

MASINATE OHUTUS
Juhtimissüsteemide ohutusega seotud osad
Osa 1: Kavandamise üldpõhimõtted

Safety of machinery
Safety-related parts of control systems
Part 1: General principles for design
(ISO 13849-1:2023)

EESTI STANDARDI EESSÕNA

See Eesti standard on

- Euroopa standardi EN ISO 13849-1:2023 ingliskeelse teksti sisu poolest identne tõlge eesti keelde ja sellel on sama staatus mis jõustumisteate meetodil vastu võetud originaalversioonil. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;
- jõustunud Eesti standardina inglise keeles juunis 2023;
- eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2023. aasta oktoobrikuu numbris.

Standardi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 77 „Masinaohutus“, standardi tõlkimist on korraldanud Eesti Standardimis- ja Akrediteerimiskeskus.

Standardi on tõlkinud OÜ Interlex, eestikeelse kavandi ekspertiisi on teinud Rein Reisberg, standardi on heaks kiitnud EVS/TK 77.

Standardi mõnedele sätetele on lisatud Eesti olusid arvestavaid märkusi, selgitusi ja täiendusi, mis on tähistatud Eesti maatahisega EE.

Euroopa standardimisorganisatsioonid on teinud Euroopa standardi EN ISO 13849-1:2023 rahvuslikele liikmetele kättesaadavaks 17.05.2023.

Date of Availability of the European Standard EN ISO 13849-1:2023 is 17.05.2023.

See standard on Euroopa standardi EN ISO 13849-1:2023 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardimis- ja Akrediteerimiskeskus ning sellel on sama staatus ametlike keelte versioonidega.

This standard is the Estonian [et] version of the European Standard EN ISO 13849-1:2023. It was translated by the Estonian Centre for Standardisation and Accreditation. It has the same status as the official versions.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 13.110

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardimis- ja Akrediteerimiskeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autoriõiguse kaitse kohta, võtke palun ühendust Eesti Standardimis- ja Akrediteerimiskeskusega: Koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

English Version

**Safety of machinery - Safety-related parts of control
systems - Part 1: General principles for design
(ISO 13849-1:2023)**

Sécurité des machines - Parties des systèmes de
commande relatives à la sécurité - Partie 1: Principes
généraux de conception (ISO 13849-1:2023)

Sicherheit von Maschinen - Sicherheitsbezogene Teile
von Steuerungen - Teil 1: Allgemeine
Gestaltungsleitsätze (ISO 13849-1:2023)

This European Standard was approved by CEN on 3 March 2023.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

SISUKORD

EUROOPA EESSÕNA.....	5
EESSÕNA.....	6
SISSEJUHATUS.....	8
1 KÄSITLUSALA.....	11
2 NORMIVIITED.....	11
3 TERMINID, MÄÄRATLUSED, TÄHISED JA LÜHENDID	12
3.1 Terminid ja määratlused.....	12
3.2 Tähised ja lühendid.....	21
4 ÜLEVAADE.....	23
4.1 Riskihindamine ja masina riski vähendamise protsess	23
4.2 Panus riski vähendamisse	25
4.3 SRP/CS-i kavandamisprotsess.....	25
4.4 Metoodika	27
4.5 Nõutav teave	27
4.6 Ohutusfunktsiooni realiseerimine alamsüsteemide abil.....	28
5 OHUTUSFUNKTSIOONIDE SPETSIFIKATSIOON.....	28
5.1 Ohutusfunktsiooni identifitseerimine ja üldine kirjeldus.....	28
5.2 Ohutunõuete spetsifikatsioon.....	29
5.2.1 Üldnõuded.....	29
5.2.2 Nõuded konkreetsetele ohutusfunktsioonidele.....	31
5.2.3 Huvitavuse muuta ohutusfunktsioonid mittetoimivateks minimeerimine.....	35
5.2.4 Kaugjuurdepääs.....	35
5.3 Iga ohutusfunktsiooni nõutava toimivustaseme (PL _r) kindlaksmääramine	36
5.4 Ohutunõuete spetsifikatsiooni (SRS) läbivaatamine	36
5.5 SRP/CS-i jaotamine alamsüsteemideks	36
6 KAVANDAMISE KAALUTLUSED.....	38
6.1 Saavutatud toimivustaseme hindamine	38
6.1.1 Toimivustaseme üldine ülevaade.....	38
6.1.2 Korrelatsioon toimivustaseme (PL) ja ohutuse tervikluse taseme (SIL) vahel.....	39
6.1.3 Arhitektuur — Kategooriad ja nende seos iga kanali MTTF _D -iga, keskmine diagnostiline katvus ja ühisest põhjusest tulenev tõrge (CCF).....	40
6.1.4 Keskmine aeg ohtliku tõrkeni (MTTF _D).....	48
6.1.5 Diagnostiline katvus (DC).....	49
6.1.6 Ühisest põhjusest tulenevad tõrked (CCF-id)	50
6.1.7 Süstemaatilised tõrked	50
6.1.8 Lihtsustatud toimimisviis alamsüsteemide toimivustaseme hindamiseks.....	50
6.1.9 Teisene toimimisviis toimivustaseme ja PFH kindlaks määramiseks ilma MTTF _D -ita	52
6.1.10 Rikke kaalutus ja rikke välistamine	54
6.1.11 Läbiproovitud komponent.....	55
6.2 Alamsüsteemide kombinatsioon ohutusfunktsiooni üldise toimivustaseme saavutamiseks.....	55
6.2.1 Üldist.....	55
6.2.2 Teadaolevad PFH väärtused.....	56
6.2.3 Tundmatud PFH väärtused.....	56
6.3 Tarkvarapõhine käsitsi parametrizeerimine.....	57
6.3.1 Üldist.....	57
6.3.2 Mõju ohutusega seotud parameetritele.....	58
6.3.3 Nõuded tarkvarapõhisele käsitsi parametrizeerimisele	58
6.3.4 Parametrizeerimise tööriista tõestamine	59

6.3.5	Tarkvarapõhise käsitsi parametrizeerimise dokumentatsioon	59
7	TARKVARA OHUTUSNÕUDED.....	60
7.1	Üldist	60
7.2	Piiratud muutlikkusega keel (LVL) ja täieliku muutlikkusega keel (FVL)	61
7.2.1	Piiratud muutlikkusega keel (LVL).....	61
7.2.2	Täieliku muutlikkusega keel (FVL)	62
7.2.3	Otsustamine piiratud muutlikkusega keele (LVL) või täieliku muutlikkusega keele (FVL) vahel.....	62
7.3	Ohutusega seotud manustarkvara (SRESW)	64
7.3.1	Ohutusega seotud manustarkvara (SRESW) kavandamine	64
7.3.2	Teisesed toimumisviisid mittejuurdepääsetava manustarkvara puhul.....	65
7.4	Ohutusega seotud rakendustarkvara (SRASW)	65
8	SAAVUTATUD TOIMIVUSTASEME TÕESTAMINE.....	68
9	KAVANDAMISE ERGONOOMIKAASPEKTID.....	68
10	VALIDEERIMINE	68
10.1	Valideerimise põhimõtted.....	68
10.1.1	Üldist	68
10.1.2	Valideerimiskava.....	70
10.1.3	Üldiste rikete loendid.....	71
10.1.4	Konkreetsete rikete loendid.....	71
10.1.5	Teave valideerimiseks	71
10.2	Ohutusnõuete spetsifikatsiooni (SRS) valideerimine.....	72
10.3	Analüüsil põhinev valideerimine	73
10.3.1	Üldist	73
10.3.2	Analüüsimeetodid.....	73
10.4	Katsetamisel põhinev valideerimine	73
10.4.1	Üldist	73
10.4.2	Mõõtetäpsus.....	74
10.4.3	Täiendavad nõuded katsetamiseks	74
10.4.4	Katseproovide arv	74
10.4.5	Katsemeetodid	75
10.5	Ohutusfunktsioonide valideerimine	75
10.6	SRP/CS-i ohutuse tervikluse valideerimine.....	76
10.6.1	Alamsüsteemi(de) valideerimine.....	76
10.6.2	Süsteematiliste tõrgete vastu suunatud meetmete valideerimine.....	77
10.6.3	Ohutusega seotud tarkvara valideerimine.....	77
10.6.4	Alamsüsteemide kombinatsiooni valideerimine.....	78
10.6.5	Ohutuse tervikluse üldine valideerimine.....	79
10.7	Keskkonnanõuete valideerimine.....	79
10.8	Valideerimise registreering.....	79
10.9	Hooldusnõuete valideerimine	79
11	SRP/CS-I HOOLDATAVUS.....	80
12	TEHNILINE DOKUMENTATSIOON	80
13	KASUTUSTEAVE	81
13.1	Üldist	81
13.2	Teave SRP/CS-i integreerimise kohta	81
13.3	Teave kasutajale.....	82
Lisa A (teatmelisa)	Juhised nõutava toimivustaseme (PL_r) kindlaks määramiseks.....	83
Lisa B (teatmelisa)	Plokkmeetod ja ohutusega seotud plokk skeem.....	88
Lisa C (teatmelisa)	Üksikute komponentide $MTTF_D$ -i väärtuste arvutamine või hindamine.....	90

Lisa D (teatmelisa) Lihtsustatud meetod iga kanali $MTTF_D$ hindamiseks	98
Lisa E (teatmelisa) Funktsioonide ja alamsüsteemide diagnostilise katvuse (DC) hinnangud	100
Lisa F (teatmelisa) Ühisest põhjusest tulenevate tõrgete (CCF) vastaste meetmete kvantifitseerimise meetod	104
Lisa G (teatmelisa) Süstemaatiline tõrge.....	108
Lisa H (teatmelisa) Mitme alamsüsteemi kombinatsiooni näide	111
Lisa I (teatmelisa) Alamsüsteemide PL-i hinnangu lihtsustatud menetluse näited	114
Lisa J (teatmelisa) SRESW realiseerimise näide	122
Lisa K (teatmelisa) Joonise 12 numbriline esitus	126
Lisa L (teatmelisa) Elektromagnetiliste häirete (EMI) häiringukindlus	130
Lisa M (teatmelisa) Ohutuse nõuete spetsifikatsiooni (SRS) lisateave	134
Lisa N (teatmelisa) Süstemaatiliste tõrgete vältimine tarkvara kavandamisel.....	136
Lisa O (teatmelisa) Juhtimissüsteemide komponentide või osade ohutusega seotud väärtused.....	155
Lisa ZA (teatmelisa) Selle Euroopa standardi seos direktiivi 2006/42/EÜ oluliste nõuetega, mida on eesmärk katta.....	158
Kirjandus.....	160

EUROOPA EESSÕNA

Dokumendi (EN ISO 13849-1:2023) on koostanud tehniline komitee ISO/TC 199 „Safety of machinery“ koostöös tehnilise komiteega CEN/TC 114 „Safety of machinery“, mille sekretariaati haldab DIN.

Euroopa standardile tuleb anda rahvusliku standardi staatus kas identse tõlke avaldamisega või jõustumisteatega hiljemalt 2023. a novembriks ja sellega vastuolus olevad rahvuslikud standardid peavad olema kehtetuks tunnistatud hiljemalt 2026. a maiks.

Tuleb pöörata tähelepanu võimalusele, et dokumendi mõni osa võib olla patendiõiguse objekt. CEN ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest.

See dokument asendab standardit EN ISO 13849-1:2015.

Dokument on koostatud standardimistaotluse alusel, mille on Euroopa Standardimiskomitee (CEN) andnud Euroopa Komisjon ja Euroopa Vabakaubanduse Assotsiatsioon, ja see toetab EL-i direktiivi(de)/regulatsiooni(de) olulisi nõudeid.

Teave EL-i direktiivi(de)/regulatsiooni(de) kohta on esitatud teatmelisas ZA, mis on selle dokumendi lahutamatu osa.

Igasugune tagasiside ja küsimused selle dokumendi kohta tuleks suunata dokumendi kasutaja rahvuslikule standardimisorganisatsioonile / rahvuslikule komiteele. Täielik loetelu nende organisatsioonide kohta on leitav CEN-i veebilehelt.

CEN-i/CENELEC-i sisereeglite järgi peavad Euroopa standardi kasutusele võtma järgmiste riikide rahvuslikud standardimisorganisatsioonid: Austria, Belgia, Bulgaaria, Eesti, Hispaania, Holland, Horvaatia, Iirimaa, Island, Itaalia, Kreeka, Küpros, Leedu, Luksemburg, Läti, Malta, Norra, Poola, Portugal, Prantsusmaa, Põhja-Makedoonia Vabariik, Rootsi, Rumeenia, Saksamaa, Serbia, Slovakkia, Sloveenia, Soome, Šveits, Taani, Tšehhi Vabariik, Türgi, Ungari ja Ühendkuningriik.

Jõustumisteade

CEN on standardi ISO 13849-1:2023 teksti muutmata kujul üle võtnud standardina EN ISO 13849-1:2023.

EESSÕNA

ISO (International Organization for Standardization) on ülemaailmne rahvuslike standardimisorganisatsioonide (ISO rahvuslike liikmesorganisatsioonide) föderatsioon. Tavaliselt tegelevad rahvusvahelise standardi koostamisega ISO tehnilised komiteed. Kõigil rahvuslikel liikmesorganisatsioonidel, kes on mingi tehnilise komitee pädevusse kuuluvast valdkonnast huvitatud, on õigus selle komitee tegevusest osa võtta. Selles töös osalevad ka ISO-ga seotud rahvusvahelised riiklikud organisatsioonid ning vabaühendused. Kõigis elektrotehnika standardimist puudutavates küsimustes teeb ISO tihedat koostööd Rahvusvahelise Elektrotehnikakomisjoniga (IEC).

Selle dokumendi väljatöötamiseks kasutatud ja edasiseks haldamiseks mõeldud protseduurid on kirjeldatud ISO/IEC direktiivide 1. osas. Eriti tuleb silmas pidada eri heakskiidukriteeriumeid, mis on eri liiki ISO dokumentide puhul vajalikud. See dokument on kavandatud ISO/IEC direktiivide 2. osas esitatud toimetamisreeglite kohaselt (vt www.iso.org/directives).

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse objekt. ISO ei vastuta sellis(t)e patendiõigus(t)e väljaselgitamise ega selgumise eest. Dokumendi väljatöötamise jooksul väljaselgitatud või selgunud patendiõiguste üksikasjad on esitatud peatükis „Sissejuhatus“ ja/või ISO-le saadetud patentide deklaratsioonide loetelus (vt www.iso.org/patents).

Mis tahes selles dokumendis kasutatud äriline käibenimi on kasutajate abistamise eesmärgil esitatud teave ja ei kujuta endast toetusavaldust.

Selgitused standardite vabatahtliku olemuse ja vastavushindamisega seotud ISO eriomaste terminite ja väljendite kohta ning teave selle kohta, kuidas ISO järgib WTO tehniliste kaubandustõkete lepingus sätestatud põhimõtteid, on esitatud järgmisel aadressil: www.iso.org/iso/foreword.html.

Selle dokumendi on koostanud tehniline komitee ISO/TC 199 „Safety of machinery“ koostöös Euroopa Standardimiskomitee (CEN) tehnilise komiteega CEN/TC 144 „Safety of machinery“ ISO ja CEN-i vahelise tehnilise koostöö lepingu kohaselt (Viini leping).

Neljas väljaanne tühistab ja asendab kolmandat väljaannet (ISO 13849 1:2015), mis on tehniliselt läbi vaadatud.

Peamised muudatused on järgmised:

- ümber on korraldatud kogu dokument, et paremini järgida juhtimissüsteemide kavandamise ja arendustegevuse protsessi;
- uus peatükk 4 riskihindamise soovitusel kohta;
- ohutusfunktsioonide spetsifikatsioon (ajakohastatud peatükk 5);
- mitme alamsüsteemi kombinatsioon (ajakohastatud peatükis 6);
- uus peatükk 7 tarkvara ohutusnõuete kohta;
- uus peatükk 9 kavandamise ergonoomikaaspektide kohta;
- valideerimine (ajakohastatud peatükk 8 ja üle viidud peatükki 10);
- uus jaotis G.5 funktsionaalse ohutuse juhtimise kohta;
- uus lisa L elektromagnetiliste häirete (EMI) häiringukindluse kohta;
- uus lisa M koos lisateabega ohutusnõuete spetsifikatsiooni kohta;
- uus lisa N, mis käsitleb rikke vältimise meetmeid ohutusega seotud tarkvara kavandamisel;
- uus lisa O juhtimissüsteemide komponentide või osade ohutusega seotud väärtuste kohta.

Standardisarja ISO 13849 kõikide osade loetelu on leitav ISO veebilehelt.

Igasugune tagasiside ja küsimused selle dokumendi kohta tuleks suunata dokumendi kasutaja rahvuslikule standardimisorganisatsioonile. Täielik loetelu nende organisatsioonide kohta on leitav veebilehelt www.iso.org/members.html.

See dokument on EVS-i poolt loodud eelvaade

SISSEJUHATUS

Ohutusstandardite struktuur masinate valdkonnas on järgnev:

- a) A-liigi standardid (põhilised standardid) annavad põhilised kontseptsioonid, kavandamise põhimõtted ja üldised aspektid, mida võib rakendada kõikidel masinatel.
- b) B-liigi standardid (üldised ohutusstandardid) käsitlevad üht või mitut ohutusaspekti või üht või mitut liiki ohutuskaitsevahendit, mida saab kasutada masinatel laiaulatuslikult:
 - B1-liigi standardid on ohutuse teatud aspektide (nt ohutusvahemikud, pinnatemperatuurid, müra) kohta;
 - B2-liigi standardid on ohutuskaitsevahendite (nt kahekäejuhtimisseadised, blokeerimisseadised, rõhutundlikud seadised, kaitsepiirded) kohta.
- c) C-liigi standardid (masinaohutuse standardid) käsitlevad teatud masinate või masinate grupi üksikasjalikke ohutusnõudeid.

See dokument on standardis ISO 12100:2010 määratletud B1-liigi standard.

Selle dokumendi esimene väljaanne avaldati 1999. aastal standardi EN 954-1:1996 (tühistatud standard) alusel. Teine väljaanne vaadati läbi 2006. aastal ja kolmas 2015. aastal.

See dokument on asjakohane eelkõige järgnevatele huvirühmadele masinate ohutuse osas:

- masinate tootjad (väikesed, keskmised ja suured ettevõtted);
- töötervishoiu ja -ohutuse valdkonna asutused (järelevalvajad, õnnetuste ennetusega tegelevad organisatsioonid, turujärelevalve).

Teised, keda võib mõjutada masinate ohutuse tase, mis saavutatakse dokumendiga:

- masinate kasutajad / tööandjad (väikesed, keskmised ja suured ettevõtted);
- masinate kasutajad / töötajad (nt ametiühingud);
- teenuseosutajad, nt hooldusteenus (väikesed, keskmised ja suured ettevõtted);
- tarbijad (st tarbijatele kasutamiseks mõeldud masinad).

Eespool nimetatud huvirühmadele on antud võimalus selle dokumendi koostamise protsessis osaleda.

Peale selle on see dokument mõeldud standardimisasutustele, kes töötavad välja C-liigi standardeid, nagu on standardis ISO 12100:2010 määratletud.

Selle dokumendi nõudeid võib täiendada või muuta C-liigi standardiga.

Masinate puhul, mis on kaetud C-liigi standardi käsitusala ja mis on kavandatud ja ehitatud vastavalt selle standardi nõuetele, on selle C-liigi standardi nõuded prioriteetsed.

MÄRKUS 1 Enamik sisu näiteid ja aluseid põhinevad tehases rakendatud paiksetel masinatel. Samas pole välistatud ka muud masinad. Selle dokumendi koostamisel pole arvestatud teatud masinatele (nt liikurmasinadele) kehtivate erinõuetega. See dokument on siiski ette nähtud kasutamiseks paljudes masinatööstustes ja alusena C-liigi standardite väljatöötajatele, kui see on asjakohane.

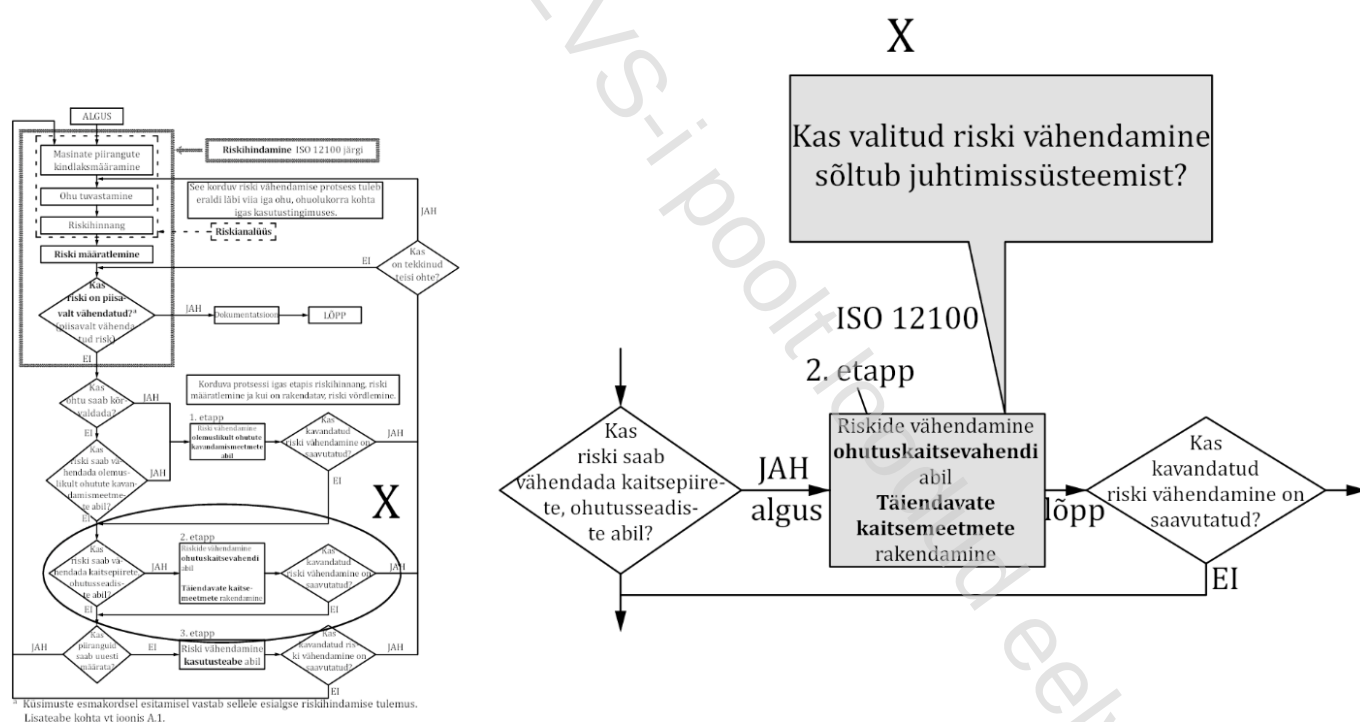
See dokument on ette nähtud andmaks juhiseid juhtimissüsteemide kavandamise ja hindamisega seotud isikutele ning B2- või C-liigi standardite koostajatele.

Riski vähendamine standardi ISO 12100:2010 6. peatüki kohaselt saavutatakse järgmises järjekorras olemuslikult ohutuid kavandamisemeid ning ohutuskaitsevahendeid ja/või täiendavaid riski vähendamise meetmeid ja kasutusteavet rakendades. Projekteerija saab riske vähendada riski vähendamise meetmetega, millel võivad olla ohutusfunktsioonid. Masina juhtimissüsteemide osi, mis on määratud täitma ohutusfunktsioone, nimetatakse juhtimissüsteemide ohutusega seotud osadeks (SRP/CS). Need võivad koosneda riistvarast või riist- ja tarkvara kombinatsioonist ning olla kas masina juhtimissüsteemist eraldiseisvad või selle lahutamatu osa. Peale ohutusfunktsioonide teostamise saab SRP/CS teostada ka toimimisfunktsioone.

Masina riskihindamisel kasutatakse standardit ISO 12100:2010. Selle dokumendi lisa A võib kasutada SRP/CS-i poolt täidetava ohutusfunktsiooni nõutava toimivustaseme (PL_r) kindlaks määramiseks juhul, kui selle PL_r pole kohaldatavas C-liiki standardis määratletud. See dokument on asjakohane SRP/CS-i ohutusfunktsioonide puhul, mida kasutatakse riskide käsitlemiseks juhtudel, kui standardi ISO 12100:2010 kohaselt läbi viidud riskihindamise käigus tehakse kindlaks, et on vaja rakendada ohutusfunktsioonile (nt blokeerivale kaitsepiirdele) tuginevat riski vähendamise meetet. Sellistel juhtudel täidab ohutusfunktsiooni ohutusega seotud juhtimissüsteem. See dokument on ette nähtud SRP/CS-i kavandamiseks ja hindamiseks. Selle dokumendi käsitlusalasasse kuulub ainult juhtimissüsteemi ohutusega seotud osa.

Joonisel 1 kujutab ISO 12100:2010 ja selle dokumendi vahelist seost. Üksikasjaliku ülevaate saamiseks vt joonist 2.

MÄRKUS 2 Lisateabe saamiseks vt ka ISO/TR 22100-2:2013.



MÄRKUS Põhineb standardi ISO/TR 22100-2:2013 joonisel 2.

Joonis 1 — Selle dokumendi (ISO 13849-1) integreerimine ISO 12100:2010 kohasesse riski vähendamise protsessi

MÄRKUS 3 Joonis 1 näitab, kus SRP/CS panustab ISO 12100:2010 2. etapi kohasesse riski vähendamise protsessi. SRP/CS toetab ohutusfunktsioonide rakendamisega kombineeritud riski vähendamise meetmeid. Juhtimissüsteemide ohutusega seotud osade võimet täita ohutusfunktsiooni ettenähtavates tingimustes liigitatakse ühte viiest tasemest, mida nimetatakse toimivustasemeteks (PL). Konkreetse ohutusfunktsiooni nõutav toimivustase (PL_r) (sõltuvalt nõutavast riski vähendamisest) määratakse kindlaks riskihinnanguga.

Selle dokumendi teatmelisa A sisaldab riskihindamise meetodit ja seda saab kasutada SRP/CS-i täidetava ohutusfunktsiooni PL_r -i kindlaks määramiseks. Hindamiskriteeriumide subjektiivsuse tõttu näitab iga riskihindamise meetod hajutatust. Lisaga A võrreldes võivad C-liigi standarditel olla masina konkreetsemate rakenduste jaoks täpsemad riskihindamise meetodid.

Ohutusfunktsiooni ohtliku tõrke sagedus sõltub mitmest tegurist, muu hulgas riist- ja tarkvara struktuurist, rikke tuvastusmehhanismide ulatusest [diagnostiline katvus (DC)], komponentide usaldusväärsusest [keskmine aeg ohtliku tõrkeni ($MTTF_D$), ühisest põhjusest tulenevast tõrkest (CCF)], kavandamisprotsessist, töökoormusest, keskkonnatingimustest ja tööprotseduuridest.

SRP/CS-i kavandamise ja saavutatud PL-i hindamise hõlbustamiseks kasutatakse selles dokumendis metoodikat, mis põhineb konkreetsete kavandamise kriteeriumidega (nt $MTTF_D$, DC_{avg}) arhitektuuride kategoriseerimisel ja määratletud käitumisel rikkeolukordades. Need arhitektuurid on liigitatud ühte viiest tasemest, mida nimetatakse kategooriateks B, 1, 2, 3 ja 4.

Funktsionaalne ohutus arvestab ohutusfunktsiooni täitvate elementide/komponentide tõrke tunnuseid. Iga ohutusfunktsiooni puhul väljendatakse seda tõrke tunnust ohtliku tõrke esinemise sagedusena tunni kohta (PFH).

Toimivustasemeid ja kategooriaid saab kohaldada SRP/CS-i suhtes, nt:

- juhtplokid (nt juhtimisfunktsioonide, andmetöötluse, seire loogikaseade);
- elektritundlikud kaitseseadised (nt fotoelektrilised tõkked), survetundlikud seadised.

Toimivustasemeid saab määratleda ja kategooriaid kindlaks määrata SRP/CS-i alamsüsteemide jaoks, kasutades ohutusosi (komponente), nt:

- ohutusseadiseid (nt kahekäejuhtimisseadised, blokeerivad seadised);
- toite juhtimiselemente (nt releed, ventiilid);
- andureid ja HMI elemente (nt asendiandurid, võimaldavad lülitid).

Selle dokumendiga hõlmatud masinad võivad ulatuda lihtsatest (nt väikesed köögimasinad või automaatsed uksed ja väravad) keerukateni (nt pakkemasinad, trükimasinad, pressid ja süsteemi integreeritud masinad).

Nii selles dokumendis kui ka standardis IEC 62061 on määratletud metoodika ning toodud sellega seotud juhised masinate ohutusega seotud juhtimissüsteemide kavandamiseks ja rakendamiseks.

Selle dokumendi peatüki 10 nõuded asendavad standardis ISO 13849-2:2012 toodud nõudeid (välja arvatud teatmelisad).

1 KÄSITLUSALA

See dokument määratleb metoodika ning esitab ohutusfunktsioone täitvate juhtimissüsteemide ohutusega seotud osade (SRP/CS) kavandamiseks ja integreerimiseks vajalikud nõuded, soovitusel ja juhised, sealhulgas tarkvara kavandamiseks.

Seda dokumenti kohaldatakse suure nõutavuse ja pidevate töörežiimide SRP/CS-ile, sealhulgas nende alamsüsteemidele, olenemata tehnoloogia ja energia liigist (nt elektrilised, hüdraulilised, pneumaatilised ja mehaanilised). Dokument ei kohaldu väikese nõutavusega töörežiimile.

MÄRKUS 1 Väikese nõutavusega töörežiimi kohta vt jaotist 3.1.44 ja standardisarja IEC 61508.

Selles dokumendis ei täpsustata konkreetsetes rakendustes kasutatavaid ohutusfunktsioone ega nõutavaid toimivustasemeid (PL_r).

MÄRKUS 2 Selles dokumendis määratletakse SRP/CS-i kavandamise metoodikat, arvesse võtmata seda, kui teatud masinatel (nt liikurmasinatel) on erinõuded. Neid erinõudeid võib käsitleda C-liigi standardis.

Selles dokumendis ei esitata erinõudeid SRP/CS-i osaks olevate toodete/komponentide kavandamiseks. Teatud SRP/CS-i komponentide kavandamise erinõuded on hõlmatud kohaldatavate ISO ja IEC standarditega.

Selles dokumendis ei sätestata turvaaspektide (nt füüsiline, infoturve, küberturvalisus) erimeetmeid.

MÄRKUS 3 Turvalisusega seotud probleemid võivad ohutusfunktsioone mõjutada. Lisateabe saamiseks vt ISO/TR 22100-4 ja IEC/TR 63074.

2 NORMIVIITED

Allpool nimetatud dokumentidele on tekstis viidatud selliselt, et nende sisu kujutab endast kas osaliselt või tervenisti selle dokumendi nõudeid. Dateeritud viidete korral kehtib üksnes viidatud väljaanne. Dateerimata viidete korral kehtib viidatud dokumendi uusim väljaanne koos võimalike muudatustega.

ISO 12100:2010. Safety of machinery — General principles for design — Risk assessment and risk reduction

ISO 13849-2:2012. Safety of machinery — Safety-related parts of control systems — Part 2: Validation

ISO 13855:2010. Safety of machinery — Positioning of safeguards with respect to the approach speeds of parts of the human body

ISO 20607:2019. Safety of machinery — Instruction handbook — General drafting principles

IEC 61508-3:2010. Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 3: Software requirements

IEC 62046:2018. Safety of machinery — Application of protective equipment to detect the presence of persons

IEC 62061:2021. Safety of machinery — Functional safety of safety-related control systems

IEC/IEEE 82079-1:2019. Preparation of information for use (instructions for use) of products — Part 1: Principles and general requirements