HZN e glasilo

Broj 4/2019
Službeno glasilo Hrvatskoga zavoda za norme

Norma 18091 donosi održivi razvoj lokalnim vlastima

Digitalno učenje transformira obrazovanje

Prikupljanje energije iz cesta

HZN

Članovi HZN-a

Nova CEN-ova norma: Bolje dijagnoze uz niz norma EN ISO 20116:2018

HZN e-glasilo

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

Godište: 11. 2019.
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 6095** **Telefax: 01/610 93 21**
Glavni urednik:	Igor Božičević, ravnatelj HZN-a
Pomoćnik glavnog urednika:	Vladimir Jaram
Tehnički urednik:	Vladimir Jaram
Uredništvo:	Ana Marija Boljanović, Melanija Grubić Sutara, Vlasta Gaćeša-Morić, Boro Jandrijević, Vladimir Jaram, Igor Božičević
Lektura:	Ivana Canosa
Korektura:	Vladimir Jaram, Sandra Knežević
Grafička obrada naslovnice:	Vladimir Jaram
Grafička priprema:	Vladimir Jaram, Sandra Knežević
Izlazi:	mjesečno
Uređenje	2019-04-30

PROSLOV

Poštovani čitatelji!

U ovome broju HZN e-glasila, možete u našim stalnim prilozima pročitati o zbivanjima u HZN-u te regionalnim i međunarodnim normizacijskim organizacijama. U vijestima iz HZN-a, nalazi se naš stalni prilog o članovima HZN-a.

U rubrici Novosti iz međunarodnih i europskih normizacijskih organizacija, u ovome broju objavljujemo iz IEC-a prilog o digitalnom učenje koje transformira obrazovanje i kako se sve veći broj škola koristi programima virtualne stvarnosti u nastavi povijesti, matematike, prirodnih predmeta... Tu su još prilozi o prikupljanju energije iz cesta te internetskim napadima na kritičnu infrastrukturu.

Iz ISO-a predstavljamo prilog o normi ISO 18091 koja donosi održivi razvoj lokalnim vlastima i trebala bi im pomoći unaprijediti njihove aktivnosti i uskladiti ih s lokalnim potrebama i očekivanjima radi zdravije i sigurnije zajednice. Tu je još i prilog o tome kako pristupiti današnjim rizicima informatičke sigurnosti.

U novostima iz CEN/CENELEC-a, donosimo prilog o novoj CEN-ovoj normi EN ISO 20166:2018, „Molekularna in vitro dijagnostička ispitivanja“! Ona bi trebala omogućiti bolju dijagnostiku te smanjiti rizik neobjektivnih dijagnoza i povećati sigurnost. Tu je također informacija o novome nizu norma EN ISO 10855 koji daje međunarodno priznate smjernice za odobalne spremnike.

Ugodno čitanje!

V. Jaram
pomoćnik glavnoga urednika

Sadržaj 4/2019

Naslovnica: *Priopćenja iz regionalnih i međunarodnih normizacijskih organizacija*

HZN Oglasnik za normativne dokumente (A1-A104)

ISSN 1847-4217

Novosti iz HZN-a

Članovi Hrvatskog zavoda za norme

Objavljujemo popis redovitih i pridruženih članova HZN-a po vrstama pravnih odnosno fizičkih osoba za koje je Upravno vijeće donijelo odluku do kraja travnja 2019. godine.

Tablica *Članovi Hrvatskog zavoda za norme* identična je tablici objavljenoj u HZN e-glasilima br. 2/2019 i 3/2019 jer do 30. travnja 2019. godine nije bilo promjena.

Vrsta članstva, vrsta pravne ili fizičke osobe	2018-12-11	2018-12-20
Članovi promatrači		
Pravne osobe koje ostvaruju dobit	8	8
Fizičke osobe	0	0
Ukupno promatračkih članova	**8**	**8**
Redoviti članovi		
Pravne osobe koje ostvaruju dobit	162	161
Pravne osobe koje ne ostvaruju dobit – javne ustanove i slično	21	21
Pravne osobe koje ne ostvaruju dobit – HGK, HOK, HUP	1	1
Pravne osobe koje ne ostvaruju dobit – strukovne komore ili udruge	5	5
Pravne osobe koje ne ostvaruju dobit – strukovna društva	9	10
Pravne osobe koje ne ostvaruju dobit – škole	1	1
Pravne osobe koje ne ostvaruju dobit – fakulteti	20	20
Fizičke osobe – pojedinci	25	22
Obrt – fizičke osobe	2	2
Tijela državne uprave	51	51
Ukupno redovnih članova	**297**	**294**
Ukupno članova HZN-a	**305**	**302**

HZN

Digitalno učenje transformira obrazovanje

Zamislite da doživljavate povijesni trenutak kao da se upravo događa, ili da otkrivate staničnu biologiju u 3D iz unutrašnjosti tijela. To je sada moguće pomoću virtualne stvarnosti

Piše: Antoinette Price

U dijelovima Azije, Sjeverne i Južne Amerike, Europe i Afrike, digitalne tehnologije omogućuju učenicima i studentima da uče djelotvornije i iz sasvim novih perspektiva.

Sve veći broj škola koristi se programima virtualne stvarnosti u nastavi povijesti, matematike, prirodnih predmeta i ostalih.

Mogućnost spajanja na internet i internet stvari (IoT), umjetna inteligencija (AI) strojno učenje i algoritmi, virtualna i uvećana stvarnost (VR/AR) neke su od inovativnih tehnologija koje donose tektonske promjene (*disruptive technologies*) u naš način života, komunikacije, putovanja na posao, zdravstvene skrbi, zabave, poljoprivrede, rada i još mnogo toga.

To vrijedi i za učenje. Širom svijeta, dok se učenici i studenti svih dobnih skupina pripremaju za budućnost, obrazovna djelatnost iznova promišlja svoje obrazovne sustave.

To se ne odnosi samo na osnovno i srednje obrazovanje. Starijim dobnim skupinama koje rade u okruženju koje se mijenja zbog tehnologije trebat će redovite prekvalifikacije ili cjeloživotno učenje.

Osim toga, neke od tih tehnologija omogućuju pristup obrazovanju ljudima u zemljama u razvoju ili udaljenim krajevima i ljudima ograničene mobilnosti, što im poboljšava opću kvalitetu života.

Dobro obrazovanje za sve

Obrazovanjem se može poboljšati kvaliteta života i stvoriti osnova za održivi razvoj. Ciljem održivog razvoja Ujedinjenih naroda, (SDG) 4 kvalitetno obrazovanje, želi se osigurati da sve djevojčice i dječaci imaju pristup besplatnom, pravičnom i kvalitetnom osnovnom i srednjem obrazovanju i da ga završe. Također se nastoji osigurati ravnopravna dostupnost jeftinog i kvalitetnog tehničkog, stručnog i tercijarnog kao i fakultetskog obrazovanja za sve žene i muškarce bez obzira na spol, invalidnost i pripadnost autohtonom narodu.

Inovativne tehnologije kao što su virtualna stvarnost, internet stvari (IoT) i umjetna inteligencija (AI) pomažu da se povećaju i razgranaju mogućnosti učenja za ljude širom svijeta u najrazličitijim situacijama.

Časopis *e-tech* razgovarao je s Erlendom Øverbyjem, koji vodi IEC-ov i ISO-ov normizacijski rad u području informacijske tehnologije za učenje, obrazovanje i usavršavanje (ITLET), o najnovijim događajima i o tome kako norme mogu pridonijeti ne samo razvoju te djelatnosti nego i ostvarenju SDG 4.

Kako tehnologija utječe na obrazovnu djelatnost u cjelini?

AI i mogućnost spajanja na internet već donose brojne koristi učenju. Naprimjer, što više podataka imamo, možemo više iz njih naučiti kroz analizu. Algoritmima se mogu izvući („iskopati“) i usporediti podaci iz raznoraznih konteksta učenja kako bi se otkrilo koje aktivnosti daju najbolji rezultat učenja. One uključuju sustave upravljanja učenjem, interaktivna okruženja učenja, inteligentne sustave poduke, edukativne igre i aktivnosti učenja bogate podacima. Krojeno učenje moguće je zahvaljujući tome što se na temelju podataka uparuje razina kompetencija učenika s njihovim aktivnostima učenja. To se može primijeniti i na procese podučavanja.

„Tehnologija sama za sebe ne osigurava učenje, obrazovanje i usavršavanje. Obrazovanje nastupa kada se sve stavi u kontekst i time upravlja ‘nastavnik’. Upotreba tehnologije mora se staviti u kontekst koji ispunjava ciljeve učenja, obrazovanja i usavršavanja. Tehnologija sama za sebe nema vrijednost; bitno je kako je odlučimo primijeniti.“

Obrazovne institucije i radna mjesta zahtijevaju redovnu obuku u računalnoj pismenosti za učitelje, nastavnike, učenike, studente i zaposlenike.

„Mora doći do pomaka u razmišljanju: računalo je alat za rješavanje problema, a ne samo stroj za računanje. To je ono što treba podučavati u školi: ako nešto ne razumijemo ili trebamo dodatne informacije, trebamo znati kako pomoću tehnologije pronaći odgovore.“

Drugo je pitanje razvoj vlasnički zaštićenih paketa tehnologije, koji u krajnjem slučaju mogu ograničiti izbor nastavnih materijala.

„Zakonodavac treba norme koje će sadržavati zahtjeve za dobavljače informatičkih programa za škole: oni moraju osigurati da tehnologija ne ovisi o uređajima i ekosustavima i da je u potpunosti interoperabilna. Tako će se izbjeći da se škole ograniče na jedan određeni sustav i omogućiti nastavnicima da odaberu najbolji način učenja za svoje učenike.

Osim toga, kod digitalnog učenja mora se osigurati sigurnost i privatnost podataka. Naprimjer, podaci stvoreni procesom učenja mogu se pohraniti i dijeliti. Ako učenici sudjeluju u simulaciji glumeći određene likove na internetu, oni mogu biti predmet internetske provale i zloupotrebe, što može dovesti do toga da netko o tim učenicima stvori pogrešnu sliku.

Koji su izazovi?

Iako mnoge zemlje imaju strategiju upotrebe digitalnih resursa u obrazovanju, još mnogo treba učiniti da bi se informatika ugradila u moderne obrazovne sustave širom svijeta. Zemlje prepoznaju prednosti modernih i ciljanih digitalnih resursa za učenje u odnosu na zastarjele udžbenike na papiru. Potrebno je još normi da bi se osiguralo da cjelokupna informacijska tehnologija koja se upotrebljava za učenje, obrazovanje i usavršavanje postane glatka i bez zapreka i zatvorenih ekosustava. Krajnji bi cilj trebao biti da svi mogu sudjelovati, bez obzira na uređaje kojima se koriste, i ostvariti najbolje moguće iskustvo učenja.

„Naš je glavni izazov da u našem radu sudjeluje što više zemlja, kako razvijenih tako i zemalja u razvoju, a također i stručnjaka. Sve zemlje koje imaju strategiju digitalnog obrazovanja trebaju preuzeti aktivnu ulogu i pružiti svoja gledišta. Tvrtke koje se bave obrazovnim tehnologijama, a planiraju globalnu prisutnost, kako etablirane tako i nove, trebaju razmišljati na način da njihova rješenja budu interoperabilna s drugim informatičkim sustavima, naprimjer radi lakše razmjene podataka.“

Budućnost učenja

Digitalno je obrazovanje u porastu. Liječnici mogu uživo emitirati složene operacije studentima širom svijeta, a djelatnici u uklanjaju posljedica katastrofa obučavaju se za postupanje sa smrtonosnim bolestima ili nesrećama pomoću VR simulacijskih programa.

Na radnom mjestu – u tvornici, bolnici ili uredu – zaposlenici se trajno usavršavaju da bi mogli raditi s procesima koji su u sve većoj mjeri automatizirani i naučiti nove informatičke programe.
IEC-ove i ISO-ove međunarodne norme za učenje, obrazovanje i usavršavanje pomoći će da se unaprijedi digitalizacija obrazovanja tako što će osigurati da programeri i proizvođači strojne opreme paze na interoperabilnost i sigurnost podataka širući tako pristupačnost i povećavajući opću kvalitetu globalnog obrazovanja.

(Izvor: https://iecetech.org/issue/2019-02/Digital-learning-is-redefining-education; priredio: V. Jaram; prijevod: T. Majić)

Prikupljanje energije iz cesta

Prikupljanje energije koristi se Sunčevim svjetlom ili mehaničkim vibracijama koje proizvode vozila i pješaci za proizvodnju električne energije. Dobivena struja može se upotrebljavati za pogon cestovne infrastrukture kao što je rasvjeta i signalizacija.

Pohranjuje se u baterije za kasniju upotrebu ili usmjerava u elektroenergetsku mrežu. S obzirom da se koristi postojećom cestovnom mrežom, nije potrebno osigurati dodatne površine.

Međunarodne norme imaju ključnu ulogu u razvoju tih rješenja. IEC-ov tehnički odbor (TC) 47 izrađuje međunarodne norme za poluvodičke uređaje, uključujući one koji prikupljaju energiju. Baterije koje se upotrebljavaju za pohranu električne energije oslanjaju se na normizacijski rad IEC-ovog tehničkog odbora IEC TC 21.

IEC TC 8 i njegov pododbor (SC) 8A izrađuju norme za sustave napajanja električnom energijom, uključujući integraciju energije koja je proizvedena iz obnovljivih izvora energije i usmjerava u elektroenergetsku mrežu. Skupina *SyC Smart Energy* bavi se normizacijom na razini sustava, koordinacijom i smjernicama u području pametnih elektroenergetskih mreža i pametne energije.

Razvijene su tehnike kojima se na površinu ceste instaliraju fotonaponski moduli koji prikupljaju solarnu energiju. Energija se može prikupljati s više od 16 milijuna kilometara asfaltiranih cesta širom svijeta koje su izložene Sunčevoj svjetlosti.

Unatoč problemima, od kojih su mnogi povezani s prianjanjem guma na cestu, nekoliko je tvrtki razvilo fotonaponske module koji mogu ili zamijeniti asfalt ili se postaviti izravno na postojeće kolnike. Ta su rješenja vlasnički zaštićena, ali se oslanjaju na međunarodne norme koje je izradio tehnički odbor IEC TC 82 koji se bavi sustavima solarne fotonaponske energije.

Širom svijeta u tijeku su pilot projekti. Nedavno su nizozemske pokrajine Noord-Holland i Zuid-Holland (Sjeverna i Južna Holandija) instalirale solarne panele na 150 metara cestovnih površina. Očekivani godišnji prinos električne energije na 100 metara solarne cestovne površine iznosi 30,000 kWh.

Za prikupljanje energije s cesta mogu se primijeniti i termoelektrični generatori (TEG). Na temelju Seebeckovog efekta, TEG mogu pretvarati geotermalnu energiju - proizvedenu iz toplinske razlike između površine ceste i slojeva ispod nje - u električnu energiju. Kako se razlika u temperaturi povećava, proizvodi se više električne energije pa je ta tehnologija prikladnija za vrlo topla područja.

Tehnički odbor IEC TC 47 izradio je 2017. godine niz normi IEC 62830-2 koji daje metode za ocjenjivanje toplinske energije tankih slojeva koji se upotrebljavaju u uređajima za prikupljanje termoelektrične energije.

Za proizvodnju električne energije mogu se iskorištavati i vibracije koje stvaraju automobili dok voze cestom. Piezoelektricitet električni je naboj koji proizvode određeni kristali pri primjeni mehaničkog opterećenja.

Piezoelektrični kristali mogu se ugraditi ispod sloja asfalta. Dok automobili prolaze cestom, kotači djeluju silom zbog koje se ti kristali deformiraju i proizvode električnu energiju.

Ona se može iskoristiti za napajanje cestovne rasvjete ili se može uskladištiti u baterijama za kasniju upotrebu. Niz normi IEC 62830–1 tehničkog odbora IEC TC 47 obuhvaća metode za ocjenjivanje svojstava uređaja za prikupljanje piezoelektrične energije proizvedene vibracijama.

Na jugozapadu Sjedinjenih Američkih Država u tijeku su istraživanja za ispitivanje te tehnologije i njezinu moguću primjenu kao rezervnog izvora energije za LED rasvjetu pista i pristupnih putova. Mogla bi se upotrebljavati kao jedini način rasvjete pista ruralnih civilnih aerodroma.

(Izvor: https://blog.iec.ch/2019/03/harvesting-energy-from-roads/; priredio: I. Andreis; prijevod: T. Majić)

Internetski napadi na kritičnu infrastrukturu

Mi se u tolikoj oslanjamo na električnu struju da bi njezin dulji nestanak ugrozio sustave prijevoza, opskrbu vodom za piće, komunikacije i bankarstvo

Piše: Michael A. Mullane

Zlonamjerni hakeri prijete javnoj sigurnosti širom svijeta. Naprimjer, u Sjedinjenim Američkim Državama, u siječanjskom izdanju izvještaja *National Intelligence Strategy Report* upozorava se: "Internetske opasnosti predstavljat će sve veći rizik za javno zdravlje, sigurnost i napredak jer su informacijske tehnologije ugrađene u kritičnu infrastrukturu, vitalne nacionalne mreže i uređaje široke potrošnje". Obraćajući se Kongresu, direktor američke Nacionalne obavještajne službe, Daniel Coats rekao je to još jezgrovitije: "Alarmne lampice svijetle crveno".

Sve su češće mete objekti kritične infrastrukture, npr. elektrane ili razni oblici javnog prijevoza (foto: cegoh, Pixabay)

Sve su češće mete objekti kritične infrastrukture, npr. elektrane, nacionalne željeznice, lokalne podzemne željeznice ili drugi oblici javnog prijevoza. Internetski napadi mogu presjeći napajanje bolnica, domova, škola i tvornica električnom strujom. Toliko se oslanjamo na djelotvornu opskrbu električnom strujom da bi njezin nestanak imao teške posljedice za druge vitalne usluge. Brojni incidenti proteklih godina pokazuju ne samo da je opasnost opipljiva nego i da smo u više navrata za dlaku izbjegli katastrofalne posljedice.

Sljedeća tri primjera ilustriraju razvoj internetskog oružja, uključujući maliciozne programe (*malware*) namijenjene ometanju funkcije kritične infrastrukture. Iako je sve veća upotreba umreženih senzora i

drugih uređaja povezanih na internet u industriji donijela koristi u smislu učinkovitosti, povećala je i površinu otvorenu za napade.

Tri puta je svijetu stao dah

Napad na nuklearnu elektranu u Natanzu u Iranu 2010. godine ima posebno mjesto u povijesnim udžbenicima. Tako se prvi put u javnosti pokazao takozvani Stuxnet maliciozni program, uspjevši zaustaviti nuklearnu elektranu. Crv Stuxnet programiran je tako da oštećuje motore koji se uobičajeno upotrebljavaju u centrifugama za obogaćivanje urana jer ih navodi da se nekontrolirano vrte. Uspio je privremeno zaustaviti 1.000 centrifuga.

Pet godina kasnije, u prosincu 2015. godine, Ukrajina je doživjela neviđen napad na svoju elektroprivrednu mrežu. Napad je izazvao nestanak struje na brojnim lokacijama. Hakeri su provalili u tri energetske tvrtke i privremeno zaustavili proizvodnju električne energije u tri ukrajinske regije. Gotovo četvrt milijuna ljudi bilo je bez struje čak šest sati usred zime. Napadači su zatvorili tri trafostanice pomoću malicioznog programa BlackEnergy 3. Vjeruje se da je maliciozni program stigao porukama e-pošte programom *spear phishing* , skriven u lažnim prilozima Microsoft Office.

Treći i najalarmantniji napad za koji znamo dogodio se 2017. godine. Internetski teroristi preuzeli su daljinsku kontrolu nad tvornicom koja se prema napisima nalazi u Saudijskoj Arabiji. Pomoću nove vrste malicioznog programa koji je nazvan Triton preuzeli su sigurnosni instrumentacijski sustav tvornice (*safety instrumented system* (SIS)). I taj je maliciozni program bio konfiguriran posebno za industrijske kontrolne sustave, koji se nazivaju i operativnom tehnologijom (OT).

Istražitelji vjeruju da se radilo o sabotaži kojoj je cilj bio izazvati eksploziju onemogućivanjem sigurnosnih sustava namijenjenih sprječavanju katastrofalnih industrijskih nesreća. Prethodni napadi bili su usmjereni na uništavanje podataka ili zatvaranje elektrana. Neki stručnjaci tvrde da je napad spriječen samo zahvaljujući pogrešci u kodiranju. Dokazi upućuju na to da se i tu radilo o *phishing* ili *spear phishing* napadu.

Što je naučeno

Ti nam incidenti pokazuju da hakeri najmanje već deset godina razvijaju maliciozne programe kojima je cilj operativna tehnologija. Činjenica da su sva tri napada izazvana malicioznim programima također ukazuje na potrebu za cjelovitim pristupom internetskoj sigurnosti koji obuhvaća procese, tehnologije i ljude.

Generalni direktor tvrtke koja se bavi internetskom sigurnošću *Security in Depth*, Michael Connory, nedavno je TV kući *Australian Broadcasting Corporation* (ABC) rekao: “Devedeset posto internetskih napada širom svijeta počinje e-mailom”. Neupitno je da snaga internetske sigurnosti ovisi o snazi najslabije karike u lancu.

Drugo je ključno pitanje razumjeti razliku između IT-a i OT-a. Operativna tehnologija postaje sve pristupačnija, zbog čega se opasnosti sada proširuju sve do najosnovnije imovine kao što su pametni termostati. Izazov se sastoji u tome što se programi internetske sigurnosti prečesto temelje na IT-u. Međutim, u stvarnosti, operativna ograničenja u sektorima djelatnosti kao što je energetika, a i u mnogim drugima uključujući proizvodnju, zdravstvo i prijevoz, znače da se za internetsku sigurnost često treba usvojiti pristup koji se temelji i na OT-u.

Glavno su težište IT-a podaci i njihova sposobnost slobodnog i sigurnog protoka. IT postoji u virtualnom svijetu, gdje se podaci spremaju, učitavaju, prenose i njima se rukuje. IT je kao fluid, s brojnim pokretnim dijelovima i ulazima, zbog čega je iznimno ranjiv i nudi široku površinu za raznorazne napade, koji se stalno mijenjaju. Za obranu od napada potrebno je zaštititi svaki sloj, a također i stalno otkrivati i ispravljati slabe točke kako bi se očuvao protok podataka.

Za razliku od toga, OT spada u fizički svijet, gdje osigurava ispravno izvršavanje svih radnji. Dok IT treba zaštititi svaki sloj sustava, OT održava kontrolu nad sustavima – uključenim ili isključenim, zatvorenim ili otvorenim. OT sustavi namijenjeni su konkretnim radnjama, npr. osiguravanju uključivanja ili isključivanja generatora ili otvaranju preljevnog ventila kad je spremnik s kemikalijama pun. OT spada u fizički svijet, gdje osigurava sigurnost i kontrolu nad onim što je nekad predstavljalo zatvorene sustave. Sve u OT-u prilagođava se prema fizičkom kretanju i kontroli uređaja i procesa kako bi sustavi funkcionirali u skladu s namjenom, s glavnim težištem na sigurnosti i povećanoj učinkovitosti.

S pojavom industrijskog interneta stvari (IIoT) i objedinjavanjem fizičkih strojeva s umreženim senzorima i programima, briše se granica između IT-a i OT-a. S obzirom da je sve više predmeta spojeno internetom, međusobno komunicira i djeluje, dolazi do ogromnog porasta broja završnih točaka i načina na koji kriminalci mogu pristupiti mrežama i infrastrukturnim sustavima.

Intervencijom se ugasi vatra, ali se ne rješavaju osnovni uzroci. Nužno je početi razmatrati sigurnosne prijetnje već u fazi početnog projektiranja i razvoja. U brojnim slučajevima, organizacije promatraju sigurnost tek nakon provedbe, umjesto da grade otpornost na internetske napade na samom početku razvoja. Rad IEC-ovog tehničkog odbora (TC) 57 dobar je primjer normizacije najbolje prakse.

Sigurnost pomoću dizajna

IEC TC 57 osnovao je radnu skupinu (WG 15) koja se bavi sigurnošću elektroenergetskih mreža na temelju dizajna. Radna skupina, koja ocjenjuje zahtjeve s gledišta tehnologije i definira normirani način njihove provedbe, utvrdila je komponente potrebne za elektroenergetski sustav siguran na temelju dizajna. One uključuju načelo šifriranja s kraja na kraj (*end-to-end encryption*), definiranje uloga za sve korisnike i upravljanje identitetima te sveprisutan nadzor nad samim sustavom.

“Sve što učinimo danas postojat će sutra, ali trebamo promijeniti težište”, kaže član WG 15 Moreno Carullo. „Prestanimo samo tražiti negativce i počnimo se baviti sigurnošću pomoću dizajna.“

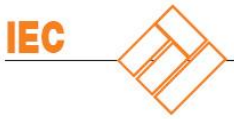
Trenutačno niz normi IEC 62351 (vidi IEC 62351-1: *Introduction for an in-depth overview*) opisuje arhitekturu sigurnoga elektroenergetskog sustava i normira njegove protokole i komponente. Radi boljeg pregleda, preporučljivo je pročitati IEC 62351-10: *Security Architecture Guidelines for TC 57 Systems*.

Norme i ocjenjivanje sukladnosti

IEC vjeruje da je pristup utemeljen na rizicima najbolji način za izgradnju otpornosti na internetske napade. Pristup utemeljen na rizicima može biti iznimno djelotvoran ako se temelji na procjeni postojećih ili mogućih internih ranjivih točaka i utvrđenih ili mogućih vanjskih prijetnji. To najbolje funkcionira u okviru cjelovitog pristupa u kojem se norme objedinjuju s ispitivanjem i certifikacijom, a koji je poznat kao ocjenjivanje sukladnosti, umjesto da se s opasnostima postupa kao s odvojenim područjima.

Takav pristup povećava povjerenje dionika jer dokazuje ne samo primjenu sigurnosnih mjera utemeljenih na najboljoj praksi nego i da je organizacija uvela te mjere učinkovito i djelotvorno. Sustavni pristup funkcionira kroz određivanje prioriteta i ublažavanje rizika do prihvatljive razine, što zahtijeva neutralan pristup uz primjenu različitih vrsta ocjene sukladnosti - od samoocjenjivanja poduzeća do nezavisnog ispitivanja treće strane - što se god čini primjerenim za razine rizika.

Mnoge organizacije temelje svoju strategiju internetske sigurnosti na usklađenosti s obveznim pravilima i propisima. To može dovesti do veće sigurnosti, ali ne može na sveobuhvatan način ispuniti potrebe pojedinačnih organizacija. Najčvršća obrana oslanja se i na‘horizontalne’ i na „vertikalne’ norme. Horizontalne norme općenite su i fleksibilne, dok vertikalne norme brinu za posebne potrebe. Ističu se dva primjera horizontalnih normi.



Novosti iz međunarodnih i europskih normizacijskih organizacija

Horizontalne i vertikalne norme

Niz normi ISO/IEC 27000 normi pomaže da se zaštite čisti informacijski sustavi (IT) i osigura slobodan protok podataka u virtualnom svijetu. Osigurava čvrst horizontalni okvir za usporedbu s najboljom praksom u provedbi, održavanju i trajnom poboljšavanju kontrolnih mehanizama.

IEC 62443, drugi niz horizontalnih normi, namijenjen je funkcioniranju sustava OT u stvarnom svijetu. Može se primjenjivati u svakom industrijskom okruženju, uključujući objekte kritične infrastrukture kao što su elektrane i nuklearne elektrane te u sektoru zdravstva i prijevoza. Programom industrijske internetske sigurnosti IECEE-a — IEC-ovog sustava shema ocjene sukladnosti elektrotehničke opremu i sastavnica — nude se globalne certifikacijske usluge na temelju niza normi IEC 62443.

Horizontalne norme nadopunjuju se krojenim rješenjima namijenjenim potrebama određenih sektora. Postoje vertikalne norme koje obuhvaćaju, između ostalog, posebne sigurnosne potrebe nuklearnog sektora, industrijskih komunikacijskih mreža, industrijske automatizacije i pomorstva.

Izgradnja otpornosti

Cilj je svake strategije internetske sigurnosti zaštititi što više stavki imovine, ali u svakom slučaju one najvažnije. S obzirom da nije izvedivo zaštititi sve u jednakoj mjeri, važno je utvrditi što je vrijedno i treba najveću zaštitu, utvrditi ranjive točke, a zatim odrediti prioritete i izgraditi arhitekturu dubinske obrane koja osigurava poslovni kontinuitet.

Najsigurniji pristup ostvarenju otpornosti obuhvaća razumijevanje i ublažavanje rizika s ciljem da se primijeni ispravna zaštita na odgovarajućim točkama u sustavu. Od velike je važnosti da taj proces bude dobro usklađen s ciljevima organizacije jer odluke o ublažavanju mogu imati ozbiljan utjecaj na poslove. U idealnom slučaju proces se temelji na sustavnom pristupu koji uključuje dionike iz čitave organizacije.

Ključni je koncept dubinske obrane (*defence-in-depth*) da je za sigurnost nužan skup koordiniranih mjera. Četiri su koraka nužna da bi se riješio rizik i posljedice internetskog napada:

1. poznavati sustav i utvrditi što je vrijedno i treba najveću zaštitu
2. shvatiti poznate opasnosti putem izrade modela opasnosti i procjene rizika
3. baviti se rizicima i primijeniti zaštitu pomoću međunarodnih normi, koje odražavaju najbolju svjetsku praksu
4. primijeniti odgovarajuću razinu ocjenjivanja sukladnosti – ispitivanja i certifikacije – u odnosu na zahtjeve.

Drugi je način abeceda internetske sigurnosti:

A. procjena (**a**ssessment)

B. najbolja praksa za bavljenje rizicima (**b**est practices)

C. ocjena sukladnosti za praćenje i održavanje (**c**onformity assessment).

Sustavni pristup utemeljen na rizicima povećava povjerenje svih dionika jer dokazuje ne samo primjenu sigurnosnih mjera utemeljenih na najboljoj praksi nego i da je organizacija uvela te mjere učinkovito i djelotvorno. To znači kombiniranje pravih normi s pravom razinom ocjene sukladnosti, umjesto da se s njima postupa kao sa zasebnim područjima.

Internetski napadi mogu presjeći napajanje bolnica, domova, škola i tvornica električnom strujom (fotografija: Nicole Köhler, Pixabay)

Svrha je ocjene sukladnosti procijeniti komponente sustava, osposobljenost osoblja koje ga projektira, vodi i održava te procese i postupke pomoću kojih se sustav vodi. To može značiti primjenu različitih vrsta ocjene sukladnosti - od samoocjenjivanja poduzeća do oslanjanja na izjave dobavljača ili nezavisne procjene i nezavisne procjene i ispitivanja treće strane – što se god čini primjerenim za razine rizika.

U svijetu u kojem su internetske opasnosti sve češće, mogućnost primjene određenog skupa međunarodnih normi u kombinaciji s namjenskim globalnim programom certifikacije dokazan je i visokodjelotvoran pristup u izgradnji dugoročne internetske otpornosti. Međutim, norme i ocjenjivanje sukladnosti mogu imati najveći učinak samo ako su dio pristupa utemeljenog na rizicima i cjelovitoj ocjeni prijetnji i ranjivih točaka. Takav pristup obuhvaća ne samo tehnologiju i procese nego i ljude, prepoznajući bitnu ulogu edukacije.

(Izvor: https://iecetech.org/Technology-Focus/2019-02/Cyber-attacks-targeting-critical-infrastructure; priredio: V. Jaram; prijevod: T. Majić)

ISO Novosti iz međunarodnih i europskih normizacijskih organizacija

Norma ISO 18091 donosi održivi razvoj lokalnim vlastima

Lokalne vlasti upravljaju svime, od prijevoza i odvodnje do javne rasvjete i civilne zaštite, pa nije neobično da građani od njih puno očekuju. Nedavno prerađene smjernice pomažu im da unaprijede svoje aktivnosti i usklade ih s lokalnim potrebama i očekivanjima radi zdravije i sigurnije zajednice.

U svakoj zemlji, javni je sektor najveći pružatelj usluga i nudi široki spektar usluga koje izravno utječu na život stanovnika. Među brojnim je izazovima i usklađivanje očekivanja građana s ograničenjima proračuna, utjecajima na okoliš i demografskim promjenama. U vremenima gospodarske krize, lokalne vlasti trebaju djelotvorno upravljati dostupnim resursima i procesima te funkcionirati zajedno kao sustav.

U tome značajnu ulogu ima norma ISO 18091, *Quality management systems – Guidelines for the application of ISO 9001 in local government* (Sustavi upravljanja kvalitetom -- Smjernice za primjenu ISO 9001:2008 u lokalnoj upravi). Svrha je te nedavno prerađene norme pomoći lokalnim tijelima da održe visoku razinu usluga, istodobno poboljšavajući održivost. Norma daje dijagnostičke modele i alate za provedbu sveobuhvatnog sustava upravljanja kvalitetom koji će pridonijeti ne samo učinkovitosti nego i pouzdanosti lokalnih tijela.

Stručnjak za lokalne vlasti Carlos Gadsden, voditelj tehničkog odbora koji je preradio normu, ističe da možemo izgraditi jače regionalne, nacionalne i međunarodne vlasti jednostavno jačajući moralni integritet u lokalnom upravljanju. Kaže: “ISO 18091 izvrstan je alat kojim lokalne vlasti mogu uvjeriti građane da u potpunosti razumiju njihove potrebe i očekivanja te ih dosljedno i pravovremeno ispunjavaju.“

ISO 18091 prva je ISO-ova norma usmjerena na javni sektor koja daje smjernice za primjenu norme ISO 9001 u lokalnoj upravi, uzimajući u obzir kontekst u kojem rade. Izmijenjena je tako da uključi zahtjeve norme ISO 9001:2015 za sustave upravljanja kvalitetom i niz dodataka koji pomažu korisnima da na najbolji način iskoriste tu normu, uključujući dijagnostičku metodologiju kojom lokalna tijela mogu ocijeniti opseg i zrelost svojih procesa i usluga.

Kako objašnjava Gadsden, ne radi se samo o dokumentu za stručnjake, nego o bitnom alatu za političare, kojim oni mogu učiniti „politički izvedivim“ ono što je stručno obvezno u lokalnoj upravi i na teritoriju njihove nadležnosti. “Lokalne vlasti mogu primijeniti te dodatke kako bi procijenile svoj napredak u odnosu na svih 17 ciljeva održivog razvoja (SDG) Ujedinjenih naroda[1)] i osigurale kontinuitet uspješnosti uprave u provedbi SDG-a na lokalnoj razini”, kaže. “To će im pomoći da budu učinkovitije i time štede resurse, da donose odluke na temelju dokaza, povećaju uključenost i, napokon, ugrade SDG u lokalni kontekst.”

1) Ciljevi održivog razvoja dio su Programa Ujedinjenih naroda za održivi razvoj do 2030. godine (*United Nations 2030 Agenda for Sustainable Development*), svjetskog plana akcije za ljude, planet i napredak sada i u budućnosti.

Normu ISO 18091 izradio je tehnički odbor ISO/TC 176, *Quality management and quality assurance*, koji je izradio i normu ISO 9001, i čije tajništvo vodi SCC, član ISO-a iz Kanade. Može se nabaviti kod nacionalnog člana ISO-a ili putem mrežne trgovine ISO Store.

(Izvor: Elizabeth Gasiorowski-Denis, 26. ožujka 2019.; https://www.iso.org/news/ref2378.html; priredio: V. Jaram; prijevod: T. Majić)

ISO Novosti iz međunarodnih i europskih normizacijskih organizacija

Kako pristupiti današnjim rizicima informatičke sigurnosti

Stručnjaci u djelatnosti procjenjuju da bi sljedeće godine godišnji gubici zbog internetskog kriminala mogli porasti na 2 bilijuna USD[1)]. S obzirom da broj meta svakodnevno raste, osobito među mobilnim uređajima i spojenim „stvarima“, nužan je udruženi pristup.

Privlačnost internetskog kriminala za hakere očita je: isprepletene mreže međudjelovanja, relativno male kazne, nepovezani pristupi pranju novca i velike mogućnosti zarade. Ključna je priprema i raspoznavanje ranjivih točaka te otpornost u smislu međudjelovanja s općim sustavima upravljanja, a tu svoju ulogu ima norma za sustave upravljanja informacijskom sigurnošću (ISMS) ISO/IEC 27001.

To je vodeća norma niza normi ISO/IEC 27000, koja je prvi put objavljena prije više od 20 godina. Norma, koju je izradio ISO/IEC JTC 1, zajednički tehnički odbor ISO-a i Međunarodnog elektrotehničkog povjerenstva (IEC) radi formalne normizacije u informacijskoj tehnologiji, stalno se prerađuje i proširuje kako bi uključila više od 40 međunarodnih normi koje obuhvaćaju sve, od stvaranja zajedničkog nazivlja (ISO/IEC 27000), upravljanja rizicima (ISO/IEC 27005) i sigurnosti oblaka (ISO/IEC 27017 i ISO/IEC 27018) do forenzičkih tehnika za analizu digitalnih dokaza i istraživanje incidenata (ISO/IEC 27042 odnosno ISO/IEC 27043).

Te norme ne pomažu samo u upravljanju informacijskom sigurnošću nego i u otkrivanju i dovođenju kriminalaca pred sud. Naprimjer, ISO/IEC 27043 nudi smjernice koje opisuju procese i načela primjenjiva na razne vrste istraga, uključujući između ostalog neovlašteni pristup, kvarenje podataka, padove sustava ili korporativne povrede informacijske sigurnosti te druge digitalne istrage.

1) Steve Morgan, “Cyber Crime Costs Projected To Reach $2 Trillion by 2019”, Forbes Online

I dalje voditi igru

Brinuti se da taj niz normi ostane prikladan za potrebe tvrtki, kako malih i velikih, kroz proces stalnog razvoja ozbiljna je odgovornost pododbora SC 27 za tehnike informacijske sigurnosti odbora ISO/IEC JTC 1. To što je i dalje jedan od najdjelotvornijih alata za upravljanja rizicima kojim se svake godine odbiju milijarde napada[2)], koji se isto tako razvijaju s obzirom na ciljeve i metode, velikim je dijelom zasluga ljudi kao što je prof. Edward Humphreys, predsjednik radne skupine koja je zadužena za razvoj ISMS-a.

Razgovarao sam s profesorom Humphreysom, stručnjakom za informacijsku sigurnost i upravljanje rizicima s više od 37 godina iskustva u savjetovanju i istraživanju. Na početku sam ga upitao o osnovama ISMS-a. Kako je moguće biti korak ispred kriminalaca i zaštititi gospodarstvenike i potrošače? „Istina je da se rizici koji ugrožavaju informacije, poslovne procese, aplikacije i usluge stalno razvijaju. ISO/IEC 27001 je norma za trajno poboljšavanje, što znači da ugrađeni proces upravljanja rizicima omogućuje poslovnim subjektima da budu korak ispred u borbi protiv internetskog kriminala."

Prema prof. Humphreysu, aspekt norme ISO/IEC 27001 koji se odnosi na trajno poboljšavanje znači da organizacija može procijeniti svoje rizike, uvesti kontrole za njihovo ublažavanje, a zatim pratiti i ocjenjivati svoje rizike i kontrole, po potrebi poboljšavajući zaštitu. Na taj je način uvijek spremna za napade. „Ako se ispravno primjenjuje, ISMS omogućuje organizaciji da vodi igru, reagirajući na promjene rizika koje predstavlja internet."

Od opasnosti do prilika

Na poslovnoj razini ostaje golem zadatak modeliranja i ublažavanja opasnosti iz svih zamislivih uglova. Jasna je potreba za primjenom jedinstvenog i objedinjenog sigurnosnog sustava za čitavu tvrtku, a, s obzirom na složenost međuodnosa, upitao sam prof. Humphreysa može li se ISMS primijeniti na mala i srednja poduzeća (MSP). „ISMS je primjenjiv na sve vrste organizacija i sve vrste poslovnih aktivnosti, uključujući MSP. Mnogi MSP dio su lanaca opskrbe, pa je nužno da imaju kontrolu nad svojom informacijskom sigurnošću i internetskim rizicima kako bi zaštitili i sebe i druge." Prof. Humphreys objašnjava da su obveze tvrtke obično definirane u ugovorima o razini usluga (SLA)

2) "Internet Security Threat Report", Volume 23, Symantec, 2018

među partnerima u lancu opskrbe kojima se utvrđuju obveze i zahtjevi usluga i uspostavljaju zakonske obveze, te da je ISMS često sastavni dio takvih ugovora.

Naravno, internetsko poslovanje MSP-a može biti spojeno s teškoćama, ali donosi i ogromne potencijale. Moglo bi se tvrditi da je tehnologija najviše prednosti donijela upravo malim tvrtkama, što je nedavno izjavio ambasador Alan Wolff iz Svjetske trgovinske organizacije. Govoreći na Općoj skupštini ISO-a 2018. godine, Wolff je primijetio da „svatko tko ima ideju, računalo, pristup mreži i pristup platformi može postati dio međunarodne trgovine."

Prednosti za društveni i gospodarski razvoj ogromne su: internet dopire do nekada izoliranih pojedinaca i zajednica u cijelom svijetu. Međutim, da bi se ublažili nedostaci, potreban je dokazan i razborit pristup kao što je ISMS. Kao što me podsjetio prof. Humphreys, „internetski napad na jednoj strani lanca opskrbe može narušiti čitav lanac", a posljedice mogu zahvatiti mnogo više od vaše tvrtke i direktnih kupaca. To vrijedi kako za zanatlije koji izrađuju igračke na Baliju tako i za nacionalne zdravstvene sustave u Europi.

Pravo na privatnost i potreba za povjerljivošću

Naš privatni život možda je manje složen od globalnog poslovanja, ali ipak je mnogo toga na kocki. Za mnoge od nas, da bismo se sačuvali od internetskih kriminalaca, u većini slučajeva trebalo bi biti dovoljno slijediti najbolju praksu u pogledu lozinki i obnavljanja sigurnosti (imajući na umu da, ako nešto izgleda sumnjivo, ili predobro da bi bilo istinito, onda vjerojatno jest sumnjivo). Ipak, ljude sve više zanima kako institucije i tvrtke spremaju, analiziraju i unovčuju ogromne količine podataka koji im dajemo više ili manje dobrovoljno.

Pitao sam prof. Humphreysa daje li niz normi ISO/IEC 27000 odgovor na takve nepoznanice. "Nedavno je pododbor SC 27 počeo raditi na novom projektu – normi ISO/IEC 27552 – koja se nadovezuje na ISO/IEC 27001 baveći se potrebama za privatnošću." Dokument, koji je u fazi nacrta, utvrđuje zahtjeve i daje smjernice za uspostavu, provedbu, održavanje i trajno poboljšavanje upravljanja privatnošću u kontekstu organizacije.

Kad je ugrožena privatnost, financije, reputacija pojedinca ili tvrtke, to narušava povjerenje i utječe na naše ponašanje, i na internetu i u stvarnom životu. Uloga niza normi ISO/IEC 27000 u našem daljnjem

napretku od ogromne je važnosti. Uz brojne razloge za bojazan zbog digitalizacije gotovo svakog aspekta života, utješno je znati da postoji niz normi na koji možemo računati u vezi sa sustavima upravljanja informacijskom sigurnošću i da svjetska skupina stručnjaka poput prof. Humphreysa radi na tome da bude korak ispred.

(Izvor: Barnaby Lewis, 10. siječnja 2019.; https://www.iso.org/news/ref2360.html; priredio: V. Jaram; prijevod: T. Majić)

Nova CEN-ova norma: Bolje dijagnoze uz niz normi EN ISO 20166:2018 ‘Molekularna in vitro dijagnostička ispitivanja’

Europske norme imaju ključnu ulogu u sigurnom pristupu zdravstvenoj zaštiti za pacijente jer utvrđuju zahtjeve za medicinske proizvode s obzirom na sigurnost, kvalitetu i svojstva. U tom kontekstu, da bi se osigurala visoka razina zdravstvene zaštite i prevencije nužno je osigurati ispravne i pravovremene dijagnoze.

Da bi se smanjio rizik neobjektivnih dijagnoza i povećala sigurnost, CEN je nedavno objavio niz normi EN 20166:2018 ‘Molecular in vitro diagnostic examinations - Specifications for pre-examination processes for formalin-fixed and paraffin-embedded (FFPE) tissue’ (Molekularna in vitro dijagnostička ispitivanja – Specifikacije za postupke prije ispitivanja za tkivo fiksirano formalinom i uronjeno u parafin (FFPE) – 1. dio: Izolirana RNK). Tri njegova dijela, koji se odnose na izoliranu RNK, izolirane proteine odnosno izoliranu DNK, obuhvaćaju procese pripreme analize, počevši od uzimanja uzoraka do postupanja, dokumentiranja, pohrane i obrade uzoraka te izolacije raznih tvari.

Norme niza 20166 namijenjene su posebno za molekularna in vitro dijagnostička ispitivanja, uključujući laboratorijska ispitivanja, koja provode medicinski laboratoriji i laboratoriji za molekularnu patologiju. Primjenjive su i na druge dionike kao što su proizvođači in vitro dijagnostike, banke bioloških uzoraka, institucije i tvrtke koje se bave biomedicinskim istraživanjima te nadzorna tijela.

Cilj je ovog niza normi smanjiti utjecaj vanjskih faktora na rezultate pretraga, osiguravajući da pacijenti dobiju što objektivniju dijagnozu. Istraživanja su dala jasne znanstvene dokaze da nekoliko faktora u fazi prije pretrage utječu na ishod in situ otkrivanja te mogu imati značajan učinak na dijagnostičke rezultate. S obzirom da pouzdanost analitičkih rezultata pretraga u velikoj mjeri ovisi o ispravnoj obradi bioloških uzoraka u fazi prije pretrage, nužna je visoka razina normizacije postupaka u toj fazi.

Niz EN ISO 20166:2018 izrađen je u okviru 4,5-godišnjeg projekta SPIDIA koji je financirala Europska unija. Doprinos sadržaju specifikacija dali su projektni partneri i predstavnici šire zajednice proizvođača, europskih i međunarodnih istraživačkih udruženja, korisnika i znanstvenika. Njegov nasljednik, 48-mjesečni projekt SPIDIA4P (**S**tandardization of generic **P**re-analytical Procedures **for I**n vitro **DIA**gnostics for **P**ersonalised Medicine), preuzeo je rad na normizaciji i poboljšanju predanalitičkih postupaka za in vitro dijagnostiku.

Niz normi izradio je tehnički odbor CEN/TC 140, 'In vitro diagnostic medical devices' u bliskoj suradnji s tehničkim odborom ISO/TC 212, 'Clinical laboratory testing and in vitro diagnostic test systems'. Tajništvo odbora CEN/TC 140 vodi DIN, nacionalno normizacijsko tijelo Njemačke, koji je jedan od partnera u projektima SPIDIA i SPIDIA4P.

Projekt SPIDIA financiran je iz Sedmog okvirnog programa za istraživanje (*Seventh Research Framework Programme*) Europske unije, FP7-HEALTH-2007-1.2.5, prema ugovoru o potpori br. 222916.

Projekt SPIDIA4P financira se iz Obzora 2020. (Horizon 2020), programa Europske unije za istraživanje i inovacije za razdoblje od 2014. do 2020. godine prema ugovoru o potpori br. 733112.

(Izvor: https://www.cen.eu/news/brief-news/Pages/NEWS-2019-010.aspx ; priredio: V.Jaram; prijevod: T. Majić)

Novi niz normi EN ISO 10855 daje međunarodno priznate smjernice za odobalne spremnike

Niz normi **EN ISO 10855 'Offshore containers and associated lifting sets'** (Odobalni spremnici i pripadajući pribor za dizanje), koji je CEN prihvatio 2018. godine, sastoji se od tri dijela: 1. dio: Projektiranje, proizvodnja i obilježavanje odobalnih spremnika; 2. dio: Projektiranje, proizvodnja i označivanje pribora za dizanje; i 3. dio: Periodička inspekcija, provjera i ispitivanje. Niz kao takav opisuje zahtjeve za projektiranje, konstrukciju, inspekciju, ispitivanje i provjeru u radu odobalnih spremnika i pripadajućeg pribora za dizanje za naftnu, petrokemijsku i industriju prirodnog plina.

Nizom EN-ISO 10855 prihvaćen je niz međunarodnih normi ISO 10855 na europskoj razini. ISO norma nastala je objedinjavanjem postojećih normi europskih, američkih i klasifikacijskih tijela u jedan usklađeni sporazum. Njezino prihvaćanje u Europi osigurava europskom sektoru nafte i plina pristup globalnom usklađenom i prihvaćenom skupu zahtjeva za odobalne spremnike, s jasnim prednostima u pogledu interoperabilnosti, sigurnosti i troškovne učinkovitosti u sektoru koji je po definiciji globalan.

Ron Winands, predsjednik Uprave organizacije *Control Union Testing & Inspection*, koji je kao stručnjak sudjelovao u izradi niza normi, objašnjava njegovu dodanu vrijednost: „pod uvjetima prijevoza i rukovanja odobalnim spremnicima, 'normalna' brzina trošenja i habanja vrlo je visoka i dovodi do oštećenja koja zahtijevaju popravke. Međutim, spremnici projektirani, proizvedeni i redovito pregledavani prema nizu normi EN ISO 10855 trebali bi imati dovoljnu čvrstoću da izdrže normalne sile u odobalnim poslovima."

Norma također osigurava da su odobalni spremnici sukladni sa zahtjevima IMO-a, Međunarodne pomorske organizacije, koji se odnose na projektiranje, konstrukciju, inspekciju, ispitivanje i provjere u radu. Pritom niz EN ISO 10855 ne donosi preklapanja; ne utvrđuje certifikacijske zahtjeve za odobalne spremnike koji su već obuhvaćeni dokumentom IMO MSC / Circular 860 i Međunarodnom konvencijom o zaštiti ljudskih života na moru (SOLAS). Naprimjer, dokumentom IMO MSC / Circular 860 već se zahtijeva certifikacija odobalnih spremnika od strane nacionalnih vlasti ili propisno ovlaštenih organizacija. Certifikat o sukladnosti opisan u EN ISO 10855 u skladu je s dokumentom IMO MSC / Circular 860. To je dobar primjer kako normizacija pridonosi usklađenosti s propisima.

Niz normi EN ISO 10855, nastao u okviru ISO-a, objavio je tehnički odbor CEN/TC 12, 'Materials, equipment and offshore structures for petroleum, petrochemical and natural gas industries', čije

tajništvo zajednički vode NEN, nacionalno normizacijsko tijelo iz Nizozemske, i CYS, nacionalno normizacijsko tijelo iz Cipra.

Ovaj tekst temelji se na duljem članku objavljenom u 1. broju u 2019. godini časopisa Ocean Energy Resources, vodećeg stručnog časopisa u Nizozemskoj za industriju nafte i plina te obnovljivih izvora. Članak se nalazi na 24. stranici izdanja u PDF-u.

(Izvor: https://www.cen.eu/news/brief-news/Pages/NEWS-2019-17.aspx; priredio: V.Jaram; prijevod: T. Majić)