



► Changes in EN ISO 13849-1 - Functional Safety Standard

Abhijit Kulkarni.

PILZ
THE SPIRIT OF SAFETY

▶ Agenda

- ▶ Introduction
- ▶ Significant Changes with respect to earlier version
- ▶ ISO 13849-1 – Significant changes 2023
- ▶ EN ISO 13849 as an instrument for achieving machinery safety
- ▶ Risk assessment and risk reduction combined with functional safety
- ▶ Evaluation of the implementation of self-developed subsystems
- ▶ Validation in accordance with EN ISO 13849-1

► Introduction

- The standard EN ISO 13849-1 is one of the main safety standards for the design of safety-related control systems for machinery.
- It is the most important functional safety standard in Engineering.
- The standard is to be applied to safety-related parts of control systems, irrespective of the technology and energy used (electrical, hydraulic, pneumatic, mechanical).
- The International Organization for Standardization (ISO) published the new edition of ISO 13849-1 on 27. April 2023.
- The revised version specifies a range of guidelines, for determining the performance level and thus provides better support with implementation.
- It also takes account of the greater significance of software and it's validation.



► ISO 13849-1 – Significant changes 2023

- Clearer structure overall, focusing on the implementation of a safety function as a combination of several subsystems
- Use of the term "subsystem" throughout the document (instead of SRP/CS)
- Improved and extended specification of safety functions (Clause 5)
- Improved guidelines and additional requirements relating to the SRS (safety requirements specification) (Clause 5)
- Clarifications regarding design aspects (Clause 6); e.g. optimized Category 2 definition, determination of CCF per subsystem and with regard to fault consideration, fault exclusion and well-tried components
- Improvements and clarifications regarding software (Clause 7)
- Validation (Clause 10); the normative requirements of ISO 13849-2 were revised and incorporated

► ISO 13849-1 – Significant changes 2023

- Determination of the required performance level (Annex A); changes with regard to parameter P
- Clarification of measures against common cause failures (CCF) - (Annex F)
- Guidelines for the management of functional safety were extended (Annex G.5)
- Details of how to guarantee that EMC noise immunity is sufficiently high (Annex L)
- Supplementary information for the safety requirements specification (Annex M)
- Avoidance of systematic failure through software design (Annex N); contains a simple example for software validation
- Additional information on safety-related values of components (Annex O), adapted to the approach of VDMA standard sheet 66413

► EN ISO 13849 as an instrument for achieving machinery safety

► Part 1 – ISO 13849-1 - General principles for design. It is technically revised to clarify and detail some requirements, without introducing any new technical concepts. (republished in 2023)

► Part 2 of the standard – EN ISO 13849-2:2012: Validation will initially remain as it is and will be revised afterwards.

- The standard is based on a probabilistic approach for the assessment of SRPCS internationally unified requirements, referring to the risk assessment, PL 'r' and identification of SRPCS.



► Risk assessment and risk reduction combined with functional safety

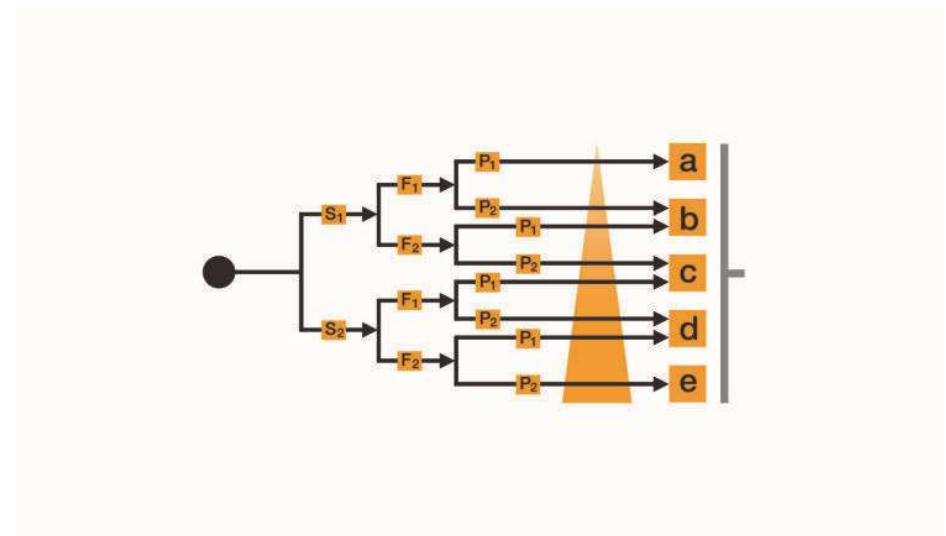
The design of the safety-related parts of control systems is an iterative process follows the following Steps

- Step 1 : Define the safety function requirements
- Step 2 : Determine the required performance level (PL)
- Step 3 : Design and technically implement the safety functions
- Step 4 : Determine and quantitatively evaluate the performance level
- Step 5 : Verification
- Step 6 : Validation

► Risk evaluation and determination of the required performance level PL

The possibility of avoiding the hazard or limiting harm is further specified through five factors for parameter P (Annex 'A')

- Speed with which the hazard arises (e.g. quickly or slowly)
- Possibilities for hazard avoidance (e.g. by escaping)
- Practical safety experiences relating to the process
- Operation by experts or non-professionals
- Operation with or without supervision



▶ Aim of EN ISO 13849-1 and the performance level – Risk reduction

A safety requirements specification (SRS) is required for a clear description of the safety functions with recorded documents

- Function description with the triggering event, reaction and safe state
- PL 'r'
- Corresponding operating modes
- Reaction times
- Error reaction and behaviour
- Priority
- Interfaces (with other safety functions)

► Evaluation of the implementation of self-developed subsystems

In ISO 13849-1 and EN ISO 13849-1, the following aspects must be defined in order to determine the PL of a subsystem.

- System category (structural requirement): Subsystem for fault detection and/or its reliability
- Mean time to dangerous failure (MTTFd)
- Diagnostic coverage (DC), defined as a measure of the effectiveness of the diagnostics:
- Common cause failure (CCF)



► Software – Informative Annex N for avoiding systematic faults

The requirements of application software have been increased in comparison with the previous version EN ISO 13849-1: 2015.

An informative Annex N has been included on the subject of avoiding faults/fault avoidance measures for the safety-related software design. ISO 13849-1 now covers various software types:

- Safety-related embedded software (SRESW)
- Safety-related application software (SRASW)
- Parameter setting software



► Validation in accordance with EN ISO 13849-1

The validation specifications have been adapted and the normative requirements regarding the validation procedure from ISO 13849-2:2012 have been revised and integrated into ISO 13849-1:2023, e.g.

- The analysis supplements the test.
- Validation and examination of the SRS is described in detail
- A simple example of software validation is also provided

► Electromagnetic compatibility requirements (EMC)

An informative Annex L has been incorporated into ISO 13849-1.

- Guarantees sufficient EMC noise immunity with basic measures against EMC Influences
- Various options are Listed with EMC measures table
- The EMC Directive regulates the essential requirements for electromagnetic compatibility.

PILZ

THE SPIRIT OF SAFETY

Pilz India Pvt. Ltd., 6th Floor Cybernex, Shankar Seth Road, Swargate Pune 411037

+91-20- 49221100, info@pilz .in,www.pilz.in

www.pilz.com



© Pilz GmbH & Co. KG 2021

CECE®, CHRE®, CMSE®, InduraNET p®, Leansafe®, Master of Safety®, Master of Security®, PAS4000®, PASca®, PASconfig®, Pilz®, PIT®, PLID®, PMCprimo®, PMCprotego®, PMctendo®, PMD®, PMi®, PNOZ®, PRBT®, PRCM®, Primo®, PRM®, PSEN®, PSS®, PVIS®, SafetyBUS p®, SafetyEYE®, SafetyNET p®, THE SPIRIT OF SAFETY® sind in einigen Ländern amtlich registrierte und geschützte Marken der Pilz GmbH & Co. KG. Wir weisen darauf hin, dass die Produkteigenschaften je nach Stand bei Drucklegung und Ausstattungsumfang von den Angaben in diesem Dokument abweichen können. Für die Aktualität, Richtigkeit und Vollständigkeit der in Text und Bild dargestellten Informationen übernehmen wir keine Haftung. Bitte nehmen Sie bei Rückfragen Kontakt zu unserem Technischen Support auf.



PILZ
THE SPIRIT OF SAFETY