Avaldatud eesti keeles: aprill 2014
Jõustunud Eesti standardina: veebruar 2009

TARNEAHELA TURVALISUSE JUHTIMISSÜSTEEMIDE SPETSIFIKATSIOON

Specification for security management systems for the supply chain (ISO 28000:2007)

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

See Eesti standard on

— rahvusvahelise standardi ISO 28000:2007 ingliskeelse teksti sisu poolest identne tõlge eesti keelde. Tõlgenduserimeelsuste korral tuleb lähtuda ametlikes keeltes avaldatud tekstidest;

— jõustunud Eesti standardina inglise keeles veebruaris 2009;

— eesti keeles avaldatud sellekohase teate ilmumisega EVS Teataja 2014. aasta aprillikuu numbris.

Standardi on tõlkinud TJO Konsultatsioonid OÜ, standardi on heaks kiitnud tehniline komitee EVS/TK 33 „Juhtimissüsteemid".

Standardi tõlke koostamise ettepaneku on esitanud EVS/TK 33, standardi tõlkimist on korraldanud Eesti Standardikeskus ning rahastanud Majandus- ja Kommunikatsiooniministeerium.

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

See standard on rahvusvahelise standardi ISO 28000:2007 eestikeelne [et] versioon. Teksti tõlke on avaldanud Eesti Standardikeskus ja sellel on sama staatus ametlike keelte versioonidega.

This standard is the Estonian [et] version of the International Standard ISO 28000:2007. It has been translated by the Estonian Centre for Standardisation. 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 47.020.99 Muud laevaehituse ja mereehitistega seotud standardid

SISUKORD

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 käsikäes ISO-ga ka rahvusvahelised, riiklikud ja valitsusvälised organisatsioonid. Kõigis elektrotehnika standardimist puudutavates küsimustes teeb ISO tihedat koostööd Rahvusvahelise Elektrotehnikakomisjoniga (IEC).

Rahvusvahelised standardid kavandatakse ISO/IEC direktiivide 2. osas esitatud reeglite kohaselt.

Tehniliste komiteede põhiülesanne on rahvusvaheliste standardite koostamine. Tehnilistes komiteedes vastuvõetud rahvusvahelised standardikavandid saadetakse hääletamiseks rahvuslikele liikmesorganisatsioonidele. Avaldamine rahvusvahelise standardina nõuab, et hääletusel osalenud rahvuslikest liikmesorganisatsioonidest kiidaks selle heaks vähemalt 75 %.

Tuleb pöörata tähelepanu võimalusele, et standardi mõni osa võib olla patendiõiguse subjekt. ISO-t ei saa pidada vastutavaks sellis(t)e patendiõigus(t)e väljaselgitamise eest.

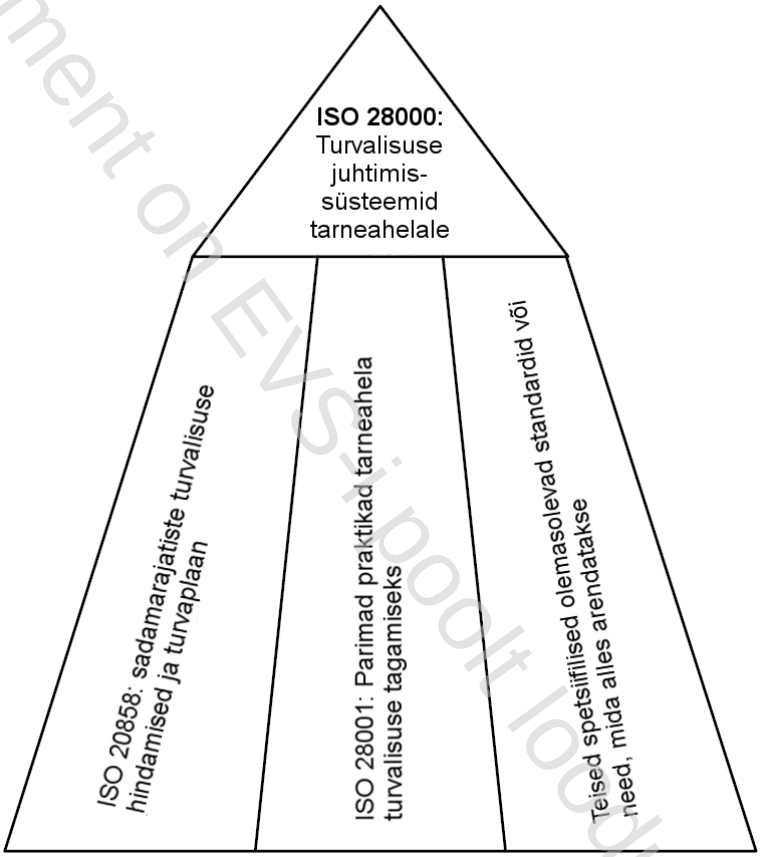
ISO 28000 on koostanud tehniline komitee ISO/TC 8 („Laevad ja meretehnoloogia“) koostöös teiste asjakohaste tehniliste komiteedega, kes vastutavad tarneahela spetsiifiliste sõlmpunktide eest.

ISO 28000 esimene väljaanne asendab dokumenti ISO/PAS 28000:2005, mis on tehniliselt üle vaadatud.

SISSEJUHATUS

See rahvusvaheline standard on töötatud välja vastusena tööstuse nõudlusele turvalisuse juhtimise standardi järele. Selle põhiliseks eesmärgiks on parendada tarneahelate turvalisust. See on kõrgema astme juhtimisstandard, mis võimaldab organisatsioonil sisse seada üldise tarneahela turvalisuse juhtimissüsteemi. See nõuab organisatsioonilt turvalisuse keskkonna hindamist ja määratlemist oma tegevusalal, kas piisavad turvameetmed on rakendatud ja kas on olemas teisi regulatiivseid nõudeid, millele organisatsioon vastab. Kui turvalisuse vajadused on selle protsessiga tuvastatud, siis peaksid organisatsioonid viima ellu mehhanismid ja protsessid nende vajaduste rahuldamiseks.

Kuna tarneahelad on oma olemuselt dünaamilised, siis võib mõni organisatsioon, kes juhib mitut tarneahelat, otsida oma teenusepakkujate hulgast selliseid, kes vastaksid riiklikele või ISO tarneahela turvalisuse standardite nõuetele. See oleks tarneahelasse kaasamise tingimuseks, et lihtsustada turvalisuse juhtimist, nagu on näidatud joonisel 1.



Joonis 1 — Seosed ISO 28000 ja teiste asjakohaste standardite vahel

See standard on mõeldud kohaldamiseks juhtudel, kus nõutakse organisatsiooni tarneahela juhtimist turvalisel viisil. Ametlik lähenemine turvalisuse juhtimisele võib otseselt kaasa aidata organisatsiooni ärialasele suutlikkusele ja usaldusväärsusele.

Vastavus sellele rahvusvahelisele standardile ei anna iseenesest immuunsust õiguslike kohustuste ees. Organisatsioonid, kes seda soovivad, võivad lasta hinnata oma turvalisuse juhtimissüsteemi vastavust sellele rahvusvahelisele standardile välise või sisemise auditi käigus.

Seoses riskipõhise lähenemisega juhtimissüsteemidele põhineb see standard ISO formaadil, mis on kohandatud standardist ISO 14001:2004. Sellele vaatamata võivad organisatsioonid, kes on kohandunud protsessipõhise lähenemisega juhtimissüsteemidele (nt ISO 9001:2000), kasutada oma olemasolevat juhtimissüsteemi selles standardis sätestatud turvalisuse juhtimissüsteemi alusena. Selle standardi kavatsuseks ei ole dubleerida valitsuse kehtestatud nõudeid ega tarneahela turvalisuse juhtimisega seonduvaid standardeid, mille suhtes on organisatsioonid juba sertifitseeritud või vastavaks tunnistatud. Nõuetekohasust võib kontrollida aktsepteeritav esimene, teine või kolmas osapool.

MÄRKUS See rahvusvaheline standard põhineb tuntud Planeeri-Tee-Kontrolli-Parenda (PDCA) metoodikal. PDCA-d võib kirjeldada järgmiselt:

— Planeeri: sea sisse eesmärgid ja protsessid, mis on vajalikud organisatsiooni turvapoliitikale vastavate tulemuste saavutamiseks.

— Tee: vii protsessid ellu.

— Kontrolli: jälgi ja mõõda protsesside vastavust turvapoliitikale, eesmärkidele, ülesannetele, õigusaktidele jm nõuetele, ning raporteeri tulemustest.

— Parenda: võta ette tegevused turvalisuse juhtimissüsteemi toimimise pidevaks parendamiseks.

1 KÄSITLUSALA

See rahvusvaheline standard määrab kindlaks nõuded turvalisuse juhtimissüsteemile, sealhulgas tarneahela turvalisuse tagamise seisukohast kriitiliste aspektide jaoks. Turvalisuse juhtimine on seotud paljude muude ärijuhtimise aspektidega. Need aspektid puudutavad kõiki tegevusi, mida organisatsioon saab ohjata ja mõjutada ning millel on mõju tarneahela turvalisusele. Nimetatud muude aspektide osas tuleks kaaluda vahetult, kus ja millal need mõjutavad turvalisuse juhtimist, sealhulgas kõnealuste kaupade transportimist tarneahelas.

Standard on kohaldatav tootmises, teeninduses, ladustamises ja transpordis igas suuruses organisatsioonide, alates väikestest kuni rahvusvahelisteni, tootmis- või tarneahela mistahes etapis, kui tootmis- või tarneahela eesmärgiks on:

a) sisse seada, ellu viia, toimivana hoida ja parendada turvalisuse juhtimissüsteemi;

b) tagada vastavus fikseeritud turvalisuse juhtimispoliitikale;

c) demonstreerida nimetatud vastavust teistele;

d) taotleda, et kolmanda osapoole akrediteeritud sertifitseerimisasutus sertifitseeriks/registreeriks turvalisuse juhtimissüsteemi; või

e) määrata või deklareerida ise vastavust sellele standardile.

On olemas seadusandlikke ja regulatiivseid reegleid, mis käsitlevad mõningaid selle rahvusvahelise standardi nõudeid.

Standardi eesmärk ei ole nõuda vastavuse dubleerivat demonstreerimist.

Kolmanda osapoole sertifitseerimise valinud organisatsioonidel on võimalik edaspidi demonstreerida oma märkimisväärset panust tarneahela turvalisusele.

2 NORMIVIITED

Normiviited puuduvad. Selle peatüki lisamise eesmärk on tagada samane numeratsioon teiste juhtimissüsteemide standarditega.

3 TERMINID JA MÄÄRATLUSED

Standardi rakendamisel kasutatakse alljärgnevalt esitatud termineid ja määratlusi.

3.1
rajatis (*facility*)
tehas, masinad, kinnisvara, ehitised, sõidukid, laevad, sadamarajatised ja muud infrastruktuuri või tehase ning nendega seotud süsteemide osad, millel on spetsiifilised ja mõõdetavad ärifunktsioonid või teenused

MÄRKUS See mõiste hõlmab mistahes turvalise tarne ja turvalisuse juhtimise rakenduse seisukohalt olulist tarkvarakoodi.

3.2
turvalisus (*security*)
vastupanu tahtlikule (tahtlikele) lubamatule teole (lubamatutele tegudele), mille eesmärk on kahjustada või vigastada tarneahelat või põhjustada tarneahela kaudu kahjustusi või vigastusi

3.3
turvalisuse juhtimine (*security management*)
süstemaatilised ja koordineeritud tegevused ja tavad, mille kaudu organisatsioon juhib optimaalselt oma riske ja nendega seotud potentsiaalseid ohte ning nende mõjusid