

MASINAOHUTUS

Seos standardiga ISO 12100

**Osa 4: Juhend masinatootjatele IT-turvalisuse
(küberturvalisuse) aspektide arvesse võtmiseks**

Safety of machinery

Relationship with ISO 12100

**Part 4: Guidance to machinery manufacturers for
consideration of related IT-security (cyber security)
aspects
(ISO/TR 22100-4:2018)**

EESSÕNA TEHNILISE ARUANDE EESTIKEELSELE VÄLJAANDELE

See väljaanne on

- CEN-i tehnilise aruande CEN ISO/TR 22100-4:2020 ingliskeelse teksti sisu poolest identne tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;
- eesti keeles avaldatud sellekohase teate ilmunisega EVS Teataja 2025. aasta septembrikuu numbris.

Dokumendi tõlke koostamise ettepaneku on esitanud tehniline komitee EVS/TK 77 „Masinaohutus“, dokumendi tõlkimist on korraldanud Eesti Standardimis- ja Akrediteerimiskeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

Dokumendi on tõlkinud Rein Reisberg, dokumendi on heaks kiitnud EVS/TK 77.

Euroopa standardimisorganisatsioon on teinud CEN-i tehnilise aruande CEN ISO/TR 22100-4:2020 rahvuslikele liikmetele kättesaadavaks 08.04.2020.

Date of Availability of the CEN Technical Report CEN ISO/TR 22100-4:2020 is 08.04.2020.

See dokument on CEN-i tehnilise aruande CEN ISO/TR 22100-4:2020 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardimis- ja Akrediteerimiskeskus.

This document is the Estonian [et] version of the CEN Technical Report CEN ISO/TR 22100-4:2020. It was translated by the Estonian Centre for Standardisation and Accreditation.

Tagasisidet tehnilise aruande 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 - Relationship with ISO 12100 - Part 4:
Guidance to machinery manufacturers for consideration of
related IT-security (cyber security) aspects
(ISO/TR 22100-4:2018)**

Sécurité des machines - Relation avec l'ISO 12100 -
Partie 4: Titre manque (ISO/TR 22100-4:2018)

This Technical Report was approved by CEN on 6 April 2020. It has been drawn up by the Technical Committee CEN/TC 114.

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, Turkey 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.....	3
EESSÕNA.....	4
SISSEJUHATUS.....	5
1 KÄSITLUSALA.....	6
2 NORMIVIITED.....	6
3 TERMINID JA MÄÄRATLUSED.....	6
4 MASINAOHUTUSE ÜLDINE ISELOOMUSTUS VÕRRELDES IT-TURVALISUSEGA.....	8
4.1 Põhieesmärgid.....	8
4.2 Riski erinevad elemendid.....	9
4.3 Riskihindamise protsessi järelused.....	10
5 SEOS OLEMASOLEVA MASINAOHUTUST KÄSITLEVA ÕIGUSLIKU JA STANDARDIMISE RAAMISTIKUGA.....	10
5.1 Õiguslik raamistik.....	10
5.2 Standardimise raamistik – seos standardiga ISO 12100.....	10
6 MASINAOHUTUSE JA IT-TURVALISUSE VAHELINE SEOS.....	11
7 OLULISED SAMMUD IT-TURVALISUSEGA TEGELEMISEKS KOGU MASINA ELUTSÜKLI JOOKSUL.....	12
8 ÜLDINE JUHEND IT-TURVALISUSE OHTUDE HINDAMISEKS SEOSSES NENDE VÕIMALIKU MÕJUGA MASINAOHUTUSELE.....	13
9 ROLLID MASINAOHUTUSELE OLULISTE IT-TURVALISUSE PROBLEEMIDEGA TEGELEMISEKS.....	14
10 JUHEND MASINATOOTJATELE IT-TURVALISUSE PROBLEEMIDEGA, MIS VÕIVAD OLLA SEOTUD MASINAOHUTUSEGA, TEGELEMISEKS.....	17
10.1 Üldist.....	17
10.2 Sobivate komponentide (riistvara/tarkvara) valimine.....	17
10.3 Sobiv masina kavandamine.....	18
10.4 Kasutuskäsiraamat (juhised masina kasutajale).....	18
Lisa A (teatmelisa) Õigusliku raamistiku näide.....	20
Kirjandus.....	21

EUROOPA EESSÕNA

Dokumendi (ISO/TR 22100-4:2018) on koostanud Rahvusvahelise Standardimisorganisatsiooni (ISO) tehniline komitee ISO/TC 199 „Safety of machinery“ ning tehniline komitee CEN/TC 114 „Safety of machinery“, mille sekretariaati haldab DIN, on selle üle võtnud kui CEN ISO/TR 22100-4:2020.

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.

Jõustumisteade

CEN on dokumendi ISO/TR 22100-4:2018 teksti muutmata kujul üle võtnud kui CEN ISO/TR 22100-4:2020.

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 dokumendi 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 kasutuse 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“.

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

Täielik loetelu kõikide ISO 22100 sarja osade kohta on leitav ISO veebilehelt.

SISSEJUHATUS

Internet, digitaalsed teenused ja tehnoloogia on olulised nutitootmise võimaldajad, mis on üks osa asjade internetist (IoT) (vt standard ISO/IEC 20924). Tootmiskeskonna alustalad on vertikaalne võrgustik ja horisontaalne integratsioon läbi kogu väärtusahela, kavandamise, tellimise, tarnimise ja tootmisvõimaluste koondumisel. See toob kaasa tavapäraste väärtusahelate ümberkujundamise ja uute ärimudelite esile tuleku. Nutitootmisel põhinevad nutitooted teavad palju üksikasju selle kohta, kuidas need on valmistatud, nende toimivust ja kuidas neid kasutatakse. Füüsiline toode on seotud oma digitaalse esitusega ja digitaalne sisu sõltub elutsükli faasist. Nutitootmise rakendamine loob tõhusa ja väga reageerimisvõimelise paketi, kasutades ära olemasolevaid tootmissüsteeme ning tehnoloogilist ja majanduslikku potentsiaali. Nutitootmine suurendab masinate nõrkust IT-turvalisuse ohtude suhtes.

Nutitootmine viib dünaamiliste, reaajas optimeeritud ja iseorganiseeruvate väärtusahelate esiletulekuni. Seetõttu on vajalik sobiv regulatiivne raamistik, samuti standarditud liidesed ja ühtlustatud äriprotsessid. Nutitootmist iseloomustavad

- a) suurem toote paindlikkus;
- b) uued olemuslikud sisseehitatud tooteomadused;
- c) paindlik töökorraldus;
- d) muutunud tootmise maht (kuni partii suuruseni 1) ja asukoht.

Nutitootmise jaoks tuleb võrgu infrastruktuuri kirjeldust veelgi laiendada, et võimaldada privaatsust, isekonfigureerimist ja kasutusmugavust. Seetõttu on vaja kiiresti kättesaadavaid, jõulisi ja turvalisi sidevõrke.

Selle dokumendi peamine eesmärk on tegeleda masinaohutuse aspektidega, mida võivad mõjutada IT-turvalisuse ründed, mis on seotud isikute otsese või kaugpääsuga ohutusega seotud juhtimissüsteemi(de)le ja selle (nende) manipuleerimisega tahtliku kuritarvitamise (mittesihotstarbelise kasutamise) eesmärgil. IT-turvalisuse ründed on üha enam potentsiaalne oht masinaohutusele. Kuigi tahtlik kuritarvitamine jääb standardi ISO 12100 ja (ohutusega seotud) riskihindamise protsessi käsitusalt välja, on mõistlik, et ka masinate tootjad arvestaksid selliste ohtudega.

Praegused tehnoloogiad võimaldavad masinaid kaugjuhtimise teel jälgida ja/või nende jõudlust parendada, kohandades parameetreid ilma masina juures kohapeal olemata. See võime pakub märkimisväärsed eeliseid, kuna masinaid saab töökorras hoida ilma seisakuajata ja hooldustöötaja kohapeale väljakutsumise kuludeta.

Ent sama võime kohandada masina parameetreid jõudluse parendamiseks võimaldab iseenesest pahatahtlike või kuritegelike kavatsustega isikutel teha kohandusi, mis võivad panna töötajad ja teised kahjustuse tekkimise riski. Näiteks saab kiirust või jõudu reguleerida ohtlikule tasemele, temperatuuri langetada alla kriitilise kontrollpunkti määratud piiri, mis põhjustab toidu saastumist, või veakode või -teateid kustutada või võltsida.

Inimlikel vigadel on IT-turvalisusega selle kitsamas tähenduses vähe pistmist. Need ettekavatsematud mõjutused (mõistlikult ettenähtavad inimlikud vead masina või selle juhtimissüsteemi parameetrite kohandamisel) on juba hõlmatud tavapärase (ohutusega seotud) riskihindamise ja sellest tuleneva juhtimissüsteemi loomupäraselt ohutu konstruktsiooniga (vt ISO 12100:2010 jaotis 6.2.11.1).

1 KÄSITLUSALA

See dokument annab masinatootjatele juhendi masinaohutusega seotud võimalike turvalisuse aspektide kohta masina kasutuselevõtul või esmakordsel turule laskmisel. See annab olulist teavet IT-turvalisuse ohtude, mis võivad masinaohutust mõjutada, tuvastamiseks ja nendega tegelemiseks.

See dokument annab juhendi, kuid ei esita üksikasjalikke spetsifikatsioone selle kohta, kuidas tegeleda IT-turvalisuse aspektidega, mis võivad mõjutada masinaohutust.

See dokument ei käsitle riski vähendamise meetmetest mööda minemist või nende mittetoimivaks muutmist füüsilise manipuleerimise teel.

2 NORMIVIITED

Allpool nimetatud dokumendid, mille kohta on selles dokumendis esitatud normiviited, on kas tervenisti või osaliselt vajalikud selle rakendamiseks. 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

3 TERMINID JA MÄÄRATLUSED

Dokumendi rakendamisel kasutatakse standardis ISO 12100 ning allpool esitatud termineid ja määratlusi.

ISO ja IEC hoiavad alal standardimisel kasutamiseks olevaid terminoloogilisi andmebaase järgmistel aadressidel:

- ISO veebipõhine lugemisplatvorm: kättesaadav veebilehelt <https://www.iso.org/obp/>;
- IEC Electropedia: kättesaadav veebilehelt <http://www.electropedia.org/>.

3.1

viirusetõrjevahend (*antivirus tool*)

tarkvara, mida kasutatakse pahatahtliku koodi tuvastamiseks, sellega süsteemi nakatamise vältimiseks ja süsteemi nakatanud pahatahtliku koodi eemaldamiseks

3.2

rünne (*attack*)

katse saada volitamata pääsu süsteemiteenustele, ressurssidele või teabele

[ALLIKAS: CNSSI-4009, muudetud — „... or an attempt to compromise system integrity, availability, or confidentiality“ on määratluse lõpust kustutatud.]

3.3

autentimine (*authentication*)

kasutaja, protsessi või seadme identiteedi tõendamine, mis on sageli eeltingimus infosüsteemi ressurssidele pääsu lubamiseks

[ALLIKAS: NIST SP 800-53]

3.4

volitamine (*authorization*)

süsteemiolemile tagatud õigus või luba süsteemiressursile pääsuks