wiadomości PKN

• NORMALIZACJA •

12/2017

- *Cyberbezpieczeństwo*
- *Normalizacja dla Smart Cities*

12/2017

„**WIADOMOŚCI PKN**” to miesięcznik elektroniczny publikowany cyklicznie na stronie internetowej PKN www.pkn.pl od numeru 9/2011.

ZESPÓŁ REDAKCYJNY
Redaktor prowadzący:
Joanna Skalska – tel. 22 556 74 62
Redaktorzy:
Marta Hejduk – tel. 22 556 77 09
Aleksandra Kurzep – tel. 22 556 75 07
Skład:
Oskar Sztajer – tel. 22 556 77 62

REDAKCJA:
00-950 Warszawa, skr. poczt. 411
ul. Świętokrzyska 14
e-mail: redakcja@pkn.pl

WYDAWCA:
Polski Komitet Normalizacyjny, ul. Świętokrzyska 14, 00-050 Warszawa

Szanowni Czytelnicy!

Internet zmienił dużo w naszym codziennym życiu. Inaczej robimy zakupy, relaksujemy się czy uczymy. Z jednej strony wiele nam ułatwia i oszczędza czas. Doceniamy to szczególnie w okresie przedświątecznym, prawda? Z drugiej – internet to przestrzeń, w której można skraść nasze pieniądze, tożsamość. Wraz z jego rozwojem rozwija się też cyberprzestępstwo.
I o tym m.in. piszemy w bieżącym numerze i jak zwykle podkreślamy, że normy mają kluczowe znaczenie właśnie w ochronie infrastruktury krytycznej.
Tradycyjnie zachęcamy do zapoznania się ze wszystkimi artykułami tego numeru i tradycyjnie

Życzymy naszym Czytelnikom, Autorom i Sympatykom
spokojnych i radosnych Świąt Bożego Narodzenia
oraz szczęśliwego Nowego Roku

Redakcja „Wiadomości PKN”

Zmiany w procedurach PKN w 2018 r.

Jolanta Kochańska

Bezstronność Przewodniczącego KT/KZ/PK

PKN jako członek europejskich organizacji normalizacyjnych CEN/CENELEC przywiązuje dużą wagę do stosowanych procedur i dba o ich zgodność z przepisami wewnętrznymi CEN/CENELEC.

Organizacje te określają również warunki, jakie powinna spełniać krajowa jednostka normalizacyjna (w tym PKN), aby być ich członkiem. Warunki te zawarto w dwóch dokumentach:

- Przewodnik CEN-CENELEC nr 20 Kryteria członkostwa w CEN-CENELEC
- Przewodnik CEN-CENELEC nr 22 Wytyczne w sprawie organizacji i sposobu przeprowadzania oceny kryteriów członkostwa w CEN i CENELEC

Powyższe przewodniki były podstawą do przeprowadzenia w PKN auditu. Jego celem było ocenienie spełnienia przez PKN kryteriów członkostwa opisanych w Przewodniku nr 20. W wyniku auditu stwierdzono między innymi niezgodność w kategorii „Bezstronność i konsens" w zakresie praw Przewodniczącego OT.

Bezstronność dotyczy procesu, procedur jak również struktury organizacyjnej KJN (krajowej jednostki normalizacyjnej), tak aby zapewnić interesariuszom możliwość prowadzenia prac normalizacyjnych w neutralnych, niedyskryminujących i niefaworyzujących żadnej z grup warunkach.

Konsens odnosi się do procesu normalizacyjnego, który powinien polegać na współpracy, braniu pod uwagę wszystkich opinii i wypracowywaniu wspólnych stanowisk z przeciwstawnych poglądów.

Bezstronność powinna być zagwarantowana na każdym etapie opracowania normy, tj.: uczestnictwa w pracach normalizacyjnych, dostępie do dokumentów roboczych, rozpatrywaniu zgłoszonych uwag, podejmowaniu decyzji na zasadzie konsensu, otrzymywania informacji i dokumentów, udostępniania norm międzynarodowych, opłat za dokumenty, wprowadzenia normy międzynarodowej w j. polskim, przeglądu norm międzynarodowych.

Tak opisaną bezstronność powinien gwarantować Przewodniczący OT. Ma to także odzwierciedlenie w Przepisach wewnętrznych CEN-CENELEC, część 2: Wspólne reguły Prac Normalizacyjnych w punkcie 3.2.3.3 Odpowiedzialność przewodniczącego.

Biorąc pod uwagę wykazaną w audicie niezgodność oraz zobowiązanie do jej usunięcia do końca 2017 r., PKN wprowadza od 1 stycznia 2018 r. odpowiednie zmiany do Procedury Z2-P1 *Organizacja i zadania Organów Technicznych powoływanych w PKN*.

Przewodniczący KT/KZ ma być osobą bezstronną, w związku z tym:

- nie będzie głosował nad uchwałami KT/KZ;
- w zadaniach Przewodniczącego KT/KZ zostanie podkreślona bezstronność;
- zostanie wprowadzony okres przejściowy do 31.12.2018 r.

Członkowie OT, których Reprezentant upoważniony do głosowania jest Przewodniczącym OT, mają czas na uporządkowanie formalności i wskazanie nowego Reprezentanta upoważnionego do głosowania do 31 grudnia 2018 r.

O planach związanych z tymi zmianami Kierownictwo PKN informowało zarówno Radę Normalizacyjną, jak i Przewodniczących KT w listopadzie 2016 roku.

„Obowiązkiem przewodniczącego, podczas prowadzenia posiedzeń komitetu technicznego i kierowania sekretariatem, jest zachowanie ścisłej bezstronności i wyzbycie się własnego, krajowego punktu widzenia. Przewodniczący nie ma prawa do głosowania. Przewodniczący powinien dołożyć wszelkich możliwych starań, aby uzyskać jednomyślną decyzję komitetu technicznego. Jeżeli nie można uzyskać jednomyślności na dany temat, wówczas przewodniczący powinien starać się osiągnąć konsens, a nie podejmować decyzję na podstawie większości głosów".

Rola Przewodniczącego w KT lub TC jest podobna do roli mediatora

Na posiedzeniach KT i w uzgodnieniach powinno się stosować zasadę zapewniającą członkom KT gwarancję, że sprawy będą omawiane w obecności Przewodniczącego jako osoby neutralnej – niezainteresowanej rozstrzygnięciem ewentualnego sporu co do treści normy na korzyść którejkolwiek ze stron sporu. Bezstronność Przewodniczącego powinna wyrażać się głównie przez to, iż nie przychyla się do stanowiska żadnej ze stron, jest neutralnym obserwatorem sporów prowadzonych przez strony i moderatorem dyskusji. Przewodniczący w równy sposób traktuje każdą ze stron, nie faworyzuje żadnej z nich. Jednocześnie musi zachowywać się neutralnie i wykazywać obiektywne podejście do omawianych kwestii. Nie jest rolą Przewodniczącego rozstrzyganie sporu pomiędzy członkami. Głównym jego zadaniem jest dbanie o prowadzenie przez strony dyskusji w spokojnej atmosferze, która ma prowadzić do wypracowania kompromisu. Rola Przewodniczącego nie polega na biernym przyglądaniu i przysłuchiwaniu się dyskusji stron, ale w przypadku gdy widzi on taką potrzebę, może zasugerować pewne rozwiązania, wskazać na pewne propozycje kompromisowe, których strony nie dostrzegają bądź z braku odpowiedniej wiedzy nie mogą dostrzec. Może pojawić się wątpliwość i pytanie, czy powyższe działanie Przewodniczącego nie jest zbyt daleko idące i nie narusza zasady bezstronności. Nie dochodzi do naruszenia zasady bezstronności, jeśli rozwiązanie zaproponowane przez Przewodniczącego nie faworyzuje którejkolwiek ze stron, nie zmierza do wywołania skutków prawnych/ekonomicznych korzystnych wyłącznie dla jednej strony.

Zmiany w podejściu do głosowania w OT za pomocą PZN

Inną znaczącą zmianą w Procedurze Z2-P1 *Organizacja i zadania Organów Technicznych powoływanych w PKN* jest zmiana zasad głosowania w OT za pomocą PZN. Została ona wprowadzona ze względu na wiele uwag członków OT krytykujących obecne zasady głosowania. W związku z tym:

1. Głosowanie nad projektem normy jest uznane za ważne, jeśli w głosowaniu uczestniczyło min. 67% uprawnionych do głosowania. Przez uczestniczenie w głosowaniu rozumie się oddanie głosu na TAK, NIE lub WSTRZYMANIE SIĘ.
2. Dopóki trwa głosowanie uprawniony ma możliwość zmiany swojego głosu w systemie PZN bez konieczności pisemnego występowania o umożliwienie mu tego działania.
3. Nie ma możliwości zmiany terminu głosowania w trakcie jego trwania.
4. W przypadku braku konsensu w głosowaniu, dopuszcza się jego powtarzanie, przy czym czas trwania powtórzonych głosowań może zostać skrócony w uzgodnieniu z Przewodniczącym OT, jednak nie powinien być krótszy niż 7 dni.
5. Przy oddaniu głosu na NIE, głosujący ma obowiązek wpisać merytoryczne uzasadnienie takiej decyzji w odpowiednim polu w PZN.

W procedurze nowością jest również przedstawienie w formie tabelarycznej zastosowania poszczególnych głosowań do prac normalizacyjnych w OT, co powinno ułatwić użytkownikom korzystanie z procedury i wybór odpowiedniego typu głosowania do danej uchwały OT.

Rodzaje głosowań

Zwykła większość	Więcej głosów na „TAK” niż na „NIE” spośród biorących udział w głosowaniu.
Nominalna większość	Powyżej 1/2 głosów na „TAK”, przy udziale w głosowaniu co najmniej 2/3 upoważnionych do głosowania.
Kwalifikowana większość	Powyżej 1/2 głosów na „TAK i nie więcej niż 1/5 głosów na „NIE”, przy udziale w głosowaniu co najmniej 2/3 upoważnionych do głosowania.

Stanowisko KT do projektów norm prPN-prEN

Ogólne zasady dotyczące głosowania stanowiska KT nie zmieniły się, jednak ze względu na praktykę dyskutowania i przyjmowania bądź odrzucania uwag w CEN/TC lub CENELEC/TC wprowadzono zalecenie dotyczące głosowania przez KT, w przypadku gdy KT ma istotne uwagi do projektu normy i zależy mu szczególnie, aby takie uwagi zostały przyjęte przez CEN/TC lub CENELEC/TC. W takim przypadku zaleca się, aby KT głosowały NO (DISAPPROVE). Jest to także zalecenie Rad Technicznych CEN i CENELEC. Stąd odpowiednie zapisy w procedurze.

YES (APPROVE)	KT głosuje za projektem wówczas, gdy jest zainteresowanie krajowe tematyką, której dotyczy projekt i uzyskano konsens w sprawie poparcia projektu. W PZN odpowiada to sytuacji, gdy KT podejmuje uchwałę kwalifikowaną większością głosów za przyjęciem projektu normy. Stanowisko może zawierać uwagi redakcyjne do treści projektu.
NO (DISAPPROVE)	KT głosuje przeciw, wówczas gdy: • w kraju są użytkownicy zainteresowani tematyką, której dotyczy projekt normy i uzyskano konsens w sprawie odrzucenia projektu. W PZN odpowiada to sytuacji, gdy kwalifikowana większość (typ C, patrz pkt 5.1.4.1) głosuje przeciw przyjęciu normy; • treść projektu nie jest w pełni akceptowalna i zgłoszono uwagi techniczne, które wymagają rozpatrzenia na poziomie europejskim. Sprzeciw wymaga uzasadnienia merytorycznego (zestawienie uwag technicznych do projektu normy).

Wprowadzenie wymagań w zakresie kwalifikacji Sekretarza KT

Procedury PKN wymagają, aby Sekretarz KT jako osoba funkcyjna posiadał określone potwierdzone kwalifikacje do pełnienia tej funkcji.

PKN opracował obowiązkowe e-szkolenie dla Sekretarzy KT, które będzie zakończone testem i certyfikatem potwierdzającym podstawową wiedzę normalizacyjną. Szkolenie będzie dostępne na portalu wiedza.pkn.pl.

Osoby wyznaczone przez podmioty do prowadzenia sekretariatu KT będą zobowiązane do odbycia szkoleń przed objęciem funkcji Sekretarza. W przypadku nowych Sekretarzy KT „Szkolenie dla Członków i Reprezentantów członków Organów Technicznych" będzie także obowiązkowe. Obydwa szkolenia będą bezpłatne dla osób podejmujących obowiązki Sekretarza po raz pierwszy.

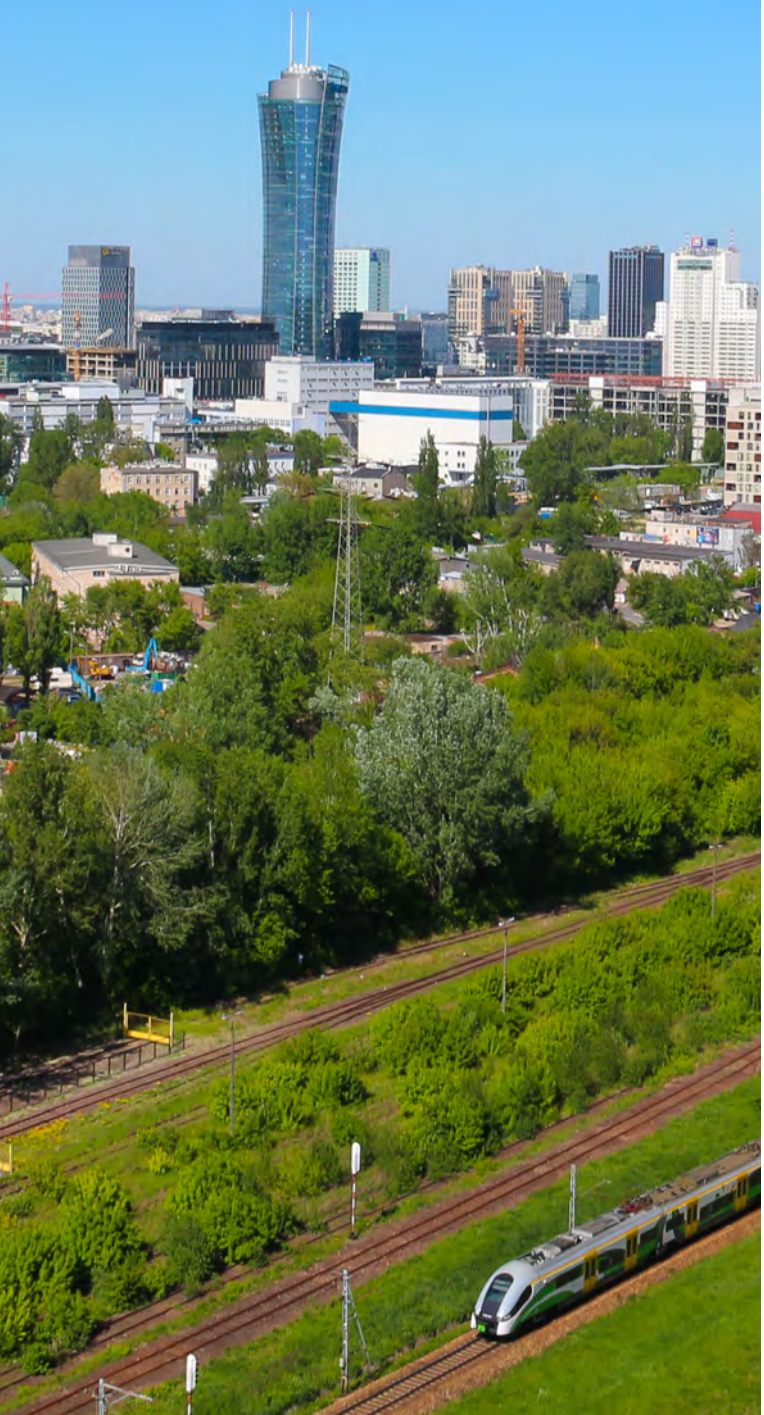
Osoby wyznaczone przez podmioty i pełniące już funkcję Sekretarza będą zobowiązane do odbycia „Szkolenia dla Sekretarzy Organów Technicznych". Szkolenie to będzie dla nich bezpłatne.

Szkolenie e-learningowe „Szkolenie dla Sekretarzy Organów Technicznych" będzie oferowane na portalu wiedza.pkn.pl również dla wszystkich innych zainteresowanych jako odpłatny produkt komercyjny.

Nowe e-szkolenie dla członków i reprezentantów członków OT

Szkolenie to będzie dostępne w formie komercyjnej – jako szkolenie dobrowolne wprowadzające w zagadnienia podstaw normalizacji i zasad pracy w organach technicznych. Szkolenie to powinno być dostępne na portalu wiedza.pkn.pl najpóźniej od lutego 2018 r.

NORMALIZACJA DLA SMART CITIES



Rok 2017 stał się czasem rozmów, wydarzeń, inicjatyw, działań szczególnie akcentujących problem rozwoju miast. Choć zajmują one niewielki procentowo obszar (zaledwie 2% powierzchni Ziemi), to mają największy wpływ na stan środowiska, klimat i komfort naszego życia. Polski Komitet Normalizacyjny, chcąc wspólnie z ekspertami i wszystkimi zainteresowanymi propagować i upowszechniać znormalizowane działania związane m.in. z bezpieczeństwem, innowacyjnością i godną jakością życia mieszkańców miast, zorganizował 16 listopada br. konferencję „Normalizacja dla Smart Cities". Tego dnia wspólnie zastanawialiśmy się nad celami, rozwiązaniami, najlepszymi praktykami, które kształtują i wspierają miasta inteligentne.

Konferencję otworzył **dr inż. Tomasz Schweitzer**, Prezes PKN, który podkreślił, że w inteligentnym i zrównoważonym rozwoju miast niezbędne są normy i uwzględnienie potrzeb przyszłych pokoleń.

Normalizację w aspekcie Smart Cities szerzej omówiła **Teresa Sosnowska**, Dyrektor Wydziału Prac Normalizacyjnych PKN, przybliżając inicjatywy międzynarodowe, regionalne i krajowe. Powiedziała m.in. o pracach Komitetu Technicznego ISO/TC 268 *Sustainable cities and communities*, opracowującego wymagania, ramy, wytyczne i narzędzia wspierające dążenia miast do osiągnięcia zrównoważonego rozwoju oraz o działaniach jego Podkomitetu *Smart community infrastructures* w zakresie inteligentnych infrastruktur miejskich. Rozwój norm z dziedziny elektrotechniki wspomagających integrację, interoperacyjność i efektywność systemów miejskich wspiera zaś Komitet Systemowy IEC *Electrotechnical aspects of smart cities*. Prelegentka zwróciła także uwagę, że znaczące są wspólne działania podejmowane przez organizacje normalizacyjne na rzecz inteligentnych miast. Jest to np. działalność ISO/IEC/JTC 1/WG 11 *Smart Cities*. Wspólną inicjatywą IEC, ISO, ITU jest platforma on-line do kontaktu i dyskusji wszystkich ekspertów i zainteresowanych szybkim rozwojem w kierunku wdrażania koncepcji i rozwiązań inteligentnych miast. Została też utworzona grupa doradcza europejskich organizacji normalizacyjnych – CEN-CLC-ETSI *Sector Forum on Smart and Sustainable Cities and Communities* – koordynująca europejskie prace normalizacyjne związane z obszarem SSCC, tworząca powiązania z odpowiednimi inicjatywami na szczeblu międzynarodowym, podejmująca działania ukierunkowane na pogłębianie świadomości co do roli norm jako kluczowych elementów budowy inteligentnych i zrównoważonych miast w Europie. Warto jeszcze dodać, że na szczeblu krajowym powołano Koordynacyjną Grupę Zadaniową PKN/KGZ 1 ds. Inteligentnego i Zrównoważonego Rozwoju Miast i Społeczności. To organ techniczny lustrzany do Forum sektorowego CEN-CLC-ETSI SSCC-SF, który umożliwia wymianę informacji na temat inicjatyw krajowych w obszarze tematycznym grupy, a ponadto obserwuje i opiniuje prace normalizacyjne na rzecz Smart Cities. Tylko więc aktywne uczestnictwo w pracach normalizacyjnych realizowanych na poziomie krajowym, regionalnym i międzynarodowym daje realny wpływ na kształt dokumentów normalizacyjnych, które w dziedzinie Smart Cities dotyczą m.in.: inteligentnego i zrównoważonego budownictwa, rozwoju społeczności, bezpieczeństwa, czystego powietrza, zaopatrzenia w wodę, ekologicznego transportu i wielu innych aspektów, które tworzą naszą codzienność w mieście.

Tomasz Schweitzer

Co sprawia, że miasto staje się inteligentne? O celach, korzyściach i wyzwaniach takiej transformacji powiedział **dr Tomasz Kulisiewicz**, Zastępca Dyrektora Ośrodka Studiów nad Cyfrowym Państwem. Miasto ma być przede wszystkim przyjaznym habitatem – dobrym miejscem do życia, gdzie zostaje zapewniony jego zrównoważony rozwój, a także rozwój jego mieszkańców. W związku z tym ważne jest też zwiększanie dobra wspólnego i kapitału społecznego. Prelegent przywołał koncepcje miast ogrodów i wskazał kilka zjawisk wpływających na polskie miasta, tj. ich depopulyzację i dezurbanizację, dezagraryzację wsi, pojawienie się „międzymieścia" *(stykają się ze sobą i mieszają ludnościowo niemiejskie miasta i niewiejskie wsie)*. Podkreślił, że kluczowym czynnikiem inteligentnego rozwoju jest inteligentna infrastruktura. Istotną przeszkodą zaś –

Teresa Sosnowska

Tomasz Kulisiewicz

Adam Kruczek

niski poziom interoperacyjności, silosowość jednostek urzędu, co przejawia się niedostatecznym poświęcaniem uwagi kwestiom współdziałania tworzonych rozwiązań informatycznych.

Na miasto smart składa się wiele czynników, które w dobie dygitalizacji, Internetu Rzeczy (IoT), ciągłego komunikowania muszą się ze sobą łączyć i współdziałać, dlatego też wyzwaniem staje się cyberbezpieczeństwo. **Dr Krzysztof Gawkowski**, Dyrektor Polskiego Instytutu Cyberbezpieczeństwa, mówił właśnie o realizacji bezpieczeństwa w strategii inteligentnego miasta. W myśleniu o bezpieczeństwie przenikają się różne obszary (energia, woda, cyfryzacja itp.), które być może nie od razu będą nam się z bezpieczeństwem kojarzyły. Dlatego też ważne jest podejście całościowe do tego zagadnienia. Należy zastanowić się, w jaki sposób dobrze zorganizować społeczeństwo, które umiejętnie to wszystko wykorzysta. Aby zadbać o bezpieczeństwo cyfrowe, należy zbierać krytyczne dane, integrować systemy, wskazywać punkty krytyczne, zastanawiać się nad dobrym wykorzystywaniem rewolucji cyfrowej, np. przez tworzenie mapy zagrożeń. Wszystko to ma także prowadzić do dobrego zabezpieczania danych, co jest współcześnie wymaganiem koniecznym.

Dr inż. Krzysztof Hajdrowski omówił inteligentne zarządzanie energią w kontekście zrównoważonego rozwoju miast z uwzględnieniem elektromobilności. Efektywność energetyczna, sieci inteligentne, zarządzanie energią to zagadnienia norm z obszaru konkurencyjnego, bezpiecznego i przyjaznego dla środowiska systemu elektroenergetycznego, którymi zajmuje się KT 304 ds. Aspektów Systemowych Dostawy Energii Elektrycznej. Energia w rozwoju miast jest kluczowa, wpływa na mobilność, zarządzanie, planowanie, budownictwo, technologie. Następuje nieunikniony rozwój inteligentnych maszyn i tym samym zmienia się intensywnie motoryzacja – od pojazdów spalinowych i hybrydowych, po elektryczne i autonomiczne. Zagadnieniem technicznym i technologicznym o dużym znaczeniu w kontekście inteligentnego zarządzania energią jest także jej magazynowanie.

Druga część konferencji poświęcona była natomiast praktycznym aspektom związanym

z certyfikowaniem Smart Cities. Bo w osiągnięciu statusu inteligentnego miasta niezbędne jest zbieranie danych, w sposób uporządkowany i obiektywny, oraz konfrontowanie ich z innymi ośrodkami miejskimi.

Adam Kruczek z ThinkIT Consulting scharakteryzował rolę, jaką odgrywa norma PN-ISO 37120 w kwestii oceny różnych obszarów rozwoju zrównoważonego miasta. Jak sprawdzić, czy przyjęta przez miasto strategia rozwoju jest właściwa, czy jej wdrażanie zapewnia jednak właściwy efekt, czy na pewno miasto wzięło pod uwagę wszystkie aspekty mające wpływ na jakość życia w mieście? I jak porównać to wszystko ze sobą? Jakie kryteria dobrać, aby były one spójne i takie same we wszystkich porównywanych miastach oraz umożliwiały porównania na przestrzeni czasu? W tym działaniu ma pomóc norma PN-ISO 37120 – zawiera ona listę wskaźników służących do śledzenia i monitorowania postępów miasta w zakresie działania usług miejskich oraz jakości życia. Zapewnia uporządkowanie spraw w zdefiniowanych zakresach tematycznych. Warto podkreślić, że ThinkIT Consulting wykonał pełny audyt przedcertyfikacyjny Gdyni, która jest pierwszym miastem w Polsce z certyfikatem Smart City.

Gdyńskimi doświadczeniami we wdrażaniu nowoczesnych rozwiązań i dobrych praktyk w kształtowaniu miasta o zrównoważonym rozwoju, a także tymi związanymi z procesem certyfikacji podzielił się **Bartosz Bartoszewicz**, Wiceprezydent Gdyni. Stwierdził, że inteligentne miasta to miasta nowoczesne o bardzo wysokiej jakości życia, w pełni wykorzystujące potencjał swojego położenia. I to jest właśnie wizja pierwszego certyfikowanego miasta w Polsce.

Następnie **Sławomir Wilczyński** omówił schemat certyfikacji na zgodność z normą PN-ISO 37120. Wskazał rolę jednostek certyfikujących oraz wartość Znaku Zgodności z PN. Posiadanie certyfikatu PN wydanego przez PKN oznacza nie tylko potwierdzenie zgodności zestawu wskaźników z normą odniesienia, lecz także ułatwienie udziału we wszelkiego rodzaju rankingach czy konkursach, w których wymagane jest podawanie wskaźników objętych normą.

Bartosz Bartoszewicz

Na zakończenie konferencji swoimi przemyśleniami o mieście, które potrafi sprostać wyzwaniom przyszłości, podzieliła się **Ewa Mikos**, Dyrektor ds. Rozwoju Biznesu, Siemens Sp. z o.o. Najważniejsze wyzwania to zarządzanie energią, dygitalizacja, bezpieczeństwo, jakość środowiska naturalnego, e-mobilność, akceptacja społeczna, nowoczesna przyjazna mieszkańcom infrastruktura. Prelegentka przybliżyła zebranym innowacje, które kształtują nasze jutro. Stwierdziła, że w niedalekiej przyszłości wszystkie pojazdy będą autonomiczne, ruch drogowy będzie obsługiwany przez inteligentne uliczne/drogowe rozproszone centra kontroli, poprawi się jakość środowiska, zredukowane zostanie zużycie energii, poziom bezpieczeństwa znacząco wzrośnie, radykalnie zwiększy się zdolność przewozowa i elastyczność, a podróże intermodalne staną się standardem.

Polskie miasta inspirują się działaniami innych państw w zakresie stosowania rozwiązań inteligentnych, ale jest to na razie kropla w morzu potrzeb. Niemniej jednak dobre praktyki są stopniowo przenoszone na nasz grunt i dostosowywane do potrzeb i stylu życia mieszkańców miast. Wszak Smart Cities to koncepcja, która zapewnia stabilność i komfort zamieszkiwania – jedna z najbardziej obiecujących koncepcji rozwoju miast i lokalnej gospodarki.

Oprac.
A. K.
J. S.

XVI Forum Dyskusyjne

„O monitorowaniu i kontrolowaniu jakości paliw, biopaliw, LPG i CNG/LNG”

7 grudnia br. pod patronatem Ministra Energii odbyło się XVI Forum Dyskusyjne „O monitorowaniu i kontrolowaniu jakości paliw, biopaliw, LPG i CNG/LNG" zorganizowane przez Polską Izbę Paliw Płynnych (PIPP). W Forum uczestniczyli przedstawiciele Departamentu Energii Odnawialnej, Ministerstwa Energii (ME), Przemysłowego Instytutu Motoryzacji (PIMOT), Urzędu Ochrony Konkurencji i Konsumentów (UOKiK), Polskiego Górnictwa Naftowego i Gazownictwa (PGNiG), Instytutu Technicznego Wojsk Lotniczych (ITWL), Operatora Logistycznego Paliw Płynnych (OLPP), Instytutu Nafty i Gazu – Państwowy Instytut Badawczy (INiG-PIB) oraz przedstawiciele firm i instytucji działających w branży paliwowej.

Przedstawiciel ME przybliżył zebranym zagadnienia dotyczące nowelizacji ustawy o biokomponentach i biopaliwach ciekłych w kontekście jej wpływu na rynek paliw, sposób osiągnięcia Narodowego Celu Wskaźnikowego. Natomiast przedstawiciel PIPP przybliżył aspekt prawny związany z nowelizacją ustawy, tj. odpowiedzialność stacji i baz paliw w perspektywie podwyższania zawartości biokomponentów w paliwach ciekłych, wprowadzenia nowych rodzajów paliw na rynek.

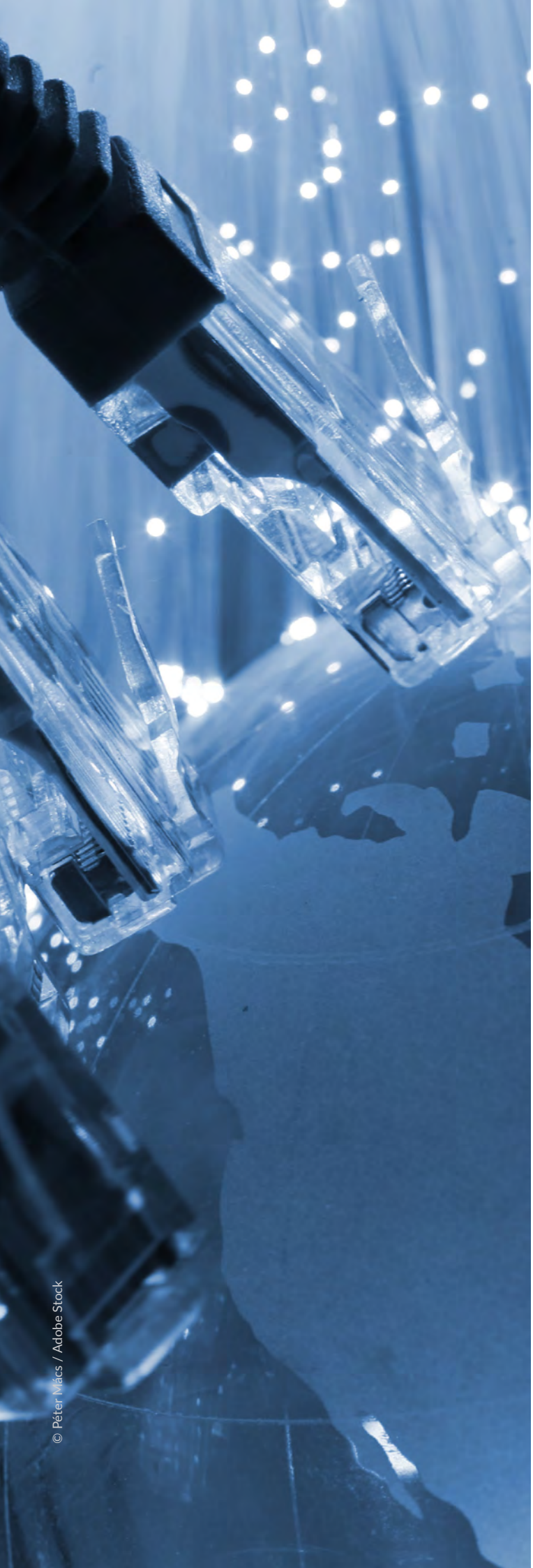
W dalszej części spotkania reprezentantka UOKiK omówiła wyniki kontroli jakości paliw z I połowy 2017 roku. Przedstawiła liczbę pobieranych próbek i kontrolowanych stacji paliw, hurtowni oraz dane liczbowe dotyczące próbek niespełniających wymagań jakości.

Następnie przedstawiciel PIMOT w prezentacji „Elektromobilność – ewolucja czy rewolucja? Zagadnienia wybrane" przedstawił perspektywy elektromobilności, potencjalny udział w rynku i wykorzystanie, a także zagrożenia w aspekcie bezpieczeństwa podróżnych oraz smogu elektromagnetycznego. Kolejna prezentacja wygłoszona przez reprezentanta PGNiG dotyczyła jakości LNG/CNG. Prelegent wyjaśnił, jak jest kontrolowana jakość gazu ziemnego i scharakteryzował badane parametry, sieć przesyłową i dystrybucyjną w kontekście zapewnienia jakości produktu. Jakość paliw lotniczych w kontekście bezpieczeństwa lotów cywilnych omówił przedstawiciel ITWL. Kolejnym poruszonym tematem było połączenie PERN i OLPP, cele i powody połączenia wyjaśnił przedstawiciel OLPP.

XVI Forum Dyskusyjne o monitorowaniu jakości paliw zakończyły wystąpienia związane z normalizacją. Przedstawicielka INiG-PIB omówiła zapisy Dyrektywy 2014/94/UE i normy PN-EN 16942:2016-11 dotyczące identyfikowania zgodności pojazd-paliwo przez wprowadzenie obowiązkowego znakowania. Natomiast przedstawicielka PIMOT w prezentacji dotyczącej kierunku rozwoju metod badawczych paliw płynnych w CEN przedstawiła ostatnio opublikowane oraz opracowywane normy z zakresu paliw płynnych.

Forum od lat stanowi ważne źródło informacji na temat zmian w prawie, wymagań stawianym uczestnikom rynku oraz jakości paliw płynnych w Polsce.

Magdalena Wienczatek
Sektor Chemii



Cyberbezpieczeństwo nowoczesnych sieci[1]

Ochrona kluczowej infrastruktury przed cyberzagrożeniami jest sprawą absolutnie priorytetową

Didier Giarratano[2]

Zmniejszanie ryzyka i przewidywanie podatności systemów sieci na zagrożenia nie dotyczy jedynie technologii instalacji, lecz także zrozumienia ryzyka.

Pojawiające się wyzwania

W branży użyteczności publicznej rozwijają się nowoczesne technologie dystrybucyjne.

Wzrasta popyt na zdigitalizowane i zintegrowane procesy, dlatego wyzwaniem dla wspomnianej branży jest zapewnienie niezawodnych dostaw energii pochodzącej przede wszystkim z trwałych i efektywnych źródeł.

Pilna potrzeba usprawnienia niezawodności infrastruktury dystrybuującej energię wymusza pewne zmiany. Jednak w miarę łączenia się sieci i ich „przyrostu inteligencji" wzrasta zagrożenie cyberatakami, co negatywnie wpływa na postęp w rozwoju tej technologii.

Systemy dystrybucji energii elektrycznej w Europie pierwotnie zbudowano jako sieci scentralizowane, obsługujące obciążenia pasywne. Nie były zaprojektowane tak, aby radzić sobie ze zmieniającą się konsumpcją energii. Dzisiaj wkraczamy w nowy świat energii; energii generowanej w sposób zdecentralizowany, uzupełnianej źródłami energii odnawialnej (jak słoneczna czy wiatrowa). Wkraczamy w świat dwukierunkowego przepływu energii zdekarbonizowanej i rosnącego zaangażowania konsumentów.

---

[1] Edytowana wersja artykułu, który po raz pierwszy ukazał się w P*ower Engineering International*.

[2] Didier Giarratano – szef Marketingu Cyberbezpieczeństwa (Marketing Cyber Security) w Energy Digital Solutions/Energy, Schneider Electric. Jest członkiem Grupy Roboczej (WG) 3 w Komitecie Systemowym IEC ds. *Smart Energy* (SyC *Smart Energy*/WG 3: *Smart Energy Roadmap*) oraz IEC *Conformity Assessment Board* (CAB)/WG 17: *Cyber security*.

Zdecentralizowany model

Obecnie budowa sieci coraz bardziej przypomina model zdecentralizowany. Tradycyjna dostawa energii jest jakby zakłócona, jednak stwarza wiele możliwości dla konsumentów i przedsiębiorców, którzy mogą przyczynić się do rozwoju sieci, wykorzystując źródła odnawialne. Dzięki temu w najbliższych latach zaobserwujemy pojawienie się nowego rodzaju konsumenta energii – zarządzającego produkcją i zużyciem energii tak, aby dostosować koszty, niezawodność i stały dostęp do energii do swoich potrzeb.

Wzrost rozproszonej energii zwiększa złożoność sieci. Zmienia branżę z tradycyjnego łańcucha wartości w oparte na współpracy środowisko, w którym klienci łączą się dynamicznie z siecią dystrybucji, dostawcami energii i rynkiem energii. Technologie i modele biznesowe będą musiały się zmienić, aby przemysł energetyczny przetrwał i dalej prosperował.

Nowa sieć będzie bardziej zdigitalizowana, elastyczna i dynamiczna. W świecie, w którym energia elektryczna stanowi większy udział w ogólnym koszyku energetycznym, sieć będzie coraz bardziej połączona i będzie musiała sprostać większym wymaganiom dotyczącym wydajności. W energetycznym ekosystemie pojawią się nowe podmioty, takie jak operatorzy systemów przesyłowych (*transmission system operators* – TSO), operatorzy systemów dystrybucyjnych (*distribution system operators* – DSOs), operatorzy generatorów rozproszonych, agregatorzy i prosumenci.

Przepis i zgodność

Cyberbezpieczeństwo koncentruje się na dostosowaniu się do norm i przestrzeganiu przepisów. Takie podejście przynosi korzyści całej branży przez zwiększanie świadomości zagrożeń i wyzwań związanych z cyberatakami. W miarę rozwoju sieci elektroenergetycznej, wraz z integracją rozproszonych zasobów energii i automatyzacją podajników, potrzebne jest nowe podejście – zorientowane na zarządzanie ryzykiem.

Obecnie interesariusze branży użyteczności publicznej korzystają z procesów cyberbezpieczeństwa, których nauczyli się od swoich odpowiedników z branży IT, co naraża ich na ryzyko. W środowisku podstacji zastrzeżone urządzenia dedykowane wyspecjalizowanym aplikacjom są teraz narażone na ataki. Internetowy dostęp do poufnych informacji, które opisują, jak działają te urządzenia, może mieć każdy.

Mając odpowiednie umiejętności, wrogie podmioty mogą włamać się do systemów firm użyteczności publicznej i uszkodzić systemy kontroli sieci. Takim działaniem stanowią zagrożenie dla gospodarki i bezpieczeństwa kraju lub regionu obsługiwanego przez tę sieć.

Organy regulacyjne przewidywały potrzebę ustrukturyzowanego podejścia do bezpieczeństwa cybernetycznego. W Stanach Zjednoczonych wymagania opracowane przez NERC CIP (North American Electric Reliability Corporation Critical

Infrastructure Protection) określają, co jest potrzebne do zabezpieczenia systemu elektrycznego w Ameryce Północnej. EPCIP (European Programme for Critical Infrastructure Protection) podobnie działa w Europie. Codziennie spotykamy się z nowymi i złożonymi atakami, z których część jest organizowana przez podmioty państwowe. Prowadzi to do ponownej oceny tych programów i ogólnego podejścia do bezpieczeństwa w branży.

Integracja na linii IT – OT

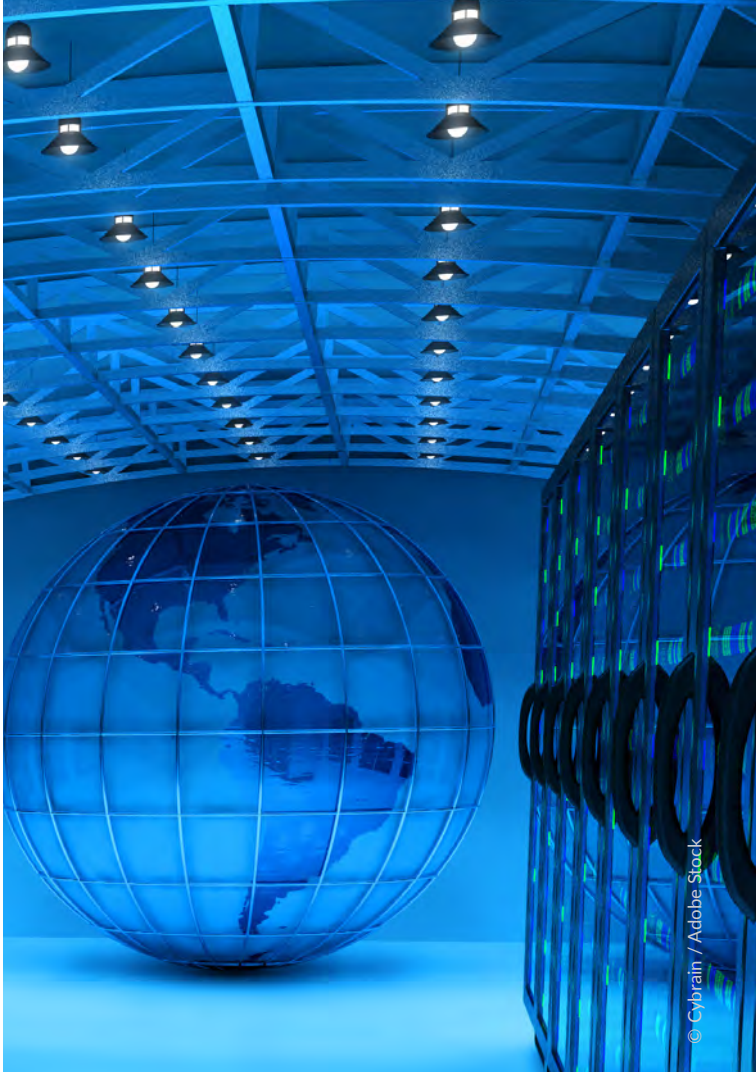
Z uwagi na przejście na otwarte platformy komunikacyjne, takie jak Ethernet i protokół internetowy (IP), systemy zarządzające najważniejszą infrastrukturą stają się coraz bardziej bezradne. Operatorzy infrastruktury o znaczeniu kluczowym analizują, jak mogą zabezpieczyć swoje systemy. Często sięgają po lepiej opracowane praktyki związane z cyberbezpieczeństwem. Jednak podejście specjalistów z branży IT do cyberbezpieczeństwa nie zawsze jest odpowiednie, szczególnie biorąc pod uwagę ograniczenia operacyjne.

Te różnice w podejściu oznaczają, że rozwiązania w zakresie cyberbezpieczeństwa i wiedza specjalistyczna nastawiona na świat IT mogą być nieodpowiednie w zastosowaniu technologii eksploatacji (*operational technology* – OT). Dziś skomplikowane ataki są w stanie wykorzystać współpracujące usługi, takie jak IT i telekomunikacja. W miarę jak branża użyteczności publicznej doświadcza konwergencji IT i OT, konieczne staje się utworzenie zespołów interdyscyplinarnych, aby sprostać wyjątkowym wyzwaniom związanym z zabezpieczeniem technologii obejmującej oba światy.

Ochrona przed cyberatakami wymaga obecnie bardziej przekrojowych działań, w których inżynierowie, managerowie IT i managerowie ds. bezpieczeństwa są zobowiązani do dzielenia się swoją wiedzą, dzięki której możliwe będzie zidentyfikowanie potencjalnych problemów i zagrożeń mogących oddziaływać na ich systemy.

Podejście czteropunktowe

Eksperci z branży cyberbezpieczeństwa zgodnie twierdzą, że normy same w sobie nie zapewnią odpowiedniego poziomu bezpieczeństwa. To nie jest kwestia „osiągnięcia" stanu bezpieczeństwa w cyberprzestrzeni. Właściwa ochrona przed zagrożeniami w cyberprzestrzeni wymaga kompleksowego zestawu



działań, procesów i środków technicznych oraz dostosowanej organizacji.

Dla firm użyteczności publicznej ważne jest zastanowienie się, jak strategie cyberbezpieczeństwa w organizacji będą się zmieniać w miarę upływu czasu. To bycie na bieżąco ze znanymi zagrożeniami i zapobieganie im w sposób zaplanowany, powtarzalny. Zapewnianie silnej ochrony przed cyberatakami to ciągły proces wymagający ciągłych starań i corocznych inwestycji. W cyberbezpieczeństwie chodzi o ludzi, procesy i technologię. Firmy użyteczności publicznej muszą uruchomić pełny program składający się z właściwej organizacji, procesów i procedur, dzięki czemu możliwe będzie pełne wykorzystanie technologii zapewniających bezpieczeństwo w cyberprzestrzeni.

Aby zbudować i utrzymać systemy cyberbezpieczeństwa, firmy użyteczności publicznej mogą zastosować zapisy z podejścia czteropunktowego.

Komitet Doradczy IEC ds. Bezpieczeństwa Informacji i Ochrony Danych (IEC *Advisory Committee on Information Security and Data Privacy* – ACSEC) pracuje nad tymi samymi kwestiami, które zostaną włączone w kolejnym IEC Guide 120, *Security aspects – Guidelines for their inclusion in publications*, opracowywanym przez ACSEC.

1. Przeprowadzanie oceny ryzyka

Pierwszy krok obejmuje przeprowadzanie kompleksowej oceny ryzyka opartej na zagrożeniach wewnętrznych i zewnętrznych. Dzięki temu specjaliści ds. technologii eksploatacji oraz interesariusze firm użyteczności publicznej mogą wychwycić, gdzie pojawiają się największe zagrożenia, a także będą mogli udokumentować stworzenie polityki bezpieczeństwa i zmniejszania ryzyka.

2. Stworzenie polityki bezpieczeństwa i procesów

Polityka cyberbezpieczeństwa firm użyteczności publicznej zapewnia formalny zbiór przepisów, jakich należy przestrzegać. Powinny się one opierać na Normach Międzynarodowych ISO/IEC 27000 dotyczących technik bezpieczeństwa IT, które obejmują zalecenia dotyczące najlepszych praktyk w zakresie zarządzania bezpieczeństwem informacji. Ta rodzina norm została opracowana przez ISO/IEC JTC 1/SC 27 *IT Security Techniques*, podkomitet Wspólnego Komitetu Technicznego powołanego do życia przez Międzynarodową Organizację Normalizacyjną (ISO) oraz Międzynarodową Komisję Elektrotechniczną (IEC). Celem polityki zakładu użyteczności publicznej jest informowanie pracowników, wykonawców i innych uprawnionych użytkowników o ich obowiązkach dotyczących ochrony technologii i aktywów informacyjnych. Opisuje listę zasobów, które muszą być chronione, identyfikuje zagrożenia dla tych zasobów i opisuje obowiązki upoważnionych użytkowników i związane z nimi uprawnienia dostępu, a także nieautoryzowane działania i odpowiedzialność wynikającą z naruszenia zasad bezpieczeństwa. Równie ważne są dobrze zaprojektowane procesy bezpieczeństwa. Ponieważ podstawy systemu bezpieczeństwa zmieniają się, aby naprawiać pojawiające się luki w zabezpieczeniach, procesy systemu cyberbezpieczeństwa muszą być regularnie przeglądane i aktualizowane. Kluczem do utrzymania skutecznego poziomu bezpieczeństwa jest przeprowadzanie przeglądu raz lub dwa razy w roku.

3. Wdrożenie planu zmniejszania ryzyka

Wybór technologii cyberbezpieczeństwa bazującej na Normach Międzynarodowych zapewni odpowiednie przestrzeganie polityki bezpieczeństwa oraz podejmowanie działań zmniejszających ryzyko. Podejście „secure by design" opiera się na Normach Międzynarodowych. Mogą one pomóc w dalszym zmniejszeniu ryzyka podczas zabezpieczania elementów systemu.

Obejmują one m.in. wieloczęściową normę IEC 62443 (*Security for industrial communication networks and for industrial automation and control systems* (IACS)), Normy Międzynarodowe IEC 62351 (*Power systems management and associated information exchange*) oraz normę IEEE 1686 (*Standard for Intelligent Electronic Devices Cyber Security Capabilities*) opracowaną przez Instytut Inżynierów Elektryków i Elektroników (Institute of Electrical and Electronics Engineers (IEEE)).

4. Zarządzanie programem bezpieczeństwa

Efektywne zarządzanie programami cyberbezpieczeństwa wymaga nie tylko uwzględnienia poprzednich trzech punktów, lecz także zarządzania cyklem życia zasobów informacyjnych i komunikacyjnych. Aby to zrobić, ważne jest utrzymanie dokładnej dokumentacji dotyczącej zasobów sprzętowych, systemów operacyjnych i konfiguracji. Wymaga to również pełnego zrozumienia unowocześniania technologii i harmonogramów zużycia w połączeniu z pełną świadomością istnienia luk w zabezpieczeniach oraz poprawek. Zarządzanie cyberbezpieczeństwem wymaga również, aby konkretne zdarzenia, takie jak określone punkty w cyklach życia aktywów lub wykryte zagrożenia, wymuszały dokonanie oceny.

Według przedstawicieli branży użyteczności publicznej bezpieczeństwo jest sprawą nas wszystkich. Politycy i organy władzy publicznej są coraz bardziej świadomi, że bezpieczeństwo narodowe zależy również od solidności lokalnych dostawców usług komunalnych.

Zmniejszanie ryzyka i przewidywanie podatności systemów sieci na zagrożenia nie dotyczy jedynie technologii instalacji. Firmy użyteczności publicznej muszą wprowadzać procesy organizacyjne, które sprostają wyzwaniom stawianym przez zdecentralizowane sieci. To oznacza konieczność regularnych kontroli i stałego usprawniania narzędzi bezpieczeństwa, zarówno cybernetycznego, jak i fizycznego, tak aby chronić nasz nowy świat energii.

Tłumaczenie I. P.
Źródło: IEC e-tech magazine, Issue 07/2017

Powstrzymać cyberkoszmar

Wzrastająca z każdym dniem liczba ataków cybernetycznych sprawia, że prace IEC mają kluczowe znaczenie w przeciwdziałaniu lub – gdy to się nie uda – ograniczaniu skutków takich ataków.

Morand Fachot

Prace normalizacyjne prowadzone przez Komitety i Podkomitety Techniczne Międzynarodowej Komisji Elektrotechnicznej (IEC), a także przez Wspólny Komitet Techniczny ISO/IEC JTC 1 mają na celu zapobieganie katastrofalnym następstwom ataków cybernetycznych na wszechobecne segmenty infrastruktury krytycznej i ich ograniczanie. Dodatkowo system IEC zgodności badań i certyfikacji sprzętu elektrotechnicznego (IECEE) pracuje nad ogólnym modelem oceny zgodności (CA), który będzie można stosować do zapewnienia bezpieczeństwa cybernetycznego.

Cele, uczestnicy i narzędzia

Liczba ataków cybernetycznych na kraje, przedsiębiorstwa, organizacje i osoby prywatne stale wzrasta.

Na ogół trudno rozpoznać inicjatorów tych ataków, nie wspominając już o złapaniu choćby jednego z nich. Często łączą ich motywy, ale oni sami są luźno zorganizowani. Są to między innymi:

- pojedyncze osoby lub zorganizowane grupy zdecydowane dokonać kradzieży pieniędzy – przez defraudację albo wymuszenia (*ransomware*; szyfrują pliki komputerów tak, że można je odblokować dopiero po zapłaceniu) – lub informacji, albo które chcą zablokować systemy informatyczne osób prywatnych czy przedsiębiorstw;
- firmy gotowe skraść poufne informacje swoim konkurentom – czy to techniczne, czy handlowe – aby uzyskać przewagę konkurencyjną;
- osoby lub grupy dążące do utrudniania działalności organizacjom czy rządom albo starające się podważyć ich dobrą opinię;
- państwa oraz podmioty niepaństwowe (funkcjonujący samodzielnie albo na zlecenie państw), którzy zamierzają uszkodzić lub zniszczyć infrastrukturę innych państw lub przedsiębiorstw, ponieważ uważają ich za swoich oponentów.

Narzędzia informatyczne używane do przeprowadzania ataków cybernetycznych są różnorodne i zależą od tego, jaki jest cel ataku. Mogą być łączone, aby zmaksymalizować skuteczność, i zwykle wykorzystują niewystarczające zabezpieczenia systemów np. nieudane aktualizacje oprogramowania i ogólny brak świadomości użytkowników tych systemów.

Destrukcyjne i kosztowne

Atak na system informatyczny przedsiębiorstwa, poza możliwymi znacznymi stratami finansowymi, może mieć również inne bardzo negatywne następstwa dla jego działalności (utrata istotnych informacji, straty wizerunkowe etc.).

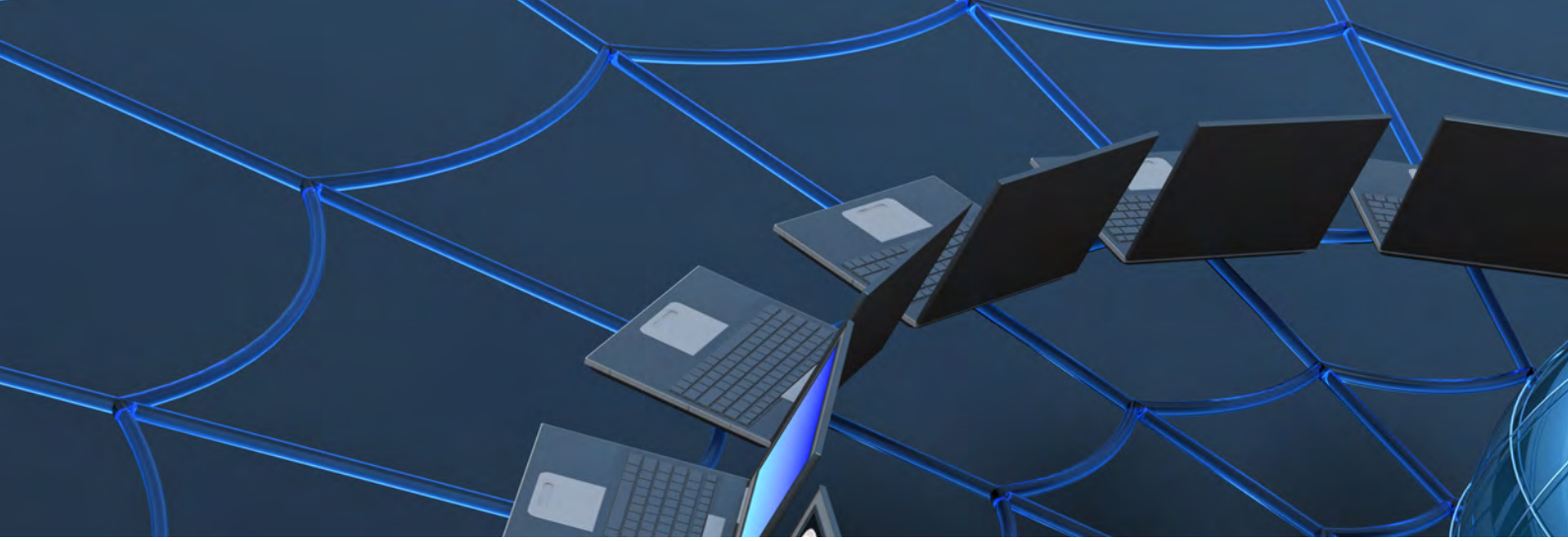
Potencjalny koszt takiego ataku może wynieść setki milionów. Dla przykładu – Grupa Żeglugowa AP Moller-Maersk ujawniła 16 sierpnia 2017 r., że koszt przeprowadzonego za pomocą oprogramowania NotPetya (17 czerwca) ataku cybernetycznego, który zakłócił działalność firmy, może wynieść nawet 200-300 milionów USD. Firma dodatkowo poinformowała, że 16 sierpnia jej zysk bazowy za drugi kwartał 2017 roku wyniósł 389 milionów USD…

Już teraz gospodarczy koszt ataków cybernetycznych jest szokująco wysoki, a i tak ma się podwoić w ciągu kilku lat, na co wskazuje raport z 2016 r. przygotowany przez firmę badawczą Cybersecurity Ventures. Przewiduje on, że roczne koszty związane z incydentami cybernetycznymi w 2021 roku sięgną 6 miliardów USD, w porównaniu do 3 miliardów w 2016 r.

Straty gospodarcze mogą być więc zatrważające, a przypuszczalnie katastrofalna byłaby poważna awaria części krajowej infrastruktury krytycznej. Uważa się, że infrastruktura krytyczna obejmuje wszystko lub większość z poniższej listy:

- dostawy energii elektrycznej (wytwarzanie, przesył, dystrybucja);
- usługi finansowe;
- systemy kontroli przemysłowej;
- opieka zdrowotna;
- telekomunikacja;
- technologie informacyjne (IT);
- ubezpieczenia.

W wielu krajach takie instalacje krytyczne, jak np. sieci energetyczne, są często niewystarczająco chronione.



Podejście do kwestii ochrony

Normy Międzynarodowe mają kluczowe znaczenie w ochronie systemów infrastruktury krytycznej.

Wiele organizacji w celu zabezpieczenia swoich danych informatycznych korzysta z rodziny Norm Międzynarodowych ISO/IEC 27000, przeznaczonych dla systemów zarządzania bezpieczeństwem informacji (ISMS). Są one opracowywane przez Wspólny Komitet ISO/IEC JTC 1/SC 27 *IT Security Techniques*.

Od września 2017 r. ukazało się około 45. publikacji na temat rodziny norm ISO/IEC 27000 przeznaczonych dla ISMS.

IEC opracowuje wiele Norm Międzynarodowych, a także innych publikacji dotyczących bezpieczeństwa cyberprzestrzeni dla konkretnych systemów i zastosowań. Niektóre z nich mogą być stosowane powszechnie, inne są właściwe tylko dla określonej domeny.

Normy Międzynarodowe IEC dotyczące bezpieczeństwa cybernetycznego są wdrażane w wielu różnych obszarach infrastruktury krytycznej, takich jak:

- systemy energetyczne;
- automatyka przemysłowa;
- elektrownie atomowe;
- opieka zdrowotna;
- transport (morski, drogowy i kolejowy).

Coraz więcej urządzeń domowych i przemysłowych zostaje połączonych; komunikują się one ze sobą za pośrednictwem tzw. Internetu Rzeczy (IoT), dlatego też pojawiają się nowe wyzwania dla bezpieczeństwa – tak połączone urządzenia stwarzają możliwość ataku obejmującego większe systemy. Poza wdrażaniem istniejących norm, potrzebne jest więc zupełnie nowe całościowe podejście w wielu dziedzinach.

Zakres prac normalizacyjnych w IEC

Komitety i Podkomitety Techniczne IEC, które przygotowują Normy Międzynarodowe chroniące określone obszary i przyczyniają się do poprawy bezpieczeństwa przemysłu i infrastruktury krytycznej:

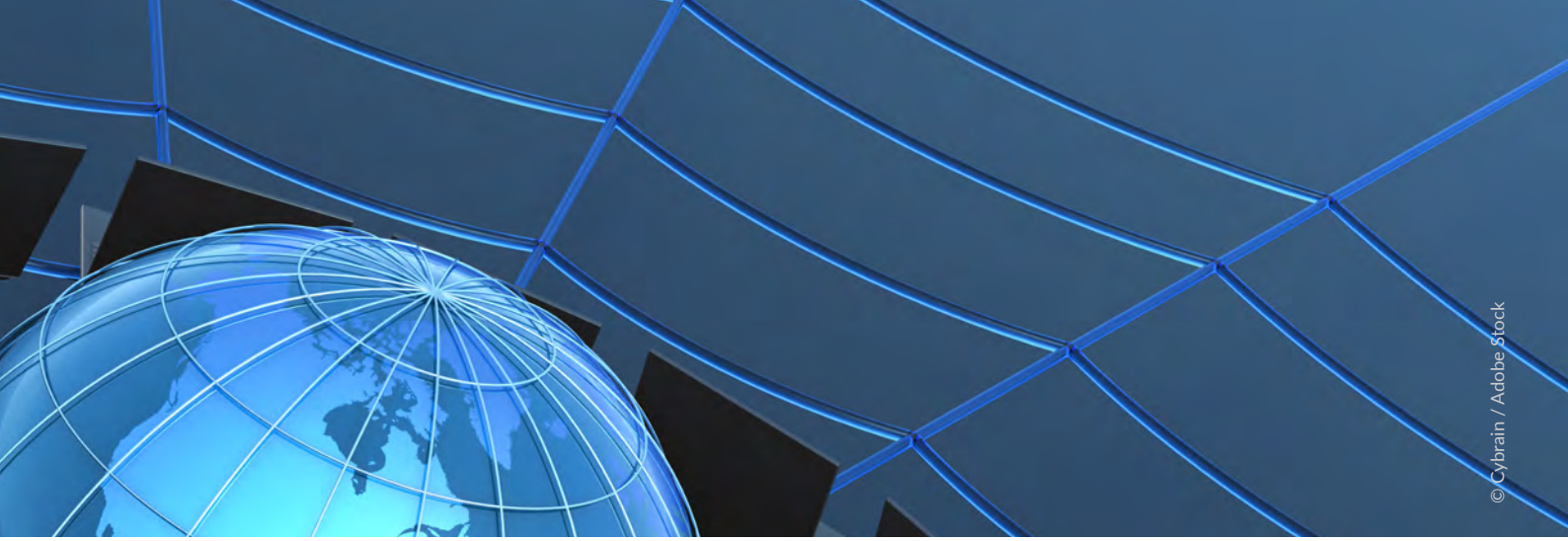
Komitet IEC/TC 57 *Power systems management and associated information exchange* opracowuje między innymi wieloczęściową normę: IEC 61850 przeznaczoną dla sieci komunikacyjnych i systemów automatyki energetycznej, a także IEC 60870 – dla systemów i urządzeń telekontroli. Te normy mają szczególne znaczenie dla infrastruktury krytycznej. Podczas dwóch cyberataków na ukraińską sieć energetyczną w grudniu 2015 i 2016 roku wykorzystano luki w ww. normach. W trakcie ostatniej konferencji BlackHat USA ujawniono, że to właśnie niekompletność w zabezpieczeniach zawartych w tych normach umożliwia zhakowanie systemów kontroli turbin wiatrowych i uszkodzenie całej instalacji. Członkowie KT 57 mają świadomość tego problemu i cały czas dokonują przeglądów norm, aby uporać się ze wszystkimi potencjalnymi niedoskonałościami zabezpieczeń.

Komitet IEC/TC 65 *Industrial-process measurement, control and automation* przygotowuje publikacje wieloczęściowej normy IEC 62443 określającej wymagania bezpieczeństwa dla przemysłowych systemów automatyki i sterowania (IACS). Normy te zostały sklasyfikowane jako najwłaściwsze dla bezpieczeństwa cybernetycznego, można je bowiem stosować w odniesieniu do prawie wszystkich produktów i systemów elektrotechnicznych, a nie tylko w automatyce przemysłowej.

Komitet IEC/SC 45A *Instrumentation, control, and electrical systems of nuclear facilities* wydał dwie publikacje dot. oprogramowania zabezpieczającego systemy komputerowe, a także koordynacji ogólnych zasad bezpieczeństwa i bezpieczeństwa cybernetycznego. Komitet przygotowuje kolejne publikacje o bezpieczeństwie cybernetycznym w obiektach nuklearnych.

Komitet IEC/TC 62 *Electrical equipment in medical practice* i Podkomitet opracowują normy, które mają chronić bezpieczeństwo danych medycznych, ich integralność oraz poufność.

Dostawcy usług medycznych i ubezpieczeniowych są coraz częściej atakowani przez przestępców, którzy próbują zdobyć dane z dokumentacji medycz-



nej w celu ich kradzieży lub dokonania oszustw na ich podstawie. Według Amerykańskiego Centrum Danych nt. Kradzieży Tożsamości (ITRC) w USA (w pięciu badanych sektorach gospodarki) więcej niż jedna trzecia wszystkich naruszeń bezpieczeństwa danych dotyczy ochrony zdrowia.

Komitet IEC/TC 80 *Maritime navigation and radiocommunication equipment and systems* opracował normę IEC 61162-450:2016, w której stwierdzono, że „pokładowa architektura bezpieczeństwa statku powinna być zgodna z najlepszymi praktykami stosowanymi w branży bezpieczeństwa informacji". Opublikował także dodatek do tej normy – IEC 61162-460:2015. Komitet Bezpieczeństwa na Morzu (MSC) Międzynarodowej Organizacji Morskiej (IMO) przyjął ostatnio „Wytyczne w sprawie bezpieczeństwa cybernetycznego na statkach", które odnoszą się do rodziny norm ISO/IEC 27000, a w szczególności do wieloczęściowej normy IEC 62443.

Nowo utworzony Wspólny Komitet Techniczny ISO/IEC JTC 1/SC 41 *Internet of things and related technologies* zainicjował badania nad wiarygodnością Internetu Rzeczy (IoT). Wiarygodność to zorientowana na użytkownika koncepcja inżynierii systemów, która obejmuje wszystkie elementy, które sprawiają, że system jest godny zaufania. Są to: zabezpieczenia, dostępność, trwałość, bezpieczeństwo, odporność i poufność. Ponieważ oczekuje się, że liczba urządzeń w Internecie Rzeczy wzrośnie z 8,3 miliarda w 2017 r. do 20,4 miliarda w 2020 r., przypuszczalnie zwiększy się też ryzyko cybernetyczne. Prace Komitetu ISO/IEC JTC 1/SC 41 powinny pomóc w ograniczeniu tego ryzyka.

Ocena zgodności też ma duże znaczenie

Oprócz prac normalizacyjnych, które mają na celu ochronę systemów przed atakami cybernetycznymi i które są prowadzone przez różne Komitety i Podkomitety IEC oraz Komitet Wspólny ISO/IEC JTC, to właśnie ocenę zgodności (CA) uważa się za następny ważny czynnik prowadzący do wzmocnienia ochrony cybernetycznej.

Częścią systemowego podejścia jakie stosuje IEC są prace Grupy Roboczej 17 (WG) Zarządu Oceny Zgodności (CAB) zajmującej się tworzeniem planów ogólnego modelu oceny zgodności, który będzie można stosować w cyberbezpieczeństwie. Ocena zgodności IEC nie chroni sama z siebie, ale daje pewność, że zastosowano najlepsze praktyki zgodne z wymaganiami norm, sama zaś zgodność została zweryfikowana i oceniona przez trzecią stronę.

IECEE (system IEC zgodności badań i certyfikacji sprzętu elektrotechnicznego) utworzył grupę zadaniową (TF) do spraw bezpieczeństwa cybernetycznego. Dokonała ona oceny certyfikacyjnej IEC 62443 i rozpoczęła prace nad systemem oceny zgodności zgodnym z tymi wymaganiami. Niedługo będzie można oczekiwać dalszych postępów.

Wciąż jest wiele do zrobienia

Częstotliwość i duży zasięg ataków cybernetycznych, które w tej chwili zagrażają tak samo osobom prywatnym, jak i przedsiębiorstwom czy nawet państwom, oznaczają, że coraz więcej dziedzin będzie wymagać ochrony, tym bardziej że upowszechnia się łączenie systemów oraz Internetu Rzeczy. Z tego powodu będzie się też rozszerzał zakres prac normalizacyjnych, koncentrujących się na zagadnieniach bezpieczeństwa, prowadzonych przez Komitety i Podkomitety IEC oraz ISO/IEC JTC 1. To samo dotyczy modelu oceny zgodności bezpieczeństwa cybernetycznego, który powstaje w IECEE.

Tłumaczenie P. M.
Źródło: IEC e-tech magazine, Issue 06/2017

© Kamaga / Adobe Stock

Dzień NIEZALEŻNOŚCI

Jak pomóc osobom niepełnosprawnym być bardziej samodzielnymi?

Catherine Bischofberger

Wykorzystywanie nowej technologii i gadżetów - aby pomóc osobom starszym i niepełnosprawnym pozostać niezależnymi w domu i poza nim - jest podejściem najchętniej wybieranym przez wielu specjalistów ds. ochrony zdrowia, a także polityków i władze. IEC, pod auspicjami SyC AAL (*Systems Committee on active assisted living*), przygotowuje Normy Międzynarodowe obejmujące działania w ramach tego podejścia.

Robot, mój przyjaciel

Roboty asystujące wyposażone w czujniki i systemy monitorujące są używane w ochronie zdrowia już od ponad dekady. W 2004 roku japoński wynalazca, dr Takanori Shibata, stworzył robota przypominającego kształtem fokę i nazwał go Paro. Robot nawiązywał kontakt wzrokowy i uczył się zachowań wywołujących pozytywne reakcje użytkowników. Od tamtego czasu trochę się jednak zmieniło. Dzisiejsze roboty asystujące pomagają ludziom przy wielu różnych czynnościach – od kąpieli po podnoszenie ciężkich przedmiotów. Jednocześnie odczytują zmiany wyrazu twarzy, reagują na komendy głosowe i rozpoznają gesty. Roboty te są wyposażone w wiele cyfrowych kamer i sprzęt stereo (głośniki i mikrofony). W ramach IEC/TC 100: *Audio, video and multimedia systems and equipment* założono *Technical Area, TA 16 Active assisted living (AAL) accessibility and user interfaces*, zajmujące się zagadnieniami związanymi z AAL.

Roboty są także wyposażone w różne czujniki, w tym monitory rytmu serca i ciśnienia krwi, a także rejestratory zmian w ruchu, detektory dźwięków i zapachów mogące zasygnalizować niebezpieczne sytuacje grożące samotnie mieszkającym osobom. IEC/SC 47E *Discrete semiconductor devices* przygotowuje Normy Międzynarodowe obejmujące projektowanie, produkcję i użytkowanie czujników.

Rewolucja w wózkach inwalidzkich

Według danych Światowej Organizacji Zdrowia (WHO) 70 milionów ludzi na świecie potrzebuje wózków inwalidzkich, aby poruszać się po domu i poza nim, jednak wielu z nich – zwłaszcza z krajów rozwijających się – nie może sobie na nie pozwolić z powodu wysokiej ceny. Szacuje się, że tylko 15% osób niepełnosprawnych w krajach rozwijających się ma wózek inwalidzki. Jeśli już uda im się go zdobyć, zazwyczaj nie jest on dobrze dopasowany – ze względu na ciężar, wielkość lub rodzaj niepełnosprawności.

Ta sytuacja zaczęła się zmieniać dzięki najnowszej technologii skanowania i drukowania 3D. Na przykład znajdująca się w Londynie organizacja charytatywna Hack On Wheels stworzyła bibliotekę online, w której można znaleźć sprawdzone projekty *open source*. Można przeszukiwać archiwum, aby znaleźć coś odpowiedniego i wydrukować to w technologii 3D, dzięki czemu dopasowanie wózka do własnych potrzeb będzie łatwiejsze i tańsze. Laboratorium w Wiedniu opracowało koncepcję inwalidzkiego wózka dziecięcego z parametrycznymi połączeniami, które mogą „rosnąć" razem z dzieckiem. Oparcie jest wykonane z pianki (jej kształt bazuje na trójwymiarowym skanie ciała), które idealnie pasuje do osoby i sprawia, że krzesło jest znacznie wygodniejsze.

Równie szybki jest postęp technologiczny w sporcie. Niedawna współpraca przemysłu z brytyjską branżą sportową zaowocowała powstaniem najnowocześniejszego wózka inwalidzkiego dla sportowców wykorzystującego kilka technologii. Czołowy niemiecki producent samochodów za pomocą skanera 3D zbadał siedzącego sportowca, aby stworzyć spersonalizowany wózek inwalidzki. Po skanowaniu opracowano model cyfrowy symulujący aerodynamiczne zmiany zachodzące podczas ruchu sportowca. Doprowadziło to do modyfikacji ramy fotela, zmniejszając jego opór o 15%. Opór wpływa na zdolność utrzymania prędkości, szczególnie podczas uderzenia w wiatr lub pochyłość. Przeprowadzono testy w tunelach aerodynamicznych BAE Systems, aby ocenić ich aerodynamiczną sprawność, a jego zwrotność została zmierzona za pomocą technologii opracowanej przez wybitny zespół wyścigowy Formuły 1.

IEC/TC 76 *Optical radiation and laser equipment* przygotowuje Normy Międzynarodowe w tym obszarze; w tym także lasery wysokiej mocy wykorzystywane w przemyśle i projektach badawczych. Ta praca jest kluczowa dla technologii skanowania i druku 3D.

IEC wraz z ISO toruje drogę normom związanym z technologią druku 3D przez pracę podkomitetu założonego w ramach ISO/IEC JTC 1 *Information technology*. IEC/ISO JTC 1/SC 28 *Office equipment* skupia się na pracach związanych z funkcjonalnością i testowaniem skanerów i drukarek 3D.

Egzoszkielety w szafie

Niektórzy wizjonerzy, jak założyciel firmy Tesla – Elon Musk, uważają, że w najbliższej przyszłości wszyscy staniemy się cyborgami w świecie, gdzie obecność robotów będzie na porządku dziennym. Póki co, taka wizja pozostaje w sferze science-fiction, choć egzoszkielety i protezy kończyn już dziś pomagają osobom z niepełnosprawnościami w codziennym radzeniu sobie z różnymi ograniczeniami.

Sieć ochotników e-NABLE kontaktuje ze sobą osoby potrzebujące protez kończyn (głównie dłoni i rąk) oraz projektantów, którzy wykorzystują technologię druku 3D, aby wytworzyć sztuczne stawy na zamówienie.

Francuska firma stworzyła kolano ALLUX – inteligentną, zdalnie sterowaną kończynę. Jeśli użytkownik się potknie, elektronika przejmie kontrolę nad kolanem dzięki czujnikom wykrywającym pojawianie się niebezpiecznych sytuacji. Mikroprocesory natychmiast zwiększają opór hydrauliczny, aby zapobiec nagłemu wyboczeniu kolana. Wbudowany akumulator litowo-jonowy zapewnia wystarczającą moc przez dwa do czterech dni użytkowania.

The Walk Again Project, wspólne przedsięwzięcie non-profit z udziałem brazylijskich, niemieckich, amerykańskich i szwajcarskich naukowców, rozwija egzoszkielety z wykorzystaniem najnowszych technologii, w tym rzeczywistości wirtualnej (VR), umożliwiając kierowanie robotycznymi elementami przez mózg użytkownika. Z ich pracy skorzystał słynny brazylijski sportowiec Juliano Pinto, który rozpoczął mistrzostwa świata w piłce nożnej 2014.

IEC/TC 21 *Secondary cells and batteries* koncentruje swoją pracę na normach obejmujących akumulatory litowo-jonowe.

Dzwonek alarmowy

Wnętrza domów z wieloma systemami alarmowymi, czujnikami, systemami monitorującymi i detektorami mogą zainteresować entuzjastów nowinek, ale są też bardzo użyteczne dla osób starszych i niepełnosprawnych. Produkty bezpieczeństwa dla środowisk AAL i inteligentnych domów obejmują kamery, czujniki ruchu, czujniki i alarmy drzwi i okien oraz elektroniczne zamki i przyciski napadowe.

Na przykład czujniki dymu przystosowane dla osób z wadami słuchu ostrzegają użytkowników przez miganie światłami. Jeśli osoba znajduje się w pozycji leżącej, może zostać ostrzeżona przez alarm wibracyjny pod poduszką. Nadajniki bezprzewodowe w niektórych z tych systemów mogą również łączyć się z systemami bezpieczeństwa w domu i wysyłać z nich powiadomienia. Innym przydatnym urządzeniem jest wskaźnik poziomu cieczy, który wydaje dźwięk, gdy filiżanka jest prawie pełna, umożliwiając osobom niedowidzącym przygotowanie gorącej herbaty bez poparzenia.

IEC TC 79 *Alarm and electronic security systems* przygotowuje Normy Międzynarodowe obejmujące szereg aplikacji i systemów w tym elektroniczną kontrolę dostępu, transmisję sygnałów alarmowych, nadzór wideo, systemy wykrywania pożaru i alarmów pożarowych.

Oświetlenie sterowane głosem lub czujnikami ruchu, zrobotyzowane odkurzacze, kontrolery okien i żaluzji, telefoniczne dialery alarmowe – wszystkie muszą być bezpieczne i wydajne, ponieważ każda wadliwa aparatura może mieć katastrofalne skutki. Elementy elektroniczne mogą być certyfikowane jako bezpieczne i niezawodne dzięki IECQ *(IEC Quality Assessment System for Electronic Components)*. Ogólnoświatowy system zatwierdzania i certyfikacji obejmuje dostawy podzespołów elektronicznych i powiązanych materiałów i procesów.

Oprac. I. P.
Źródło: IEC e-tech magazine, Issue 06/2017

© jim / Adobe Stock

KT 210 ds. Armatury Przemysłowej i Rurociągów Przemysłowych

© 3dmentat / Adobe Stock

W październiku 2017 r. opublikowano w angielskiej wersji językowej siedem części normy PN-EN 13480 Rurociągi przemysłowe metalowe:

- Część 1: Postanowienia ogólne,
- Część 2: Materiały,
- Część 3: Projektowanie i obliczenia,
- Część 4: Wykonanie i montaż,
- Część 5: Kontrola i badania,
- Część 6: Wymagania dodatkowe dla rurociągów podziemnych,
- Część 8: Wymagania dodatkowe dla rurociągów z aluminium i stopów aluminium.

Ta wieloczęściowa norma zastępuje siedem części normy PN-EN 13480 z 2012 roku i stanowi wprowadzenie do Polskich Norm nowego wydania siedmiu części EN 13480 z 2017 r.

Wydanie normy z 2017 r. obejmuje normę z 2012 r. wraz ze zmianami i poprawkami publikowanymi w latach 2012-2017. Uaktualniono także powołania normatywne i poprawiono błędy edycyjne. Każda z siedmiu części normy zawiera informacyjny Załącznik Y *History of EN 13480-x* (Historia EN 13480-x), w którym podano wykaz istotnych zmian względem wydania z 2012 r.

Znak „x" w numerze normy (EN 13480-x) oznacza numer części normy.

Wydanie ujednoliconej wersji ułatwia posługiwanie się normą. Wszystkie aktualne postanowienia zawarte są w danej części normy i nie ma potrzeby korzystania z odrębnych dokumentów zawierających zmiany i poprawki.

Wieloczęściowa EN 13480 Rurociągi przemysłowe metalowe została opracowana przez Komitet Techniczny CEN/TC 267 Rurociągi przemysłowe i wydana po raz pierwszy w 2002 r. W 2012 r., ze względu na dużą liczbę poprawek i zmian do licznych wzorów, tablic i rysunków, zadecydowano o wydaniu ujednoliconej wersji. Obecna wersja z 2017 r. jest trzecim wydaniem normy.

W normie EN 13480 podano wymagania dotyczące przemysłowych instalacji rurociągowych i zamocowań, łącznie z systemami bezpieczeństwa, wykonanych z materiałów metalowych, uwzględniając zapewnienie bezpiecznej eksploatacji. Norma ta dotyczy rurociągów naziemnych, kanałowych lub podziemnych, bez względu na ciśnienie.

Normy nie stosuje się do kanałów przepływu wody (takich jak rurociągi zasilające czy szyby ciśnieniowe do instalacji hydroelektrycznych), rurociągów na pojazdach, rurociągów zamocowanych trwale na statkach, rakietach, samolotach, elementów specjalnych do zastosowania jądrowego, sprzętu wiertniczo-kontrolnego używanego w przemyśle wydobywczym, rurociągów wielkich pieców, obudów bezpieczeństwa systemów przesyłowych (takich jak kable energetyczne i telefoniczne), rurociągów wewnętrznych w urządzeniach medycznych.

Norma EN 13480 jest jedną z podstawowych Norm Europejskich w zakresie wyposażenia ciśnieniowego i stanowi podstawę domniemania zgodności z dyrektywą Unii Europejskiej dotyczącą urządzeń ciśnieniowych 2014/68/UE. Części normy 13480 od 1 do 6 oraz 8 są ogłoszone w Dzienniku Urzędowym Unii Europejskiej jako normy zharmonizowane.

Grażyna Borusińska
Sektor Maszyn i Inżynierii

ORGANY TECHNICZNE
listopad 2017

Komitety Techniczne

Nowi Przewodniczący Komitetów Technicznych

W listopadzie Prezes PKN powołał na 4-letnią kadencję do pełnienia funkcji Przewodniczącego:

- w KT 49 ds. Optyki i Przyrządów Optycznych **mgra inż. Antoniego Buraczewskiego** reprezentującego Stowarzyszenie na Rzecz Rozwoju Fotografii Humanistycznej FOTO HUMANUM
- w KT 115 ds. Hałasu w Środowisku **dra inż. Radosława Kucharskiego** reprezentującego Instytut Ochrony Środowiska - Państwowy Instytut Badawczy
- w KT 259 ds. Poczty **mgra Dariusza Parzuchowskiego** reprezentującego Pocztę Polską SA
- w KT 325 ds. Projektowania Konstrukcji i Elementów Budowlanych ze Szkła **dra inż. Artura Piekarczuka** reprezentującego Instytut Techniki Budowlanej

Nowi Sekretarze Komitetów Technicznych

W listopadzie Prezes PKN powołał do pełnienia funkcji Sekretarza:

- w KT 37 ds. Ryb i Przetworów Rybnych **mgr Martę Zadrożną** z Polskiego Komitetu Normalizacyjnego
- w KT 38 ds. Przetworów Owocowych i Warzywnych **mgr Martę Zadrożną** z Polskiego Komitetu Normalizacyjnego
- w KT 54 ds. Chemicznych Źródeł Prądu **inż. Barbarę Rybicką** z Polskiego Komitetu Normalizacyjnego
- w KT 61 ds. Elektrycznego Wyposażenia Trakcyjnego **Panią Agnieszkę Kaczorek** reprezentującą Instytut Kolejnictwa

- w KT 72 ds. Elektroenergetycznego Sprzętu Ochronnego i do Prac pod Napięciem **mgr Agnieszkę Kamieniecką** z Polskiego Komitetu Normalizacyjnego
- w KT 80 ds. Ogólnych w Sieciach Elektroenergetycznych **mgra Pawła Puchalskiego** z Polskiego Komitetu Normalizacyjnego
- w KT 92 ds. Nasion Roślin Oleistych, Tłuszczów Roślinnych i Zwierzęcych oraz ich Produktów Ubocznych **mgr Martę Zadrożną** z Polskiego Komitetu Normalizacyjnego
- w KT 110 ds. Surowców i Przetworów Zielarskich **mgr Martę Zadrożną** z Polskiego Komitetu Normalizacyjnego
- w KT 229 ds. Kawy, Herbaty i Kakao **mgr Martę Zadrożną** z Polskiego Komitetu Normalizacyjnego
- w KT 310 ds. Systemów Zarządzania Bezpieczeństwem Żywności **mgr Martę Zadrożną** z Polskiego Komitetu Normalizacyjnego

Nowi członkowie Komitetów Technicznych

W listopadzie Prezes PKN powołał na członków KT następujące podmioty:

- **Euroglas Polska Sp. z o.o.** do KT 198 ds. Szkła
- **Fundacja GS1 Polska** do KT 259 ds. Poczty
- **Izba Gospodarcza Sprzedawców Polskiego Węgla** do KT 316 ds. Ciepłownictwa i Ogrzewnictwa
- **Polski Rejestr Statków SA** do KT 22 ds. Odzieżownictwa
- **PONAR Wadowice SA** do KT 160 ds. Napędów i Sterowań Hydraulicznych
- **Stowarzyszenie Elektryków Polskich Oddział Warszawski im. Kazimierza Szpotańskiego** do KT 8 ds. Terminologii, Dokumentacji i Symboli Graficznych, Oznaczeń Wielkości i Jednostek Miar w Elektryce
- **Urząd Dozoru Technicznego** do KT 128 ds. Projektowania i Wykonawstwa Konstrukcji Metalowych i Konstrukcji Zespolonych i KT 183 ds. Bezpieczeństwa Urządzeń Informatycznych, Telekomunikacyjnych i Biurowych

Odwołania członków Komitetów Technicznych

W listopadzie Prezes PKN odwołał z członka KT:

- COBRABID - BBC Biuro Badań i Certyfikacji Sp. z o.o. z KT 2 ds. Sportu i Rekreacji i KT 100 ds. Wyrobów z Drewna i Materiałów Drewnopochodnych
- EKOTECH J. Rząsa i T. Stanowski Sp.J. z KT 1 ds. Osób Niepełnosprawnych
- GAMRAT SA z KT 143 ds. Elektryczności Statycznej i-SEC Krzysztof Ciesielski z KT 52 ds. Systemów Alarmowych Włamania i Napadu
- SATEL Sp. z o.o. z KT 52 ds. Systemów Alarmowych Włamania i Napadu
- TÜV Rheinland Polska Sp. z o.o. z KT 215 ds. Projektowania i Wykonawstwa Konstrukcji z Drewna i z Materiałów Drewnopochodnych

Podkomitety Techniczne

Nowy członek Podkomitetu Technicznego

W listopadzie Prezes PKN powołał do pełnienia funkcji Przewodniczącego

- w KT 176/PK 8 ds. Eksploatacji Uzbrojenia i Sprzętu Marynarki Wojennej **Pana Dariusza Świrskiego** reprezentującego Inspektorat Marynarki Wojennej DG RSZ

RODO - Ochrona danych osobowych od podstaw

SZKOLENIE

Szkolenie wprowadza w tematykę ochrony danych oraz przepisów krajowych i unijnych (w tym do zmian wynikających z RODO). Uczestnicy po szkoleniu będą umieli stworzyć i aktualizować dokumentację bezpieczeństwa, przeprowadzać sprawdzenia, przygotowywać sprawozdania, realizować obowiązki informacyjne wobec podmiotów danych, prowadzić rejestry przetwarzania danych, przeprowadzić analizę ryzyka i zagrożeń, a także monitorować incydenty bezpieczeństwa.

Zagadnienia:

- Przepisy prawa - omówienie
- Wprowadzenie do podstawowych zagadnień
- Określanie podstawy legalności przetwarzania danych
- Realizowanie obowiązków informacyjnych wobec podmiotów danych
- Identyfikowanie zbiorów danych oraz prowadzenie rejestru
- Analiza ryzyka i zagrożeń
- Zasady opracowywania dokumentacji bezpieczeństwa
- Zarządzanie incydentami
- Planowanie i przeprowadzanie sprawdzeń ze zgodności przetwarzania danych z przepisami

Miejsce szkolenia:

Polski Komitet Normalizacyjny
ul. Świętokrzyska 14
Warszawa

Cena szkolenia:

520,00 zł netto + 23% VAT/osobę

Więcej szczegółów na stronie wiedza.pkn.pl

PKN POLSKI KOMITET NORMALIZACYJNY

Kontakt: szkolenia@pkn.pl; tel. 22 55 67 766