

METSTA

ISO TC199 / WG8
Safe Control Systems



ISO 13849-2

Safety of machinery — Safety-related parts of control systems — Part 2: Application of principles for the design and validation

CD2

- Kommentointivaihe päättyi 28.7. ja kommentteja saatiin 154kpl

Kommentit käyty pääsääntöisesti läpi

- Pieniä tarkennuksia ja termistökorjauksia
- Työryhmätyö avoimien kommenttien osalta käynnissä parhaillaan, marraskuun aikana toivottavasti valmista

Esiarviointi HAS-konsultilta

- Normatiiviseen osaan pientä muutosta
- Rakenne pysynee ennallaan
- Pysyy harmonisoituna standardina

ISO 13849-2

Safety of machinery — Safety-related parts of control systems —
Part 2: Application of principles for the design and validation

1. Scope

2. Normative references

3. Terms and definitions

4. Design and validation

4.1 General

4.2 Integration of safety principles and fault exclusions

Annex A (informative) Validation tools for mechanical systems

Annex B (informative) Validation tools for pneumatic systems

Annex C (informative) Validation tools for hydraulic systems

Annex D (informative) Validation tools for electric systems

Basic safety principles, well-tried safety principles, well-tried components, faults and fault exclusions +

Annex D.3 Soft errors

Annex E. on poistettu kokonaan

ISO/TR 13849-3

Safety of machinery — Safety-related parts of control systems — Part 3: Markov model-based PFH calculation

- Technical Report (ei harmonisointia)
- Tämänhetkinen teksti hyväksytty ISO/CS:n toimesta
- Seuraavaksi FDIS vaiheeseen, äänestysaika 8 viikkoa
- Tavoitejulkaisuaika vielä avoinna

Validointityökalut

ISO 13849-2, Liitteet A-D

- Turvallisuuden perusperiaatteet ja hyvin koetellut turvallisuusperiaatteet:
 - Lisätty määritelmä mille taholle kunkin periaatteen toteuttaminen on olennaista.
- Ilmaisutapoja yhdenmukaistettu turvallisuuden perusperiaatteiden ja hyvin koeteltujen turvallisuusperiaatteiden osalta
- Hyvin koetellut komponentit pneumatiikassa ja hydrauliikassa:
 - Liitteisiin B ja C lisätty taulukot hyvin koetelluista komponenteista ja kriteereistä milloin nämä voidaan katsoa hyvin koetelluiksi.
 - Koskee vain kategorian 1 mukaisia toteutuksia
 - Komponenttien määrittäminen hyvin koetelluiksi edelleen vahvasti sovelluskohtainen
 - Korostettu että päättelyn onko komponentti hyvin koeteltu on perustuttava dokumentoituu tietoon komponentin soveltuvuudesta kohteessa tai käytettävä validointi ja verifiointi toimia joille voidaan osoittaa komponentin olevan hyvin koeteltu sovelluksessa

Table B.1 — Basic safety principles		
Basic safety principle	Remarks	Relevant for (see Table 2)
Use of suitable materials and adequate manufacturing	Selection of material, manufacturing methods and treatment in relation to, e.g. stress, durability, elasticity, friction, wear, corrosion, temperature characteristics of compressed air.	M, D
Correct dimensioning and shaping	Consider, e.g. stress, strain, fatigue, surface roughness, tolerances, sticking, manufacturing.	M, D
Correct selection, combination, arrangements, assembly and installation of components or systems related to the application	Apply the installation and operation instructions provided by the manufacturer, e.g. catalogue sheets, installation instructions, specifications, and use of good engineering practice in similar components or systems.	M, D, U
Abbreviations M – Design and manufacturing of components D – Design of subsystems U – Use of the machine		

Esimerkki tehtävänjaosta turvallisuuden perusperiaatteiden osalta

Soft error

IEC 61508-4 kohta 3.6.12:

Soft-error, tilapäinen (data) virhe: virheelliset muutokset datan sisältöön muttei muutoksia itse fyysiseen piiriin

- “Soft errors are relevant for hardware containing semiconductors with volatile memories and sequential logic”
- Tyypillisesti satunnainen ja hetkellinen vikatila jossa signaali tai data “vioittuu” ilman laitteiston varsinaista vaurioitumista.
 - Esim. Haluttu ohjelma ei toimi suunnitellusti soft-error vian vuoksi.
- Soft error aiheutuu tyypillisesti säteilyn aiheuttamista häiriöistä, mutta muitakin tekijöitä on (EMI, sähköhäiriöt, jännitepiikit, radikaali lämpötilan muutos jne.)

D.3 Soft errors	57
D.3.1 General	57
D.3.2 Introduction to soft errors	57
D.3.3 Relevance of soft errors for functional safety	57
D.3.4 Avoidance and control of soft errors during subsystem design	58
D.3.4.1 Analysis	58
D.3.4.2 Avoidance and reduction of soft errors	58
D.3.4.3 Control of soft errors	58
D.3.4.4 Determination of soft error rates to estimate PFH	59
D.3.4.5 Priority for the determination of soft error rates	59
D.3.4.6 Non-accessible hardware	59
D.3.5 Example demonstrating the contribution of soft errors to estimate PFH	60

Soft error kappaleen sisältö

Esa Laine

Specialist, Machinery Safety

esa.laine@sgs.com

+358 40 669 2447



Jenni Kiviaho

Product safety manager

jenni.kiviaho@valmet.com

+358 44 242 3387

