

ISO/IEC 17305

IEC 62061 e ISO 13849-1 Unificazione in ISO/IEC 17305

ISO/IEC 17305

Safety of machinery – Safety functions of control systems

The new standard committee under French chairmanship

Objectives of ISO/IEC 17305

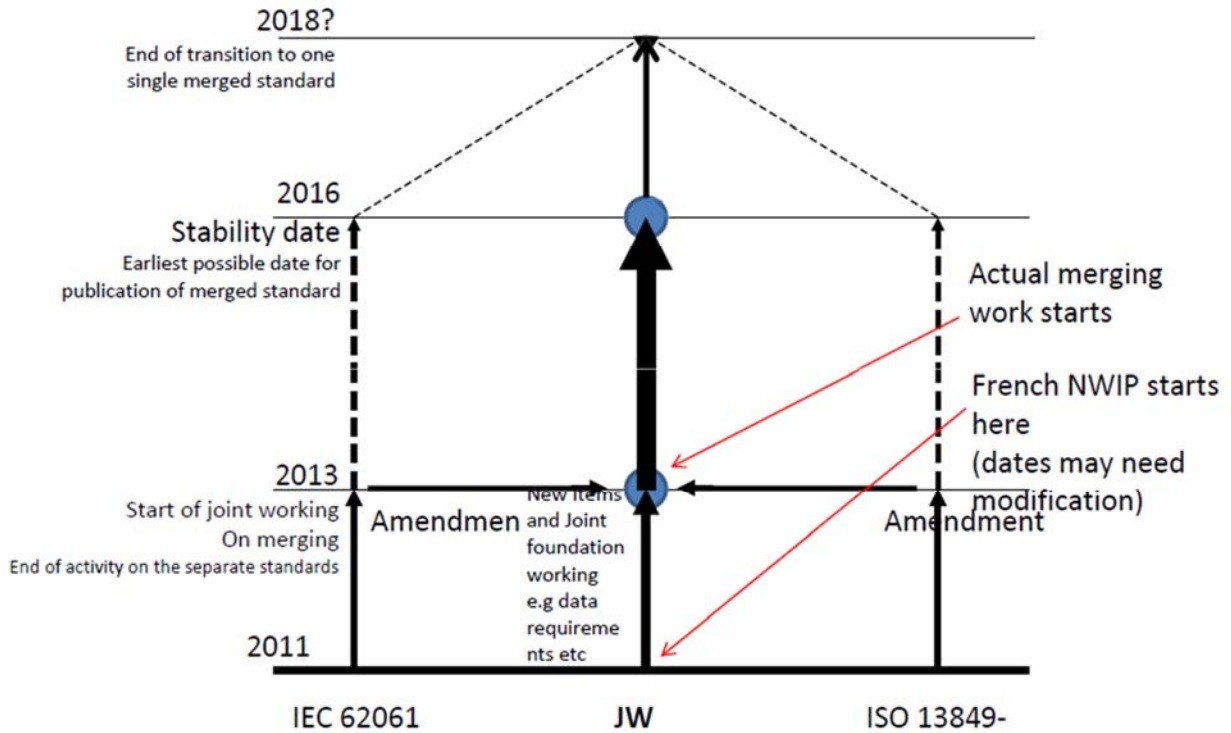
Based on the feedback gathered from approximately five years, this proposal aims at merging:

- ISO 13849-1 Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design and
- IEC 62061 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems.

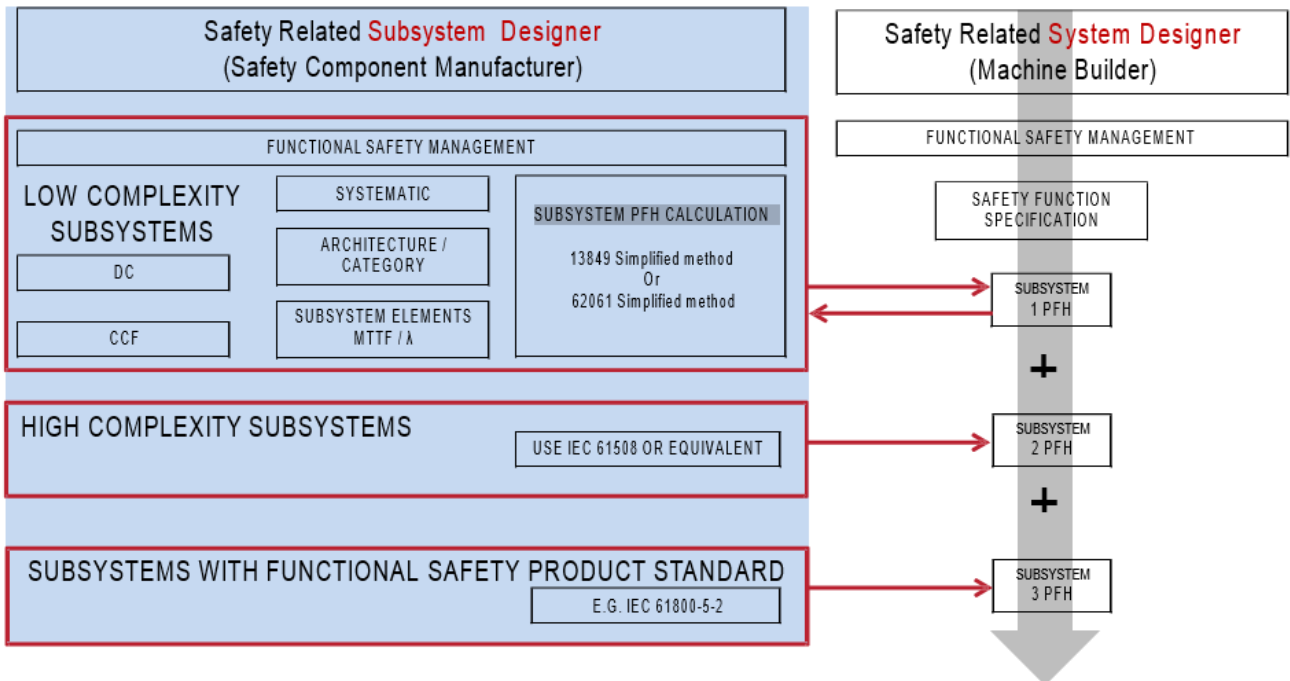
It is based on the following principles:

- No alteration of the methodology or of the basic approach introduced by both standards
- Deletion of overlaps
- Simplification of the use
- Introduction of additions stemming from the feedback

Process Preview



Fonte: Rockwell Automation



Fonte: Rockwell Automation


Current status

Fonte:

K.A. SCHMERSAL Holding GmbH & Co. & BG ETEM

It is also worth keeping an eye here on the development of an amendment to EN ISO 13849-1 that is currently in progress and is intended to iron out any contradictions in the standard and to facilitate more flexible use.

The following slides were shown by the **engineer Klaus-Dieter Becker**, from the Employer's Liability Insurance Association for Energy, Textiles, Electrical and Media products (**BG ETEM**), print and paper processing industry, during the trade congress "Control of print and paper processing machines" in June 2012 in Bernried. They give an overview of the current status of considerations (warning: DRAFT! – please do not take at face value!):



Modifications


- Deletion of Table 1
- It is not permissible to mix requirements of the standards when designing safety-related parts of control systems (SRP/CS) (ISO 13849-1 and IEC 61508/ IEC 62061)
- The maximum MTTFd value for Category 4 is increased to 2500 years because in Category 4 the other quantifiable aspects, structure and DC, are at their maximum point. This allows to combine a greater number of subsystems with Category 4 and PL e and still stay in PL e according to Clause

Vortragstitel, Autor, Veranstaltung 01.06.2012 Seite 2

As an aid to understanding:

This concerns the table "Recommended application of IEC 62061 und ISO 13 849-1" which was actually obsolete from the start.

- Needs no further explanation. No "cherry picking"!
- Special question. No further remarks.

 BG ETEM

Modifications

For the designated architectures, the following typical assumptions are made:

- mission time, 20 years (see Clause 10);
- constant failure rates within the mission time;
- for category 2, demand rate $\leq 1/100$ test rate;
- or testing occurs immediately upon demand of the safety function and the fault detection and reaction time is shorter than the time to reach the hazard

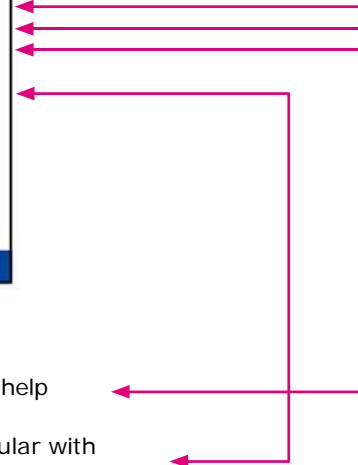
(see also ISO 13855);


Vortragstitel, Autor, Veranstaltung 01.06.2012 Seite 3

As an aid to understanding:

As far as we know, nothing actually new; however it may help to clarify uncertainties.

New possibilities for realising control category 2, in particular with traditional technologies (fluidics, electromechanics).



 BG ETEM

For standard components performing a safety related function implementing embedded software, e.g. standard PLCs, normally no information about the fulfilment of SRESW requirements is available for the integrator. If standard components for industrial use are implemented in SRP/CS the fulfilment of the above SRESW requirement is not mandatory under the following alternative conditions:


1. the SRP/CS is limited to PL a or b and uses Category B, 2 or 3;
2. the SRP/CS is limited to PL c or d and uses two components for two channels in Category 2 or 3 and the two components use diverse embedded software or diverse technologies so that failure detection concerning embedded software fulfils the required DC (e.g. cross monitoring);
3. the SRP/CS is limited to PL c or d and uses two components for two channels in Category 2 or 3 and uses two diverse application software channels so that failure detection concerning embedded software fulfils the required DC (e.g. cross monitoring).

Vortragstitel, Autor, Veranstaltung 01.06.2012 Seite 4

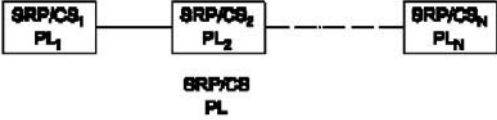
As an aid to understanding:

Applies to necessary clarifications when using programming electronics under normal operating conditions, and in particular standard PLCs.



 BG ETEM


If the PFHD values of all SRP/CSi are known, the PFHD of the combined SRP/CS is the sum of all N PFHD values of the SRP/CSi.



Vortragstitel, Autor, Veranstaltung 01.06.2012 Seite 5

As an aid to understanding:

As far as we know, nothing actually new; however it may help to clarify uncertainties.


 BG ETEM

This methodology to estimate the PLr is not mandatory. It is a generic approach which considers worst case assumption for the probability of occurrence of a hazardous event. E.g. in Type C-standards the resulting PLr can deviate from the generic approach because of machine specific conditions and experiences. Other appropriate risk estimation methods leading to a PLr can also be used.

Vortragstitel, Autor, Veranstaltung 01.06.2012 Seite 6

As an aid to understanding:

In our opinion important clarification on the informative character of the risk graph in the informative Annex A of EN ISO 13849-1.

 **BG ETEM**


Probability of Occurrence of a Hazardous Event

The probability of occurrence of a hazardous event depends on either human behaviour or technical failures. In most cases, the appropriate probabilities are unknown or hard to identify. Therefore, in a worst case approach the probability of occurrence of a hazardous event is set to 1 P2. Where the probability can be reasonably estimated, the PLr may be reduced by one level

Vortragstitel, Autor, Veranstaltung 01.06.2012 Seite 7

As an aid to understanding:

Explanation of why the otherwise commonly used parameter “probability of occurrence of a hazardous event” is not present in the risk graph for EN ISO 13849-1; in future this parameter will be available under certain conditions.

 **BG ETEM**

Overlapping hazards

When using ISO 13849-1, all hazards are being considered as specific hazard or hazardous situation. For the quantification each hazard can be evaluated separately.

EXAMPLE 1 Welding robots have different specific hazardous situations: crushing by movement and burning by the welding process.

The actuators involved in the specific hazardous situation can be summarized or separated depending on their effect (e.g. kinematic chains).


EXAMPLE 2 In one robot cell with separate robots working, each robot is considered separately.

EXAMPLE 3 As a result of a risk assessment it can be sufficient to consider at round table with clamping devices each clamping device separately.

Vortragstitel, Autor, Veranstaltung 01.06.2012 Seite 8

As an aid to understanding:

“1st class burial” of the discussion on overlapping hazards.




If the following criteria are met, the MTTFd value for a single hydraulic component, e.g. valve, can be estimated at 150 years. If the mean number of annual operations (nop) is below 1.000.000 the MTTFd value can be estimated higher as indicated in table C.1

But if either a) or b) is not achieved, the MTTFd value for the single hydraulic component has to be given by the manufacturer. Instead of using a fixed value for the MTTFd as described above it is permissible to use the B10d-concept for MTTFd of pneumatic, mechanical and electromechanical components also for hydraulic components if the manufacturer can provide data.

Vortragstitel, Autor, Veranstaltung 01.06.2012 Seite 9

As an aid to understanding:

New options when using fluidic technology in SRP/CSs.



	Typical values: MTTFd (years) B10d (cycles)
Mechanical components	MTTFd = 150
Hydraulic components with $n_{op} \geq 1\,000\,000$	MTTFd = 150
Hydraulic components with $1\,000\,000 > n_{op} \geq 500\,000$	MTTFd = 300
Hydraulic components with $500\,000 > n_{op} \geq 250\,000$	MTTFd = 600
Hydraulic components with $250\,000 > n_{op}$	MTTFd = 1 200

Vortragstitel, Autor, Veranstaltung 01.06.2012 Seite 10

As an aid to understanding:

New options when using hydraulic technology in SRP/CSs

This is one of the subjects we will cover in detail during the tecnicum seminar K1/12 on 30.08 and 20.11.2012 in Wuppertal and on 25.09 and 22.11.2012 in Maulbronn/Sternenfels.