manual reset function shall be selected so that the inclusion of the manual reset function does not diminish the safety required of the relevant safety function.

…

# Manual reset function

## ISO/DIS 13849-1

**5.2.3.2 Manual reset function**

The re-establishment of the safety function by resetting of the safeguard cancels the stop command. If indicated by the risk assessment, this cancellation of the stop command shall be confirmed by a manual, separate and intended action (manual reset).

The manual reset function shall

— be provided through a separate and manually operated device which is separate from start command within the SRP/CS,

— only be achieved if all affected safety functions and safeguards are operative,

— not initiate a hazardous situation by itself,

— be by intended action,

— enable the control system to accept a separate start command,

— be accepted by signal change.

The parts providing the manual reset function shall be selected so that they do not diminish the safety required of the relevant safety function.

When the function “manual reset” is required to be a safety function (e.g., prevention of unexpected start), the required performance level has to be determined.

…

# General Purpose PLC’s

4.6.2 **Safety-related embedded software (SRESW), EN ISO 13849-1:2015**

…

For components for which SRESW requirements are not fulfilled, e.g. PLCs without safety rating by the manufacturer, these components may be used under the following alternative conditions:

— the SRP/CS is limited to PL a or b and uses category B, 2 or 3;

— the SRP/CS is limited to PL c or d and may use multiple components for two channels in category 2 or 3. The components of these two channels use diverse technologies.

**7.2 Safety-related embedded software (SRESW), ISO/DIS 13849-1**

…

For components for which SRESW requirements are not fulfilled, e.g. PLCs without safety rating by the manufacturer, these components may be used under the following alternative conditions:

— the subsystem is limited to PL a or b and uses category B, 2 or 3;

— the subsystem is limited to PL c with category 2 or PL d with category 3 and it is necessary to fulfil the diversity requirements of the CCF, which means that both channels must have own non-safe PLC’s, which both use diverse technologies compared to each other.

The associated hardware shall be assessed in accordance with the requirements of this standard.

# Maintenance

EN ISO 13849-1

**9 Maintenance**

Preventive or corrective maintenance can be necessary to maintain the specified performance of the safety-related parts. Deviations with time from the specified performance can lead to a deterioration in safety or even to a hazardous situation. The information for use of the SRP/CS shall include instructions for the maintenance (including periodic inspection) of the SRP/CS.

The provisions for the maintainability of the safety-related part(s) of a control system shall follow the principles given in ISO 12100:2010, 6.2.7. All information for maintenance shall comply with ISO 12100:2010, 6.4.5.1 e).

# Maintenance

ISO/DIS 13849-1

**11 Maintenance**

Preventive or corrective maintenance can be necessary to maintain the specified performance of the SRP/CS.

NOTE 1 Exceeding specified lifetime or test can lead to deterioration in safety or to a hazardous situation.

When designing a machine, the following maintainability factors shall be taken into account to enable maintenance of the machine:

— accessibility, taking into account the environment and the human body measurements, including the dimensions of the working clothes and tools used;

— ease of handling, taking into account human capabilities;

— limitation of the number of special tools and equipment;

— required illumination levels.

# Ergonimska aspekter

**4.8 Ergonomic aspects of design (EN ISO 13849-1:2015)**

The interface between operators and the SRP/CS shall be designed and realized such that no person is endangered during all intended use and reasonable foreseeable misuse of the machine [see also ISO 12100, EN 614-1, ISO 9355-1, ISO 9355-2, ISO 9355-3, EN 1005-3, IEC 60204-1:2005, Clause 10, IEC 60447 and IEC 61310].

Ergonomic principles shall be used so that the machine and the control system, including the safetyrelated parts, are easy to use, and so that the operator is not tempted to act in a hazardous manner.

The safety requirements for observing ergonomic principles given in ISO 12100:2010, 6.2.8, apply.

**9 Ergonomic aspects of design (ISO/DIS 13849-1)**

The interface between operators and the SRP/CS shall be designed and realized to minimize exposures to hazards during the intended use and the reasonable foreseeable misuse of the machine due to neglecting ergonomic principles.

Ergonomic principles shall be applied so that the control system, including the safety-related parts, is as easy to use, as practicable.

The aim to use ergonomic principles is to avoid defeating control systems or unintended misuse of the machine.

The ergonomic principles given in ISO 12100:2010, 6.2.8, apply.

# Information från tillverkare av subsystem

**6.1.1 General overview of Performance level PL**

…

It is not necessary to determine DC, MTTF, CCF and to evaluate SRESW for subsystems, which already have PL or SIL, and $PFH_D$-value from manufacturer.

ABB