

HZN **e**glasilo

Broj 5/2025

Službeno glasilo Hrvatskoga zavoda za norme



korjenite promjene
u zaštiti na radu:

uloga **umjetne inteligencije i**
digitalizacije u radu.



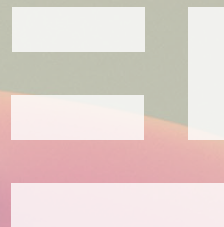
HZN/TO 159,
Ergonomija

HZN/TO 556,
Osobna zaštitna oprema

HZN/TO 557,
Zaštitna odjeća

HZN/TO 558,
Zaštita dišnih putova

Svjetski dan
sigurnosti i
zdravlja na
radu
/
2025



HZN e-glasilo

Službeno glasilo Hrvatskog zavoda za norme sa
stalnim dodatkom
Oglasnik za normativne dokumente

Godište: 17. 2025.
ISSN 1847-4217
URL: <http://www.hzn.hr>

Izdavač: Hrvatski zavod za norme
MB: 1957406
OIB: 76844168802
Sjedište: Ulica grada Vukovara 78,
10000 Zagreb
Telefon: 01/610 60 95
Telefax: 01/610 93 21

Glavni
urednik: Igor Božičević, v.d. ravnatelja HZN-a

Pomoćnik
glavnog
urednika: Sandra Knežević

Tehnički
urednik: Sandra Knežević

Uredništvo: Ana Marija Boljanović, Ivo Andreis,
Marina Babić, Melanija Grubić Sutara,
Tatjana Majić

Lektura: Kristian Lewis

Grafička
priprema: Sandra Knežević

Izlazi: mjesečno

Datum
objave: 2025-05-31

Opremu tekstova obavlja uredništvo. Za sadržaj poimence potpisanih priloga odgovorni su njihovi autori. Oni ne iskazuju obvezno stav Hrvatskoga zavoda za norme. Objavljeni prilozi u službenom glasilu Hrvatskog zavoda za norme autorski su zaštićeni. Iznimka su sadržaj, novosti iz HZN, novosti iz europskih i međunarodnih normiranih tijela i s normizacijom povezane aktivnosti koji se mogu objavljivati u drugim stručnim časopisima uz obveznu naznaku izvora i dostavljanje časopisa u kojemu su objavljeni tako preuzeti prilozi. Za priloge iz rubrike Normizacija i Tehničko zakonodavstvo potrebno je zatražiti pisano odobrenje za njihovo objavljivanje od autora i od Hrvatskoga zavoda za norme.

Poštovani čitatelji!

Pred vama je peti broj službenoga glasila Hrvatskog zavoda za norme u 2025. godini.

Donosimo prigodni tekst u povodu obilježavanja Svjetskog dana sigurnosti i zdravlja na radu, koji se obilježava 28. travnja.

Kao i u svakom broju, u rubrici Novosti iz HZN-a nalazi se tablica u kojoj je dan brožčani prikaz članstva u Hrvatskom zavodu za norme.

U rubrici Novosti iz međunarodnih i europskih normizacijskih organizacija možete pročitati zanimljivosti iz rada ISO-a, IEC-a, CEN-a, CENELEC-a i ETSI-ja.

Tu je i prilog o novim izdanjima ISO-ovih norma.

CEN-ov tehnički odbor CEN/TC 278, *Intelligent Transport Systems*, izradio je normu EN 16072:2025, *Intelligent transport systems – ESafety – Pan-European eCall operating requirements*, kojom se utvrđuju operativni zahtjevi za e-poziv, automatski sustav za hitne pozive iz vozila koji se spajaju izravno s hitnim službama. Da bi e-poziv zaista postao sveeuropski, vozila i pozivni centri za hitne slučajeve u svim članicama EU-a moraju „govoriti” istim stručnim jezikom. Tu ulogu ima norma EN 16072:2025.

U svijetu koji se sve više digitalizira važnije je nego ikad osigurati pouzdano visoku kibernetičku sigurnost u složenim sustavima s više dionika. Nova europska norma EN 18037:2025, *Guidelines on a sectoral cybersecurity assessment*, koju je izradio tehnički odbor JTC 13, *Cybersecurity and Data Protection*, odgovor je na tu potrebu.

CENELEC je objavio novu važnu normu za željeznice EN 50388-2:2025 – novi alat za koordinaciju sustava napajanja električne vuče i željezničkih vozila.

Donosimo prijevod IEC-ova članka *Standards to power our planet on Earth Day* u kojemu je istaknuta vrijednost norma u mjerama i poticajima za borbu protiv klimatskih promjena kako bi se Dan planeta Zemlje mogao zaista slaviti.

ETSI je izradio tehničku specifikaciju ETSI TS 104 22 kojom se utvrđuje mjerilo za osiguravanje sustava umjetne inteligencije (UI) u kontekstu sve većih prijetnji kibernetičkoj sigurnosti. Više informacija pronađite u prijevodu članka *ETSI Technical Specification sets international benchmark for securing Artificial Intelligence*.

Ugodno čitanje!

Sadržaj 5/2025

Proslov

- Svjetski dan sigurnosti i zdravlja na radu 2025. 4

Novosti iz HZN-a

- Članovi Hrvatskog zavoda za norme 6

Novosti iz HZN/TO-a

- Poziv za uključivanje u rad tehničkog pododbora HZN/TO T4/PO 1, *Normizacija u telekomunikacijama; Kvantna i kvantno otporna kibernetička sigurnost* 7

Novosti iz međunarodnih i europskih normizacijskih organizacija

ISO

- Trendovi u normama 8

IEC

- Norme za energiju našeg planeta na Dan planeta Zemlje 10

CEN i CENELEC

- Pristup sektorskoj kibernetičkoj sigurnosti koji se temelji na riziku: Uvod u EN 18037:2025 11
- Sveeuropski e-poziv: kad automobili zovu upomoć 13

ETSI

- ETSI-jeva tehnička specifikacija postavlja međunarodno mjerilo za osiguravanje umjetne inteligencije 15

Naslovnica: *Poster povodom obilježavanja Svjetskog dana sigurnosti i zdravlja na radu - 28. travnja.*

HZN Oglasnik za normativne dokumente (A1-A51)

ISSN 1847-4217

Svjetski dan sigurnosti i zdravlja na radu 2025.

„Korjenite promjene u zaštiti na radu: uloga umjetne inteligencije i digitalizacije u radu” tema je ovogodišnjeg Svjetskog dana sigurnosti i zdravlja na radu, koji se obilježava 28. travnja.

Digitalizacija i automatizacija transformiraju milijune radnih mjesta diljem svijeta stvarajući snažne prilike za poboljšanje sigurnosti i zdravlja na radu. Automatizacijom i sustavima pametnog praćenja može se smanjiti opasna izloženost, spriječiti ozljede i poboljšati opći radni uvjeti. Međutim, napretkom se stvaraju i novi rizici koji zahtijevaju proaktivne i prilagodljive mjere.

Dok roboti preuzimaju opasne poslove, radnicima koji ih održavaju, popravljaju ili surađuju s njima prijete nove opasnosti. Nepredvidljivo ponašanje robota, kvarovi sustava ili kibernetičke prijetnje ugrožavaju sigurnost. Interakcijom čovjeka i robota i upotrebom nosivih elemenata i egzoskeleta koji ne pristaju dovoljno dobro, nisu praktični ili udobni mogu nastati ergonomski rizici. Zbog prekomjernog oslanjanja na umjetnu inteligenciju i automatizaciju smanjuje se ljudski

nadzor i time povećaju rizici za sigurnost i zdravlje na radu, a zadaci utemeljeni na algoritmima i stalnoj komunikaciji mogu pridonijeti stresu, izgaranju i problemima mentalnog zdravlja.

Politike i propisi diljem svijeta sve više uključuju nove mjere koje obuhvaćaju sigurnost robota i interakciju čovjeka i robota, pravo na isključivanje, poboljšano algoritamsko upravljanje radom te siguran rad na daljinu i rad na platformama.

U svakoj fazi prihvatanja tehnologija bitna je uključenost radnika. Za bezopasnu primjenu novih tehnologija nužne su inicijative za osposobljavanje i podizanje svijesti. Da bi se u potpunosti razumjeli dugoročni učinci digitalne transformacije na sigurnost i zdravlje na radu, bit će potrebna daljnja istraživanja.

Unatoč znatnom napretku u području sigurnosti i zdravlja na radu (OSH), nesreće i bolesti povezane s radom i dalje se prečesto događaju, što ima razoran učinak na radnike, poduzeća te cijele zajednice i gospodarstvo.

“

- **2,93 milijuna radnika godišnje izgubi život zbog uzroka povezanih s radom**

[A call for safer and healthier working environments \(ILO 2023\)](#)

- **395 milijuna radnika godišnje pretrpi ozljedu na radu bez smrtno posljedicu**

[A call for safer and healthier working environments \(ILO 2023\)](#)

- **2,41 milijarda radnika godišnje izložena je prekomjernoj vrućini**

[Ensuring safety and health at work in a changing climate \(ILO 2024\)](#)

- **361 milijarda dolara iznosi ušteda koja bi se mogla ostvariti na globalnoj razini provedbom poboljšanih mjera za sprječavanje ozljeda uzrokovanih prekomjernom vrućinom na radnom mjestu**

[Heat at work: Implications for safety and health \(ILO 2024\)](#)



Izvor: ILO
Priredila: Sandra Knežević
Prijevod: Tatjana Majić

Hrvatske norme iz područja sigurnosti i zaštite zdravlja na radu izrađuju sljedeći tehnički odbori Hrvatskoga zavoda za norme:

HZN/TO 159, *Ergonomija*

HZN/TO 556, *Osobna zaštitna oprema*

HZN/TO 557, *Zaštitna odjeća*

HZN/TO 558, *Zaštita dišnih putova*

Za dodatne obavijesti o radu navedenih odbora možete se obratiti:

Boženi Mesek, višoj stručnoj savjetnici za normizaciju u području zdravlja, okoliša i medicinske opreme (bozena.mesek@hzn.hr)

Detaljnije informacije o hrvatskim normama koje su izradili i prihvatili navedeni tehnički odbori možete pronaći u [katalogu hrvatskih norma](#) te [repozitoriju HRN4You](#).

Za besplatan uvid u sadržaj norma možete najaviti svoj dolazak u [normoteku](#), a za kupnju navedenih norma ili bilo kojega normativnog dokumenta pošaljite popunjeni [obrazac za ponude](#) na e-adresu prodaja@hzn.hr.



HZN

Hrvatski zavod za norme
Croatian Standards Institute



International
Labour
Organization

#safety2025

Revolutionizing OSH through AI and digitalization



Članovi Hrvatskog zavoda za norme

Objavljujemo popis redovitih članova i članova promatrača HZN-a po vrstama pravnih odnosno fizičkih osoba za koje je Upravno vijeće donijelo odluke u travnju 2025. godine.

Tablica Članovi Hrvatskog zavoda za norme identična je tablici objavljenoj u prethodnom broju HZN e-glasila jer od travnja 2025. godine nije bilo promjena.

Tablica – Članovi Hrvatskog zavoda za norme

Vrsta članstva, vrsta pravne ili fizičke osobe	2025-04-30
Članovi promatrači	
Pravne osobe koje ostvaruju dobit	6
Pravne osobe koje ne ostvaruju dobit – visokoškolske ustanove	1
Fizičke osobe	0
Ukupno članova promatrača	7
Redoviti članovi	
Pravne osobe koje ostvaruju dobit	162
Pravne osobe koje ne ostvaruju dobit – javne ustanove	17
Pravne osobe koje ne ostvaruju dobit – HGK, HOK, HUP	1
Pravne osobe koje ne ostvaruju dobit – strukovne komore i udruženja registrirana u Sudskom registru	6
Pravne osobe koje ne ostvaruju dobit – strukovna društva i udruge osnovane prema Zakonu o udrugama i registrirane u Registru udruga	11
Pravne osobe koje ne ostvaruju dobit – osnovne i srednje škole	2
Pravne osobe koje ne ostvaruju dobit – visokoškolske ustanove	22
Fizičke osobe – pojedinci	20
Fizičke osobe – obrtnici	2
Tijela državne uprave	25
Ukupno redovitih članova	268



HZN

Hrvatski zavod za norme
Croatian Standards Institute

Poziv za uključivanje u rad tehničkog pododbora HZN/TO T4/PO 1, Normizacija u telekomunikacijama; Kvantna i kvantno otporna kibernetička sigurnost

S Instituta „Ruđer Bošković” u Hrvatski zavod za normizaciju (HZN) došla je inicijativa za praćenje normizacije u području kvantnih tehnologija i to zahvaljujući projektu „Hrvatska kvantna komunikacijska infrastruktura – CroQCI”.

Partneri na projektu su Institut Ruđer Bošković (IRB), Sveučilišni računski centar (SRCE) Sveučilišta u Zagrebu Institut za fiziku (IFZ), Fakultet elektrotehnike i računarstva (FER) Sveučilišta u Zagrebu, Fakultet prometnih znanosti (FPZ) Sveučilišta u Zagrebu, tvrtka Odašiljači i veze d. o. o. (OIV) i Ured Vijeća za nacionalnu sigurnost (UVNS).



DODATNE OBAVIJESTI:

Alica Glavaš, dipl. ing. prom.
viša stručna savjetnica za
normizaciju u području
telekomunikacija

e-pošta: alica.glavas@hzn.hr
tel. (01) 610 60 53

Kao punopravni član ETSI-ja HZN svojim članovima omogućuje sudjelovanje u radu bilo kojeg ETSI-jeva tehničkog odbora, što je kolegama iz hrvatskog konzorcija projekta CroQCI iznimno zanimljivo te su zainteresirani za sudjelovanje u radu ETSI-jeva TO CYBER.

Postojeći HZN/TO T4, *Normizacija u telekomunikacijama* prati rad svih tehničkih odbora ETSI-ja, stoga je HZN odlučio osnovati pododbor HZN/TO T4/PO 1, *Normizacija u telekomunikacijama; Kvantna i kvantno otporna kibernetička sigurnost* koji će pratiti samo ETSI-jev tehnički odbor CYBER.

Novi pododbor ima sljedeće područje rada:

- priprema norma i drugih normativnih dokumenata u području koje nudi rješenja za normizaciju kibernetičke sigurnosti usmjereno na tržište, savjete i smjernice za korisnike, proizvođače, operatore mreža, infrastrukture i usluga te regulatore
- razvoj norma koje povećavaju privatnost i sigurnost za organizacije i građane diljem Europe i svijeta, primjenjive u različitim domenama za sigurnost infrastrukture, uređaja, usluga, protokola i za stvaranje sigurnosnih alata i tehnika
- rad na tehničkim normama koje se mogu upotrebljavati za zaštitu podataka u skladu s GDPR-om
- norme koje podržavaju sigurnost i privatnost potrošačkih mobilnih uređaja i interneta stvari, kibernetičku sigurnost interneta stvari i kibernetičku sigurnost za kritične nacionalne infrastrukture te općenito sigurnost mreže
- rad na normama koje opisuju napredni standard šifriranja (AES) i vodič za kriptografiju temeljenu na identitetu
- tehnička dokumentacija u obliku digitalnih materijala koji su toliko jaki da se mogu upotrebljavati u pravnim ili kaznenim postupcima
- norme koje obuhvaćaju metode kibernetičke sigurnosti s analizom prijetnja, ranjivosti, rizika i protumjere
- izravna podrška zakonodavstvu EU-a
- razvoj preporuka i specifikacija za prijelaz na kvantno sigurne aplikacije, normiranje metoda koje ublažavaju potencijalno disruptivnu tehnologiju kvantnog računalstva; fokus je na praktičnoj implementaciji kvantno sigurnih primitiva, uključujući razmatranja performansa, mogućnosti implementacije, protokole, mjerila usporedbe (benchmarking) i praktična razmatranja arhitekture za specifične primjene
- rad na normizaciji implementacije kvantnih tehnologija u komunikacijskim infrastrukturama, s nekoliko mreža za distribuciju kvantnih ključeva (QKD) u izgradnji diljem svijeta; trenutačna visoka razina aktivnosti u kvantnim komunikacijama izazvala je potrebu za hitnim razvojem industrijskih norma za tehnologiju.

Pozivaju se članovi Hrvatskog zavoda za norme i ostale zainteresirane organizacije za uključivanje u rad tehničkog pododbora HZN/TO T4/PO 1, *Normizacija u telekomunikacijama; Kvantna i kvantno otporna kibernetička sigurnost*.

Making lives
easier, safer
and *better.*



TRENDOVI U NORMAMA

ISO 18750:2025

Intelligent transport systems — Local dynamic map **(Inteligentni prometni sustavi (ITS) — Lokalna dinamička mapa)**

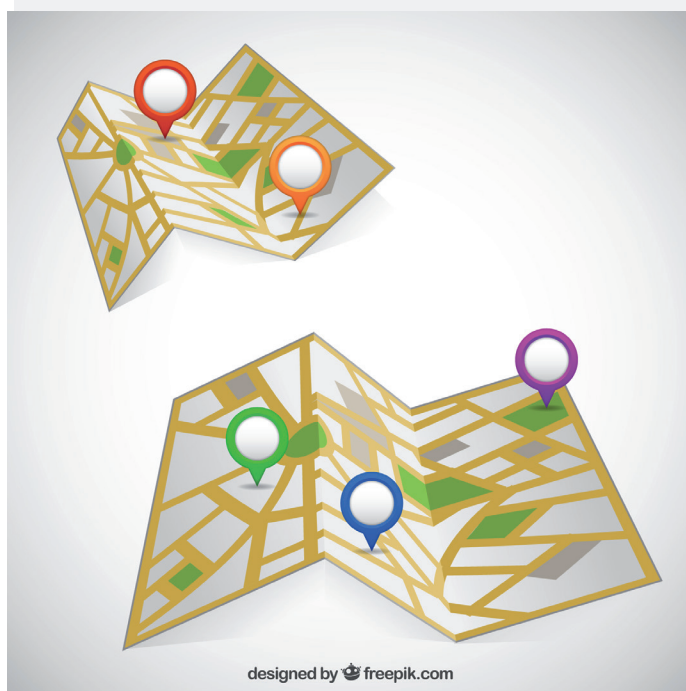
SAŽETAK

U ovom se dokumentu:

- opisuje funkcionalnost „lokalne dinamičke mape” (LDM) u kontekstu „ograničene zaštićene upravljane domene” (BSMD)
- određuju:
 - opće karakteristike podatkovnih objekata koji se mogu pohraniti u LDM-u (LDM-DO), tj. informacija o stvarnim objektima kao što su vozila, dionice radova na cesti, dionice usporenog prometa i dionice s posebnim vremenskim uvjetima, za koje je minimalni zahtjev da imaju oznaku lokacije i vremensku oznaku
 - funkcije pristupnih točaka za usluge koje osiguravaju sučelja u postaji inteligentnog prometnog sustava (ITS-S) za pristup LDM-u za:
 - sigurno dodavanje, ažuriranje i ukidanje pristupa za potrebe postupaka primjene ITS-S-a
 - siguran pristup za čitanje (upite) za potrebe postupaka primjene ITS-S-a
 - sigurne obavijesti (nakon pretplate) o postupcima primjene ITS-S-a
 - pristup upravljanju:
 - sigurna registracija, otkazivanje registracije i opoziv postupaka primjene ITS-S-a u LDM-u
 - sigurna pretplata i otkazivanje pretplate na postupke primjene ITS-S-a
 - postupci u LDM-u s obzirom na:
 - sredstva za održavanje sadržaja i cjelovitosti pohrane podataka
 - mehanizmi kojima se podupire nekoliko LDM-ova u konkretnoj fizičkoj postaji ITS-S-a.

OPĆE INFORMACIJE

Status: objavljeno	Datum objave: travanj 2025.
Izdanje: 2.	Broj stranica: 68
Tehnički odbor: ISO/TC 204	
ICS: 03.220.20; 35.240.60	



ISO/IEC 19762:2025

Information technology – Automatic identification and data capture (AIDC) techniques – Vocabulary
(Informacijska tehnologija – Tehnike automatske identifikacije i prikupljanja podataka (AIDC) – Terminološki rječnik)

SAŽETAK

Ovim se dokumentom definiraju opći nazivi koji se upotrebljavaju pri automatskoj identifikaciji i prikupljanju podataka (AIDC) i na kojima se temelje daljnji specijalizirani odjelci u različitim stručnim područjima te bitni nazivi koje korisnici koji nisu stručnjaci trebaju upotrebljavati u komunikaciji sa stručnjacima u AIDC-u.

OPĆE INFORMACIJE

Status: objavljeno	Datum objave: travanj 2025.
Izdanje: 2.	Broj stranica: 88
Tehnički odbor: ISO/IEC JTC 1/SC 31	
ICS: 01.040.35; 35.040.50	

ISO 18650-2:2025

Building construction machinery and equipment – Concrete mixers – Part 2: Procedure for examination of mixing efficiency
(Građevinski strojevi i oprema – Miješalice za beton – 2. dio: Postupak ispitivanja učinkovitosti miješanja)

SAŽETAK

U ovom se dokumentu utvrđuju postupak i zahtjevi za ispitivanje učinkovitosti miješanja šaržnih i kontinuiranih miješalica za beton definiranih u normi ISO 18650-1. Dokument se primjenjuje na miješalice za beton nazivnog kapaciteta najmanje 0,5 m³.

OPĆE INFORMACIJE

Status: objavljeno	Datum objave: ožujak 2025.
Izdanje: 3.	Broj stranica: 19
Tehnički odbor: ISO/TC 195/SC 1	
ICS: 91.220	

ISO 7240-27:2025

Fire detection and alarm systems – Part 27: Point type fire detectors using a smoke sensor in combination with a carbon monoxide sensor and, optionally, one or more heat sensors
(Sustavi za otkrivanje i dojavu požara – 27. dio: Točkasti detektori požara koji se koriste senzorom dima u kombinaciji sa senzorom ugljikova monoksida i, po izboru, jednim senzorom topline ili više senzora topline)

SAŽETAK

U ovom se dokumentu navode zahtjevi, metode ispitivanja i kriteriji učinkovitosti za točkaste detektore požara s više senzora koji uključuju senzor dima, senzor ugljikova monoksida (CO) i, po izboru, jedan senzor topline ili više senzora topline za uporabu u sustavima za otkrivanje i dojavu požara ugrađenima u zgradama (vidi ISO 7240-1).

Ovaj dokument nije primjenjiv na detektore požara sa senzorom dima, ugljikova monoksida i, po izboru, topline koji imaju posebna svojstva i namijenjeni su za posebne rizike. Za ispitivanje drugih vrsta detektora požara sa senzorom dima, ugljikova monoksida i, po izboru, topline koji rade na drukčijim načelima ovaj se dokument može primijeniti samo za orijentaciju.

OPĆE INFORMACIJE

Status: objavljeno	Datum objave: travanj 2025.
Izdanje: 3.	Broj stranica: 61
Tehnički odbor: ISO/TC 21/SC 3	
ICS: 13.220.20	

Izvor: ISO insights - newsletter
Priredila: Sandra Knežević
Prijevod: Tatjana Majić

Norme za energiju našeg planeta na Dan planeta Zemlje

22. travnja 2025.,
Boris Inderbitzen, IEC, voditelj vanjskih odnosa

Živimo u svijetu paradoksa. Godina 2024. bila je najtoplija dosad zabilježena godina, s rekordnim brojem toplinskih valova i brojnim ekstremnim vremenskim prilikama. Siječanj 2025. bio je najtopliji siječanj otkako postoje mjerenja. Istodobno, nikad prije nismo imali toliki rast kapaciteta obnovljive energije. Prema Međunarodnoj agenciji za obnovljive izvore energije (IRENA), više od 90 % globalnog širenja energije u 2024. godini otpada na obnovljive izvore energije.



Danas je Dan planeta Zemlje. Ove godine njegov je slogan „Naša snaga, naš planet“, koji nas podsjeća na to da moramo više nego ikada prihvatiti obnovljivu energiju i utrošiti svjetsku proizvodnju čiste električne energije do 2030. godine. Tehnologija je tu i imamo rješenja za rješavanje problema klimatskih promjena i smanjenje emisija. No to nije dovoljno i što više odgađamo, više ćemo plaćati. Moramo djelovati odmah.

To možemo učiniti ako postoji dovoljna predanost, potpora politike i ulaganja. Međunarodne norme i sustavi ocjenjivanja sukladnosti alati su koji vlade i oni koji imaju moć da uvedu promjene već sada mogu primijeniti u ostvarenju ciljeva. Oni predstavljaju neka od najboljih svjetskih znanja, rješenja i prakse u svim sektorima koji mogu pridonijeti ciljevima, među ostalim u vezi sa Sunčevom energijom, energijom oceana, vjetroturbinama, tehnologijom gorivnih članaka i pametnim mrežama. Norme pomažu da se osigura bezopasan, pouzdan i učinkovit rad tih sustava u elektroenergetskoj mreži i izvan nje. Pomažu i u poboljšanju energetske učinkovitosti. Osim toga, potiču povjerenje u nove i inovativne tehnologije koje će poticati proizvodnju i uporabu obnovljive energije.

Primjer je IEC-ov fond *Global Impact Fund*. Njegov je prvi projekt utvrđivanje izvedivosti ponovne uporabe rabljenih litijских baterija u obnovi solarnih fotonaponskih instalacija na važnim lokacijama poput škola i zdravstvenih ustanova u Keniji uz pomoć međunarodnih norma. Ako se taj pristup pokaže izvedivim, očekuje se da će se primjenjivati masovnije i proširiti na druge solarne fotonaponske instalacije u supsaharskoj Africi.

Taj je rad važan jer je pristup energiji mnogo bitniji nego što se čini na prvi pogled. Bitan je za poboljšanje obrazovanja, zdravstvene skrbi i socioekonomskih prilika za sve.

Očekuje se da će prvi projekt Fonda poboljšati život mnogih Kenijaca u ruralnim područjima osiguravajući im pristup pouzdanim i čistim izvorima električne energije.

No, ne zaboravimo da je to globalni izazov i da zahtijeva globalna rješenja. Tiče se svih nas. Zato će glavna tema naše ovogodišnje glavne skupštine biti „Poticanje održivog svijeta“. U rujnu će se članovi zajednice IEC-a okupiti i raspravljati o tome kako norme mogu bolje odgovoriti na glavne izazove i potaknuti prijelaz na sustave održive energije.

Bit ćemo vrlo aktivni i na konferenciji COP 30, gdje ćemo s donositeljima odluka o klimi voditi važne razgovore o tome kako globalno prihvaćene norme pridonose pretvaranju obveza u pogledu zaštite klime u učinkovite i mjerljive mjere. Međunarodne norme i sustavi ocjenjivanja sukladnosti moćni su saveznici vlada jer pružaju konkretna rješenja i okvire za usmjeravanje i provedbu politika potrebnih za postizanje trajnih promjena. Olakšavaju i pristup globalnim tržištima jer niti jedna zemlja to ne može učiniti bez njih.

Ne smijemo gubiti vrijeme, moramo djelovati sada. Norme su alat koji već postoji i pomaže nam. Pouzdane su i rezultat globalnog dogovora i podupiru transformaciju obveza i planova u području klime u učinkovite i mjerljive mjere. Pozivamo vlade da iskoriste vrijednost norma u mjerama i poticajima za borbu protiv klimatskih promjena kako bi se Dan planeta Zemlje mogao zaista slaviti.

Izvor: IEC
Priredio: Ivo Andreis
Prijevod: Tatjana Majić

Pristup sektorskoj kibernetičkoj sigurnosti koji se temelji na riziku: Uvod u EN 18037:2025

*U svijetu koji se sve više digitalizira važnije je nego ikad osigurati pouzdano visoku kibernetičku sigurnost u složenim sustavima s više dionika. Nova europska norma **EN 18037:2025, Guidelines on a sectoral cybersecurity assessment**, koju je izradio tehnički odbor **JTC 13, Cybersecurity and Data Protection**, odgovor je na tu potrebu. U normi je prikazan pristup utvrđivanju zahtjeva kibernetičke sigurnosti, certifikacije i jamstva za proizvode, procese i usluge IKT-a u složenim sektorskim sustavima s više dionika utemeljen na riziku.*

Proces sektorske procjene kibernetičke sigurnosti obuhvaća sve potrebne korake za utvrđivanje, provedbu i održavanje tih zahtjeva. Sektorski sustavi IKT-a prevladavaju u područjima primjene kao što su mobilne mreže, digitalni identitet, e-zdravstvo, javni prijevoz i platni sustavi. Ti sustavi u pravilu uključuju brojne organizacije dionice koje rade u svojim definiranim ulogama i pružaju sektorske usluge. Neke uloge, poput uloga operatera mobilnih mreža ili pružatelja usluga javnog prijevoza, mogu uključivati natjecanje među dionicima.

Kibernetička sigurnost i jamstvo ključni su ne samo iz perspektive potrošača već i za poticanje povjerenja među dionicima u sektoru. Nužna je jasna i dosljedna definicija zahtjeva kibernetičke sigurnosti i jamstva prilagođenih ulogama dionika jer nedostaci u sigurnosti jednog dionika mogu predstavljati rizik za poslovne ciljeve drugih dionika u ekosustavu.

Važnost norme i promjena koje ona donosi

Sektorske usluge imaju sve važniju ulogu u svakodnevnom životu. Međutim, do sada nije postojala norma koji bi ponudila cjelovit i dosljedan pristup upravljanju kibernetičkom sigurnošću u svim uslugama i njihovim pratećim sustavima.

Norma **EN 18037** odgovara na tu potrebu uvođenjem **sektorske metodologije za procjenu kibernetičke sigurnosti**, kojom se podupiru standardizirane procjene rizika i usklađene ocjene rizika u svim organizacijama dionicama. Također olakšava utvrđivanje zahtjeva na razini sigurnosti i jamstva za proizvode, procese i usluge IKT-a u skladu s njihovom namjenom u određenom sektorskom sustavu.

Ključne su metodološke značajke sljedeće:

- **Kontekstualizacija poslovnih procesa:** procjena počinje analizom poslovnih procesa koje podupiru sektorski sustavi IKT-a i odgovarajućih poslovnih ciljeva pojedinih dionika. Njome se utvrđuje glavna i pomoćna imovina bitna za sigurnu implementaciju.
- **Povezivanje (kartiranje) imovine i sustava:** evidentiraju se sustavi, proizvodi i procesi IKT-a pod kontrolom dionika koji su bitni za osiguranje glavne imovine. Temeljita analiza sektorske systemske arhitekture pruža detaljan uvid u njihovu namjenu.
- **Stjecanje spoznaja o kibernetičkim prijetnjama (CTI):** stječu se spoznaje o bitnim tipovima napadača, njihovim motivima i sposobnostima. Time se omogućuje davanje prioriteta scenarijima rizika koji najviše zaslužuju daljnju analizu, optimiziranje upotrebe analitičkih resursa i podržavanje dodjele prilagođenih zahtjeva kibernetičke sigurnosti i jamstva.
- **Procjena rizika:** rizici se procjenjuju na temelju učinka kibernetičkih incidenata na poslovne ciljeve i vjerojatnosti nastanka takvih incidenata. Vjerojatnost se izvodi iz motiviranosti i sposobnosti napadača koje su utvrđene CTI-jem.
- **Referentne razine:** metodologijom se uvodi sustav referentnih razina unutarnjeg rizika, sigurnosti, jamstva i potencijala napada. Kad se upotrebljavaju zajedno, njima se podupire dosljednost u definiranju rizika za kibernetičku sigurnost. Podaci o riziku izvedeni iz pristupa prema normi ISO/IEC 27005 mogu se prenijeti u okvir iz niza norma ISO/IEC 15408 za utvrđivanje zahtjeva za jamstvo. Te norme zajedno omogućuju pouzdanu definiciju potreba za kibernetičkom sigurnošću i jamstvom na temelju rizika.

Koristi za gospodarstvo i društvo

Sektorska metodologija iz norme EN 18037, koja je prvotno razvijena radi potpore pripremi programa certificiranja kibernetičke sigurnosti u skladu sa Zakonom EU-a o kibernetičkoj sigurnosti, pokazala je širu primjenjivost pružajući konkretne koristi sektorskim dionicima, korisnicima usluga i dobavljačima proizvoda IKT-a:

- **Donošenje odluka na temelju rizika:** metodologija omogućuje utvrđivanje rizika povezanih s namjenom sustava, usluga i procesa IKT-a na svim razinama sektorske arhitekture IKT-a. Organizacije dionice mogu bolje uskladiti svoju toleranciju rizika s ulaganjima potrebnima za ublažavanje rizika, potičući transparentnost i suradnju u području sigurnosti. Time će se vjerojatno povećati prihvaćanje zahtjeva i odgovarajućih sustava certificiranja na tržištu.
- **Usklađenost među programima:** usklađivanjem provedbe razina sigurnosti i jamstva norma EN 18037 omogućuje ponovnu uporabu certifikata u različitim programima certifikacije. Time se promiče operativna učinkovitost pružatelja proizvoda i usluga i jača povjerenje potrošača. Istodobno se fleksibilnim okvirom iz norme podupire integracija novih programa certificiranja prilagođenih konkretnim potrebama tržišta.
- **Ujednačeni sigurnosni kontrolni mehanizmi:** zajedničkim konceptom razina sigurnosti pojednostavnjuje se razvoj sigurnosnih kontrolnih mehanizama koji se mogu višekratno upotrebljavati u svim sustavima certificiranja, čime se omogućuju prilagodljivi i interoperabilni pristupi jamstvu.

Praktična primjena norme

Kao što je izvorno predviđeno, **metodologijom sektorske procjene kibernetičke sigurnosti** opisanom u normi EN 18037 osigurava se potpuna osnova za razvoj sustava certificiranja usklađenih sa zahtjevima Zakona EU-a o kibernetičkoj sigurnosti. Praktična primjena već je vidljiva u razvoju nacionalnih i europskih programa certificiranja koji se temelje na normi EN 17640, *Fixed-time cybersecurity evaluation methodology for ICT products*, na koju se poziva **Program rada Europske unije**.

Nedavno se pojavilo neočekivano, ali obećavajuće područje primjene: **potpora proizvođačima** preciznim sektorskim sigurnosnim zahtjevima za predviđenu namjenu njihovih proizvoda. Konkretno, proizvođači proizvoda koji žele ispuniti obveze iz **Zakona EU-a o kibernetičkoj otpornosti** mogu imati znatne koristi od primjene metodologije iz norme EN 18037.

Ovaj članak napisan je u suradnji s Elzbiatom Andrukiewicz i Cordom Bartelsom.

Izvor: CEN/CENELEC
Prijevod: Tatjana Majić



Hrvatski zavod za norme prihvatio je u hrvatsku normizaciju europsku normu EN 17640:2022, *Fixed time cybersecurity evaluation methodology for ICT products* kao hrvatsku normu **HRN EN 17640:2022**, *Metodologija procjene kibernetičke sigurnosti na određeno vrijeme za ICT proizvode (EN 17640:2022)*.

Tekst hrvatske norme **HRN EN 17640:2022** pripremio je tehnički odbor **TO 582, Informacijska sigurnost i upravljanje kontinuitetom poslovanja** Hrvatskoga zavoda za norme.

Detaljnije informacije o navedenoj normi te ostalim hrvatskim normama možete pronaći u [katalogu hrvatskih norma](#) te [repozitoriju HRN4You](#).

Za dodatne obavijesti o radu tehničkog odbora HZN/TO 582 možete se obratiti **Dinki Ilić-Roller**, višoj stručnoj savjetnici za normizaciju u području informacijske tehnologije (dinka.ilic.roller@hzn.hr)

Za besplatan uvid u sadržaj norma možete najaviti svoj dolazak u [normoteku](#), a za kupnju navedenih norma ili bilo kojega normativnog dokumenta pošaljite popunjeni [obrazac za ponudu](#) na e-adresu prodaja@hzn.hr.



HZN

Hrvatski zavod za norme
Croatian Standards Institute

Sveeuropski e-poziv: kad automobili zovu upomoć

U teškim prometnim nesrećama na europskim cestama svake godine tisuće ljudi izgube život. Iako hitne službe daju sve od sebe, kad se nesreća dogodi na udaljenom mjestu ili je vozač preteško ozlijeđen da bi pozvao pomoć, može biti izgubljeno dragocjeno vrijeme.

Kako bi bilo da vaš automobil sam može pozvati hitnu pomoć?

Upravo to čini sveeuropski sustav hitnog pozivanja iz vozila (e-poziv, engl.: eCall), a nedavno izmijenjena norma osigurava njegovo još bolje funkcioniranje.



Normom EN 16072:2025, *Intelligent transport systems – ESafety – Pan-European eCall operating requirements*, koju je izradio tehnički odbor CEN/TC 278, *Intelligent Transport Systems*, utvrđuju se **operativni zahtjevi** za e-poziv, automatski sustav za hitne pozive iz vozila koji se spajaju izravno s hitnim službama.

Što je e-poziv?

E-poziv inteligentni je prometni sustav koji u slučaju teške prometne nesreće automatski poziva najbližu **pristupnu točku za javnu sigurnost (PSAP)**. Njime se prenose glasovna veza i **minimalni skup podataka (MSD)** kao što su točna lokacija, vrsta vozila i smjer putovanja kako bi interventno osoblje moglo brzo i učinkovito reagirati.

Sustav se može aktivirati **automatski**, na primjer pri otvaranju zračnih jastuka, ili **ručno** pritiskom na tipku SOS u vozilu.

Zašto je važna normizacija?

Da bi e-poziv zaista postao **sveeuropski**, vozila i pozivni centri za hitne slučajeve u svim članicama EU-a moraju „govoriti” istim stručnim jezikom. Tu nastupa norma EN 16072:2025. Njome se osigurava sljedeće:

- Svaki automobil sa sustavom e-poziva može se povezati s centrima za hitne slučajeve bez obzira na zemlju.
- Poslani podaci dosljedni su i pouzdani.
- Zaštićena je privatnost i sigurnost vozača.
- Glasovna i podatkovna komunikacija neometano funkcionira čak i u prekograničnim situacijama.

Što je novo u izdanju iz 2025. godine?

Nova verzija zamjenjuje izdanje iz 2022. godine i donosi nekoliko poboljšanja:

- jasniji način postupanja s podacima o lokaciji i smjeru
- bolje upute za operatore PSAP-a o tome kako reagirati, osobito kada glasovna veza nije moguća
- strože mjere zaštite privatnosti kako bi se osiguralo da se e-poziv aktivira samo u stvarnim hitnim slučajevima.

Dodane su i nove tehničke pojedinosti radi kompatibilnosti sa starijim mobilnim mrežama (npr. GSM-om) i novijim sustavima koji se koriste internetom (komunikacija utemeljena na IP-u).

Koristi za ljudi i društvo

Sustav e-poziva nije samo tehnička značajka – on spašava živote. Prema procjenama EU-a potpuna primjena sustava e-poziva diljem Europe mogla bi spasiti **do 2500 života godišnje** i znatno smanjiti težinu ozljeda u prometu.

Osim toga, slanje točnog podatka o lokaciji pomaže interventnom osoblju da brže stigne do mjesta nesreće, čak i onog koje je teško pronaći, npr. seoske ceste ili mjesta u inozemstvu.

Budući da je e-poziv u skladu sa zakonom o zaštiti podataka, vozači mogu biti sigurni da njihov automobil ne omogućuje praćenje – sustav se **aktivira samo u hitnim slučajevima**.

Europska suradnja

Ova norma pokazuje da promišljeno projektiranje i suradnja mogu omogućiti da tehnologija funkcionira u korist svih. Pretvarajući samo vozilo u hitnu službu, **e-poziv skraćuje vrijeme između sudara i pomoći koja spašava život**.

Izvor: [CEN/CENELEC](#)

Prijevod: Tatjana Majić

CEN i CENELEC

CEN (Europski odbor za normizaciju) i CENELEC (Europski odbor za elektrotehničku normizaciju) priznati su od strane Europske unije (EU) i Europskog udruženja slobodne trgovine (EFTA) kao europske normizacijske organizacije zadužene za izradu normi na europskoj razini.

Članovi CEN-a i CENELEC-a nacionalna su normizacijska tijela i nacionalni elektrotehnički odbori 34 europske zemlje. Europske norme (EN) i ostali normativni dokumenti koje objavljuju CEN i CENELEC prihvaćeni su i priznati u svim tim zemljama. Europske norme pridonose povećanju sigurnosti, poboljšanju kvalitete, olakšavanju prekogranične trgovine i jačanju europskoga jedinstvenog tržišta. CEN i CENELEC promiču međunarodno usklađivanje normi u okviru sporazuma o stručnoj suradnji s ISO-om (Međunarodnom organizacijom za normizaciju) i IEC-om (Međunarodnim elektrotehničkim povjerenstvom).

Mrežna stranica CEN-a i CENELEC-a: www.cencenelec.eu



ETSI-jeva tehnička specifikacija postavlja međunarodno mjerilo za osiguravanje umjetne inteligencije



ETSI predstavlja svoju najnoviju tehničku specifikaciju kojom se utvrđuje mjerilo za osiguravanje sustava umjetne inteligencije (UI) u kontekstu sve većih prijetnji kibernetičkoj sigurnosti.

„ETSI TS 104 223 – Osiguranje umjetne inteligencije (SAI); osnovni zahtjevi za kibernetičku sigurnost modela i sustava umjetne inteligencije” nova je specifikacija u kojoj se daju pouzdane i provedive smjernice za kibernetičku sigurnost radi zaštite krajnjih korisnika. Uzimajući u obzir pristup utemeljen na cjeloživotnom ciklusu, definiran je skup od 13 temeljnih načela te ukupno 72 ostvariva načela za pet faza životnog ciklusa u svrhu povećanja razine sigurnosti svih sustava UI-ja.

U specifikaciji se detaljno navode transparentna opća načela i odredbe za osiguravanje UI-ja. Dioncima u lancu opskrbe u području UI-ja, od razvojnih programera i trgovaca do integratora i operatera, daje se čvrst skup osnovnih sigurnosnih zahtjeva koji pomaže u zaštiti sustava UI-ja od kibernetičkih prijetnji koje se stalno mijenjaju.

Umjetna inteligencija predstavlja jedinstvene izazove u usporedbi s tradicionalnim softverom, uključujući rizike poput trovanja podataka, skrivanja modela (*model obfuscation*), neizravnog ubacivanja odzivnih poruka (*indirect prompt injection*) i ranjivosti povezanih s upravljanjem složenim podacima. Uzimajući u obzir te razlike, u specifikaciji ETSI TS 104 223 daju se ciljane smjernice kojima se uhodani postupci u području kibernetičke sigurnosti i umjetne inteligencije objedinjuju s novim pristupima.

Specifikaciju je izradio ETSI-jev tehnički odbor za osiguravanje umjetne inteligencije (TC SAI) koji uključuje predstavnike međunarodnih organizacija i vladinih tijela te stručnjake za kibernetičku sigurnost. Interdisciplinarnom suradnjom osigurava se da zahtjevi budu primjereni na globalnoj razini i provedivi u praksi.

Osim tehničke specifikacije ETSI će objaviti i praktični vodič za primjenu namijenjen malim i srednjim poduzetnicima i drugim dionicima.

Vodič će sadržavati studije slučaja u raznim okružjima primjene koji će korisnicima pomoći u djelotvornoj primjeni sigurnosnih zahtjeva.

„U doba kada rastu i opseg i složenost kibernetičkih prijetnji i one negativno utječu na organizacije svih vrsta važno je da projektiranje, razvoj, puštanje u rad te rad i održavanje modela umjetne inteligencije budu zaštićeni od zlonamjernih i neželjenih uplitanja”, izjavio je Scott Cadzow, predsjednik ETSI-jeva Tehničkog odbora za osiguravanje umjetne inteligencije. *„Sigurnost mora biti temeljni zahtjev, ne samo u fazi razvoja već i tijekom cijelog životnog ciklusa sustava. Nova specifikacija pomoći će da se to postigne, ne samo u Europi nego i u cijelom svijetu. Ova je publikacija prvi korak na međunarodnoj razini u utvrđivanju jasnog temelja za osiguravanje umjetne inteligencije kojom Tehnički odbor za osiguravanje umjetne inteligencije zauzima važan položaj na putu prema povjerenju u sigurnost umjetne inteligencije za sve dionike.”*

O ETSI-ju

ETSI članovima pruža otvoreno okruženje koje uključuje sve interesne strane i podupire pravodobnu izradu, prihvaćanje i ispitivanje globalno primjenjivih norma za sustave, aplikacije i usluge utemeljene na informacijsko-komunikacijskoj tehnologiji (IKT) u svim sektorima gospodarstva i društva.

Mi smo neprofitno tijelo s više od 900 organizacija članica širom svijeta iz 62 zemlje na pet kontinenata.

Članovi čine raznoliku bazu velikih i malih privatnih tvrtka, znanstvenih organizacija, sveučilišta, državnih i javnih tijela. ETSI je jedno od triju tijela koja Europska unija službeno priznaje kao europske normizacijske organizacije.



Izvor: ETSI
Pripremila: Alica Glavaš
Prijevod: Tatjana Majić