Wiadomości PKN

· NORMALIZACJA ·

11/2016

INTERNET RZECZY

WYDAWCA
POLSKI KOMITET NORMALIZACYJNY
www.pkn.pl

wiadomości PKN
NORMALIZACJA
11/2016

„**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
Redaktor:
Barbara Kęsik - tel. 22 556 74 60
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 Państwo,

W tym numerze zachęcamy do lektury dwóch artykułów odnoszących się do świata, w którym wkrótce przyjdzie nam żyć i na który przemożny wpływ będzie miał Internet Rzeczy. Kiedy myślimy o podłączeniu do Internetu to większość z nas wyobraża sobie komputery, tablety i smartfony. Tymczasem Internet Rzeczy oznacza, że prawie wszystko może być podłączone, równocześnie komunikując się między sobą. Innymi słowy świat fizyczny staje się w ten sposób wielkim systemem informacyjnym. Internet Rzeczy jest więc w rzeczywistości internetem danych.

Z artykułu „Czy jesteśmy bezpieczni w Internecie Rzeczy?" dowiedzą się Państwo, jakie zagrożenia niesie ze sobą IoT. Kierunek, w jakim zmierzamy to świat, w którym dosłownie wszystko, co można sobie wyobrazić zostanie podłączone do internetu. Stwarza to wiele możliwości zarówno dla firm, jak i konsumentów, ale niesie także zagrożenia i wyzwania takie jak ochrona prywatności i bezpieczeństwo.

Jak można zmniejszyć niebezpieczeństwo? Czy normalizacja może być w tym pomocna? Okazuje się, że Normy Międzynarodowe są niezbędne w tworzeniu globalnego rynku bezpiecznych, energooszczędnych i interoperacyjnych systemów i urządzeń działających w ramach IoT. Istnieje już także współpraca między trzema międzynarodowymi organizacjami normalizacyjnymi i jest to niezwykle istotne, jeśli chcemy przyspieszyć pomyślne wdrażanie IoT.

Zachęcamy do zapoznania się z innymi artykułami oraz informacjami z bieżącego numeru.

Redakcja

Bezpieczeństwo informacyjne w szkole i placówce oświatowej

III Specjalistyczna Konferencja

Z inicjatywy Ośrodka Edukacji Informatycznej i Zastosowań Komputerów w Warszawie oraz Polskiego Komitetu Normalizacyjnego została zorganizowana III Specjalistyczna Konferencja „Bezpieczeństwo informacyjne w szkole i placówce oświatowej". Konferencja odbyła się 26 października 2016 roku w Warszawie i była skierowana do dyrektorów, nauczycieli szkół, przedszkoli i placówek oświatowych oraz przedstawicieli organów prowadzących; do tych osób, których obowiązkiem jest ochrona aktywów informacyjnych przetwarzanych w szkole, w tym danych osobowych. Na konferencji wieloaspektowo przedstawiono kwestie bezpieczeństwa informacyjnego w dziedzinie oświaty i edukacji.

Uroczystego otwarcia dokonał Tomasz Schweitzer, Prezes PKN. Następnie głos zabrała Marzenna Przesmycka-Baranek, Dyrektor OEIiZK. Uczestników przywitała Aurelia Michałowska, Mazowiecki Kurator Oświaty.

Wykład inauguracyjny „Normy a bezpieczeństwo" wygłosił Zygmunt Niechoda, doradca Prezesa PKN.

Następnie w kolejnych prezentacjach przedstawiono szeroki wachlarz poglądów i informacji nt. bezpieczeństwa informacyjnego w szkołach i placówkach oświatowych.

Od strony prawnej „Zagrożenia w obszarze bezpieczeństwa informacji w szkole i jak można im zapobiec" przedstawił Dariusz Skrzyński - specjalista w zakresie prawa oświatowego. Na początku podał przykłady zagrożeń związanych z ujawnieniem informacji. Nawiązywał do konkretnych sytuacji w szkole i analizując akty prawne, rozstrzygał dylematy: czy i kiedy można ujawniać dane osobowe mediom bądź w postępowaniu sądowym, czy można przetwarzać dane osobowe i in. Poinformował o nowym prawie o ochronie danych osobowych, tzw. ogólnym rozporządzeniu PE i Rady (UE). Podał listę najważniejszych zmian w tym rozporządzeniu.

T. Schweitzer

Kolejny referat dotyczył „Oceny stopnia zapewnienia bezpieczeństwa informacji w szkolnych pracowniach informatycznych, klubach i czytelniach komputerowych w oparciu o wymagania normy PN-ISO/IEC 27001 - wyniki badań w projekcie PWUPAE" - a jego autorami byli Magdalena Szeżyńska z CISA oraz Krzysztof Gołofit z Instytutu Systemów Elektronicznych WEiTI PW. Przedstawili, jakie były cele projektu *Profilaktyka agresji elektronicznej wśród polskich nastolatków*. Zaliczyli do nich m.in. stworzenie programu skoncentrowanego na pozytywnej profilaktyce oraz metodach przeciwdziałania agresji elektronicznej. W rezultacie ma powstać kompletny program wraz z podręcznikiem, który zostanie udostępniony nauczycielom z całej Polski. Opierając się na zapisach PN-ISO/IEC 27001, omówiono wybrane zagadnienia oceny stanu bezpieczeństwa. Poruszono m.in. zagadnienie zabezpieczenia przed kodem złośliwym. Ponadto omówiono zarządzanie nośnikami wymiennymi, zmianami oraz przywilejami. Wstępne wyniki badania wskazują, że zabezpieczenia w placówkach szkolnych są niedostateczne i nie sprzyjają zachowaniu prywatności użytkowników.

Kolejna prezentacja dotyczyła tematu „Normy a technologie informacyjno-komunikacyjne". Izabela Rudnicka - nauczyciel konsultant w Pracowni Edukacji dla Bezpieczeństwa OEIiZK wypowiedziała się nt. norm pracy w sieci, zasad bezpiecznej nauki i pracy z nowymi technologiami. Omówiła aplikacje przydatne w tworzeniu grafiki, plakatów i infografik.

Następnie Paweł Górski, Pełnomocnik Prezesa PKN ds. Polityki Edukacyjnej przedstawił informacje o V Konkursie „Normalizacja i ja".

W II części prelegenci skupili się na praktycznych aspektach budowania bezpiecznej sieci w szkole oraz standardach bezpieczeństwa informatycznego.

Do doświadczeń konkretnej szkoły nawiązał Artur Rudnicki, Wicedyrektor Zespołu Szkół, który przedstawił prezentację nt. „Bezpieczna sieć w szkole, na przykładzie Zespołu Szkół Technicznych im. T. Kościuszki w Radomiu". Na początku zdefiniował, co rozumie przez bezpieczną sieć i określił jej pożądane cechy. Następnie scharakteryzował sieć w swojej szkole. Przedstawiając konfigurację sieci w szkole, poinformował, że każdy uczeń i nauczyciel ma swoją imienną nazwę użytkownika i bez tej nazwy nie ma możliwości uruchomienia komputera. Wszystkie komputery pracują w domenie szkolnej, czyli pod kontrolą serwera. Te i inne zabiegi techniczne przedstawione przez prelegenta służą idei bezpiecznej sieci w szkole.

Kolejno Dariusz Stachecki, Wicedyrektor Gimnazjum skupił się na standardach bezpieczeństwa informatycznego na przykładzie gimnazjum w Nowym Tomyślu. Omówił mobilne środowisko edukacyjne, czyli nowe metody pracy i nowe narzędzia, nowe kanały dystrybucji treści, indywidualizację kształcenia i nauczanie interdyscyplinarne. Wskazał, jak powinna wyglądać sieć w szkole. Położył nacisk na kwestię filtrowania treści, autentykację i autoryzację użytkowników oraz bezpieczny dostęp do dokumentacji szkolnej. Przedstawił fragmenty funkcjonujących w szkole zasad bezpieczeństwa informacji. Wśród mocnych stron systemu wymienił m.in. wzrost świadomości i odpowiedzialności, wyeliminowanie przejawów cyberbullyingu, utrzymanie EDUSYSTEMU w sprawności.

Konferencja zakończyła się prezentacją Michała Grześlaka, Administratora Systemów Informatycznych OEIiZK nt. budowania świadomości użytkowników systemu zarządzania bezpieczeństwem informacji. Z wystąpienia wynikało, że bezpieczeństwo informacji to zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności.

M. Grześlak, G. Gregorczyk

Na konferencji zaprezentowano różne opinie dot. świadomości wagi bezpieczeństwa informacyjnego w placówkach oświatowych. Ze wstępnych wyników projektu *Profilaktyka agresji elektronicznej wśród polskich nastolatków* wynika, że ochrona aktywów informacyjnych przetwarzanych w placówkach oświatowych jest więcej niż niewystarczająca. Natomiast prezentacje bazujące na konkretnych przykładach tego nie potwierdzają. Stwierdzono w nich, że placówki szkolne mają świadomość wagi zabezpieczeń i skutecznie wdrażają odpowiednie rozwiązania.

To tylko wskazuje, że świadomość bezpieczeństwa informacyjnego w placówkach oświatowych jest bardzo zróżnicowana, dlatego tego typu konferencje są ważnym źródłem informacji. Obok jakości usług edukacyjnych bezpieczeństwo informacyjne stało się prawdziwym wyzwaniem dla współczesnej szkoły.

red.

Kwalifikacje kontrolerów placów zabaw

Posiedzenie CEN/TC 136/SC 1/WG 17

W dniach 27 i 28 października 2016 r. w siedzibie PKN w Warszawie obradowała Grupa Robocza CEN/TC 136/SC 1/WG 17 Framework for the competence of Playground Inspectors. W posiedzeniu wzięli udział przedstawiciele Finlandii, Wielkiej Brytanii, Austrii, Szwecji i Polski.

Grupa Robocza została utworzona w 2014 r. z powodu konieczności określenia wytycznych związanych z kwalifikacjami kontrolerów placów zabaw. W składzie WG 17 znaleźli się zarówno kontrolerzy, jak i producenci wyposażenia placów zabaw.

Głównym celem posiedzenia było omówienie uwag zgłoszonych do projektu Raportu Technicznego „Playground and recreational areas - requirements for quality of inspections and competence of inspectors" i podjęcie decyzji odnośnie do wprowadzenia zmian do dokumentu.

Projekt zawiera informacje dotyczące przygotowania, sprawdzania i oceny kompetencji kontrolerów placów zabaw i terenów rekreacyjnych. Podano w nim wymagania w zakresie wiedzy i doświadczenia kontrolerów. Opisano także szczegółowo rodzaje kontroli oraz wyjaśniono, w jaki sposób powinny być one przeprowadzane.

Dokument może być stosowany odnośnie do kwalifikacji kontrolerów następującego rodzaju sprzętu:

- wyposażenia placów zabaw (EN 1176, części od 1 do 6 oraz 10 i 11);
- infrastruktury dla użytkowników sprzętu rolkowego (EN 14974);
- aren do uprawiania wielu dyscyplin sportowych (EN 15312);
- siłowni plenerowych (EN 16630);
- sztucznych ścian wspinaczkowych (EN 12572-2);
- bramek do piłki nożnej (EN 16579);
- urządzeń do parkour (EN 16899);
- przygodowych placów zabaw.

Należy zwrócić uwagę, że dokument nie ma zastosowania w przypadku kontroli zabawek (EN 71), torów linowych (EN 15567), a także nadmuchiwanego sprzętu do zabawy (EN 14960).

Temat jest ważny - zapewnienie prawidłowej kontroli terenów, na których bawią się dzieci, powinno wpłynąć na zwiększenie ich bezpieczeństwa. Obecnie dokument stanowi propozycję Raportu Technicznego, ale ze względu na jego znaczenie WG 17 zamierza dążyć do tego, aby stał się normą.

Posiedzenie Grupy Roboczej było okazją do wymiany doświadczeń wynikających z praktyki w zakresie kontroli placów zabaw oraz w zakresie produkcji wyposażenia tego typu obiektów. Eksperci analizowali różnego typu przypadki występujące podczas kontroli placów zabaw oraz porównywali systemy związane z przeprowadzaniem tego typu kontroli w różnych krajach.

Podjęto również dyskusję na temat propozycji certyfikacji dotyczącej kwalifikacji kontrolerów placów zabaw. Obrady na ten temat będą kontynuowane na następnym posiedzeniu CEN/TC 136/SC 1/WG 17, które odbędzie się w styczniu 2017 r. w Wielkiej Brytanii.

Kamila Drużbiak

Druga edycja Eurokodów
Spotkanie Przewodniczących KT

19 października 2016 r. w PKN odbyło się spotkanie Przewodniczących Komitetów Technicznych działających w ramach Sektora Budownictwa i Konstrukcji Budowlanych, których tematyka obejmuje projektowanie konstrukcji. Spotkanie odbyło się z inicjatywy prof. Henryka Zobla, Przewodniczącego Rady Sektorowej SBD oraz KT 102 i KT 251 i dotyczyło opracowywanej obecnie w CEN drugiej edycji Norm Europejskich dotyczących projektowania - Eurokodów.


© Delphotostock - Fotolia.com

Do udziału w spotkaniu zostali zaproszeni Przewodniczący dwunastu KT odpowiedzialnych za poszczególne części Eurokodów oraz o tematyce z nimi powiązanej.

Wprowadzenie do spotkania stanowiło sprawozdanie prof. Henryka Zobla z bieżących działań Komitetu CEN/TC 250 *Structural Eurocodes* w ramach opracowywania drugiej edycji Eurokodów. Prof. Zobel od wielu lat czynnie uczestniczy w pracach normalizacyjnych, kilka razy w roku biorąc udział w posiedzeniach plenarnych CEN/TC 250 i CEN/TC 250/SC 1. Głównym celem spotkania było przekazanie zebranym aktualnej wiedzy na temat prac nad nowymi Eurokodami oraz naświetlenie potencjalnych problemów i wyzwań, które mogą pojawić się wraz z ich opublikowaniem.

W ramach sprawozdania uczestnicy spotkania zostali poinformowani o toczących się od kilku miesięcy pracach dwudziestu pięciu Grup Projektowych (Project Teams) działających przy CEN/TC 250. Pierwsze wstępne projekty nowych Eurokodów mają zostać opracowane na początku 2017 r., pozostałe – w połowie 2017 roku. Publikacja całego zbioru nowych norm planowana jest na 2020 rok. Ponieważ prace są już na dość zaawansowanym etapie, prof. Zobel zaapelował do Przewodniczących, aby wraz z innymi członkami swoich KT rozpoczęli poszukiwania doświadczonych ekspertów, którzy w przy-

szłości mogliby zająć się przetłumaczeniem nowych Eurokodów.

Następnie zrelacjonowane zostały następujące sprawy bieżące CEN/TC 250:

- powstanie nowych podkomitetów: SC 10 - EN 1990 *Basis of structural design* oraz SC 11 - *Structural Glass*;
- planowane utworzenie podkomitetu SC 12 zajmującego się konstrukcjami z kompozytów polimerowych;
- rozważane wprowadzenie 3. stanu granicznego – Stanu Granicznego Trwałości – i związane z tym utworzenie osobnego Eurokodu dotyczącego trwałości konstrukcji, za którego opracowanie odpowiadałby ewentualnie kolejny nowo powstały podkomitet SC 13;
- funkcjonowanie tzw. Horizontal Groups – HG Bridges i HG Fire – planowane utworzenie osobnych Eurokodów dla mostów (a nie jak dotychczas tylko ich części) oraz idea utworzenia jednej normy dotyczącej projektowania konstrukcji w warunkach pożaru;
- Załączniki krajowe (NA) - w ramach upraszczania i harmonizacji norm projektowych planowane jest ograniczenie do niezbędnego minimum liczby NA do Eurokodów. Docelowo zakłada się pozostawienie do ustalenia krajowego jedynie parametrów odnoszących się do oddziaływań klimatycznych i sejsmicznych oraz opisujących warunki gruntowe.

W związku z planowanym uczestnictwem w posiedzeniu plenarnym CEN/TC 250 w Paryżu w dniach 28-29 listopada br. i zamiarem przedstawienia w jego trakcie stanowiska Polski w sprawie redukcji liczby NA, prof. Zobel zwrócił się do Przewodniczących z prośbą o wyrażenie – i przekazanie przed terminem posiedzenia – opinii na temat NA do poszczególnych części Eurokodów.

Po wysłuchaniu sprawozdania uczestnicy spotkania odbyli dyskusję, w ramach której omówiono następujące zagadnienia:

- współpracę KT 180 ds. Bezpieczeństwa Pożarowego Obiektów z pozostałymi KT przy tzw. częściach pożarowych Eurokodów;
- dużą liczbę Załączników krajowych do Eurokodów, których zapisów w Polsce nie stosuje się (jako argument dla ograniczenia ich liczby);
- potrzebę stosowania jednego systemu norm projektowych poprzez ostateczne zlikwidowanie możliwości korzystania z wycofanych przez Eurokody norm PN-B;
- możliwości pośredniego zrezygnowania z dobrowolności stosowania norm projektowych poprzez odpowiednie powoływanie ich w przepisach;
- problemy z finansowaniem w Polsce badań na cele normalizacyjne;
- perspektywę przetłumaczenia nowych Eurokodów oraz wynikającą z niej konieczność znalezienia odpowiednich podmiotów i ekspertów, którzy opracowaliby tłumaczenia na wysokim merytorycznym poziomie;
- konieczność rozważenia powołania 3 nowych KT w ramach SBD: ds. tuneli, konstrukcji z kompozytów polimerowych oraz szkła konstrukcyjnego.

W ramach podsumowania spotkania prof. Zobel zapowiedział informowanie Przewodniczących na bieżąco o postępach w pracach nad drugą edycją Eurokodów oraz cykliczne spotkania w tej sprawie. To dobry pomysł i należy mieć nadzieję, że zajęcie się sprawą drugiej edycji Eurokodów na poziomie krajowym na tak wczesnym etapie przyczyni się znacząco do sprawnego opracowania dobrej jakości tłumaczeń nowych – tak istotnych dla branży budowlanej norm.

Bogumiła Papierowska
Sektor Budownictwa i Konstrukcji Budowlanych

Jak Internet Rzeczy zmieni nasze życie?

Elizabeth Gasiorowski-Denis

Internet Rzeczy (Internet of Things, IoT) ma moc, by zmienić nasz świat. Gdy zaczynamy dostrzegać jego niesamowity wpływ, znajdujemy się dopiero na początku drogi transformacji. Spójrzmy na obecny stan rzeczy w normalizacji IoT i na to, co inni myślą na jego temat.

© BillionPhotos.com - Fotolia.com

Wkrótce każde urządzenie, a w zasadzie prawie każdy obiekt, który możemy sobie wyobrazić – będą połączone z Internetem. Czy to telefon, urządzenie przenośne czy przedmioty gospodarstwa domowego – Internet Rzeczy (IoT) połączy nas na takie sposoby, o jakich jeszcze nam się nie śniło. Twój termostat, system alarmowy, czujnik dymu, dzwonek do drzwi i lodówka już teraz mogą być „połączone", ale zmiany zaczynają się zakorzeniać także w infrastrukturze miejskiej. Lepsze zarządzanie energią, wodą, transportem publicznym i bezpieczeństwem przybliża ludzi do ich otoczenia i wizji „błogostanu" urbanizacji – w pełni zintegrowanego, inteligentnego i zrównoważonego miasta. Wreszcie widzimy także znaczny wzrost aktywności i innowacyjności po stronie wytwórców, gdzie potencjał systemów cyberfizycznych zwiększających wydajność procesów produkcyjnych jest naprawdę ogromny. Jak można sobie wyobrazić, życie za 10 lat będzie wyglądać inaczej niż w 2016 roku, zwłaszcza jeśli uwzględnimy coraz szybsze zmiany technologiczne, co częściowo możemy zawdzięczyć popularyzacji IoT. W pewnym sensie pojęcie IoT jest pustym terminem w żargonie technicznym. Trudno jest jednakowo rozpatrywać wszystkie różne, niepowiązane kwestie i mówić o nich sensownie. Podejmując więc próbę zrozumienia tej rozwijającej się technologii, spójrzmy na plany budowy IoT w przyszłości.

Paradygmat przejścia w technologii

Firma konsultacyjna Gartner Inc. przewiduje, że w tym roku na całym świecie używane będzie 6,4 miliarda przedmiotów połączonych, jest to

30-procentowy wzrost w stosunku do roku ubiegłego. Przewiduje się, że ta liczba do roku 2020 wzrośnie ponadtrzykrotnie - do 21 miliardów. Ponad połowa dużych firm do 2020 roku wprowadzi do swojej działalności jakiś element IoT, zapewnia Gartner. Wpływ na życie konsumentów i modele działalności gospodarczej jest coraz większy. Jest to cena za „oprzyrządowanie" przedmiotów czujnikami i połączenie ich z innymi: urządzeniami, systemami, ludźmi. Technolog i futurysta, Chuck Evanhoe, który wypowiadał się już na temat IoT, wyjaśnia (..): „IoT będzie niesamowitym narzędziem ułatwiającym zdobywanie i wymianę informacji zarówno w środowisku konsumenckim, jak i biznesowym. Wierzę, że wpływ IoT obejmie wszystkie płaszczyzny życia. Wszystkie systemy, o których nie myślimy na co dzień, będą bardziej wydajne a my – ludzie – bardziej produktywni. IoT wpłynie na bardzo wiele obszarów życia". Błyskotliwe aplikacje technologii konsumenckich oczywiście generują większość medialnego szumu, ale IoT to coś więcej niż tylko codzienne sytuacje i komunikacja. Urządzenia w sieci miały obniżyć koszty i podnieść poziom wydajności produkcji – oferowały nie tylko bardziej wydajną, ale także „inteligentniejszą" pracę. Evanhoe wymienia liczne zalety: „od 'Smart Appliance' do 'Smart Factory', będziemy zbierać dokładniejsze, lepsze informacje, będziemy mieć lepszą kontrolę nad przedmiotami niezbędnymi do funkcjonowania, tymi znanymi i nieznanymi. Przez pojęcie 'nieznane' mam na myśli przedmioty, nad którymi ludzie się nie zastanawiają do momentu aż pojawia się jakiś problem, jak np. sieć energetyczna. Dzięki tej technologii systemy będą mogły działać bez interwencji człowieka do momentu, gdy zajdzie taka potrzeba, np. przeprowadzenie konserwacji zapobiegawczej".

Witamy w Przedsiębiorstwie 4.0

Tradycyjny przemysł na całym świecie jest w tej chwili w środku wielkiej zmiany, wyraźnie widoczny jest początek „inteligentnej produkcji" (Smart manufacturing) lub też Przedsiębiorstwa 4.0. Codziennie technologie oparte na IoT sprawiają, że fabryki są „inteligentniejsze", bezpieczniejsze i bardziej zrównoważone pod względem ochrony środowiska. IoT zapewnia fabrykom dostęp do szerokiego spektrum inteligentnych rozwiązań produkcyjnych. Ulepszenia wprowadzane w procesie produkcji i zmniejszenie kosztów mają w ciągu najbliższej dekady poprawić produktywność i przynieść miliardowe zyski. Taka transformacja jest ogromnym przedsięwzięciem. IoT daje producentom możliwość „śledzenia" obiektów, uzyskania informacji dot. tego, jak konsumenci używają danego produktu oraz określenia, która z cech produktu jest tą najważniejszą. Dzięki temu możliwe jest ustalenie, jakie poprawki należałoby wprowadzić w kolejnych produktach, aby ich użytkowanie było łatwiejsze, a ceny przystępniejsze. Wiedza o tym, co konsumenci robią z zakupionym produktem jest czymś, o co marki zabiegają. Może im to zapewnić właśnie technologia IoT. Według badań, których wyniki Gartner opublikował na początku tego roku, oczekuje się, że do końca 2016 roku 43% przedsiębiorstw zaadaptuje rozwiązania technologii IoT. Większość z tych firm będzie reprezentować m.in. przemysł paliwowy, sektor użyteczności publicznej oraz sektor produkcji. IoT ma przynieść zmiany także w przemyśle motoryzacyjnym. Zmiany, jakich jeszcze nie przewidzieliśmy, a już teraz wpływają na producentów samochodów i na ich myślenie o przyszłości swoich produktów. Igor Demay, Przewodniczący *ISO/TC 22 Road vehicles*, wyjaśnia: „Technologia IoT w przemyśle motoryzacyjnym pojawiła się na początku XXI w. razem z systemami nawigacji, które w znacznym stopniu zmieniły relację kierowca-pojazd. Jesteśmy teraz w drugim okresie wykorzystywania „urządzeń lustrzanych", takich jak telefony komórkowe czy przenośne nawigacje znane jako urządzenia nomadyczne*, używane przez kierowców i właścicieli pojazdów podczas jazdy". Ta sytuacja będzie się pogłębiać, jeśli więcej samochodów będzie się „łączyć", a konsumenci będą żądać więcej tego typu technologii w swoich pojazdach. „Trzecim krokiem" – twierdzi Demay -„będzie wprowadzenie zaawansowanych systemów wspomagania kierowcy oraz rozwiązań umożliwiających autonomiczną jazdę samochodu". Rozwiązania technologii IoT są przyszłością przemysłu motoryzacyjnego, jednak wyzwania są tym większe im bardziej wzrasta poziom zaawansowania technologicznego.

Największe wyzwanie

Tak jak każda nowa technologia, IoT na początku będzie postrzegany jako dezorientujący i groźny, zwłaszcza kiedy dyskusje krążą wokół kwestii normalizacji. Obecnie największym problemem związanym z IoT jest brak odpowiednich norm. Podczas gdy część aspektów technologii IoT nie jest

objęta żadnymi normami, do innych odnosi się wiele konkurujących ze sobą norm; zwycięzcy jednak nie widać. Bez „wspólnej metody komunikacji" urządzenia będą mogły łączyć się jedynie z innymi urządzeniami tej samej marki, co znacznie osłabi użyteczność urządzeń połączonych. Aby zrozumieć, jak brak jednolitych norm może utrudnić rozwój produktu i wzrost przemysłowy należy skupić się na kwestii komunikacji. Jeśli na przykład firma opracowująca inteligentną odzież będzie inna niż firma zajmująca się inteligentnymi urządzeniami domowymi, szanse na połączenie ich produktów są nikłe. Stałoby się tak, ponieważ różne urządzenia używają różnych protokołów komunikacji. Nie możemy wówczas mówić o interoperacyjności. Daleko nam także do oczekiwań konsumentów. Jeśli jednak obie firmy będą korzystać z tej samej normy komunikacji, łatwiej będzie osiągnąć interoperacyjność. Nic więc dziwnego, że technologia IoT jest gorącym tematem w środowisku normalizacyjnym. Wspólny komitet techniczny ISO i IEC (ISO/IEC/JTC 1) utworzył grupę roboczą (WG 10), która zajmie się zagadnieniem Internetu Rzeczy. Ma opracować architektoniczny model interoperacyjności systemów IoT. Wiele potrzebnych norm już prawdopodobnie istnieje, jednak ich relatywne znaczenie, wdrożenie i zastosowanie nie są w 100% zrozumiałe. W odpowiedzi na zaistniałą sytuację ISO utworzyło Strategiczną Grupę Doradczą (Strategic Advisory Group, SAG) ds. Przedsiębiorstwa 4.0. Jej Przewodniczący Kai Rannenberg uważa, że kluczem jest komunikacja sieciowa umożliwiająca urządzeniom zbieranie i wymianę danych. „IoT otwiera przed nami wiele możliwości i nieprzewidywalnych zastosowań. Może być jednak ryzykowny, np. jeśli poziom gromadzenia danych zostanie zawyżony albo kiedy urządzenia połączone z Internetem nie zostały do tego celu zaprojektowane". Rannenberg postrzega normy z zakresu IoT jako wsparcie przy tworzeniu bardziej wydajnych i odpowiadających potrzebom konsumentów sys-

temów. „Będzie dużo interfejsów. Potrzebne są normy, aby uniknąć sytuacji, w której interfejsy są powodem zatoru we wprowadzaniu produktów na rynek. Normy odegrają także znaczącą rolę w koordynującej cykle produkcji architekturze Przedsiębiorstwa 4.0/inteligentnej produkcji". Dla Rannenberga i pozostałych ekspertów kulminacją prac SAG będzie seria norm, które zapewnią bezproblemowe łączenie się urządzeń z dostępem do Internetu, bez względu na chip, system operacyjny czy producenta.

Współpraca i dzielenie się

Mimo iż wiele organizacji, w tym grupy interesariuszy i konsorcja przemysłowe, podejmuje próby opracowania norm dotyczących IoT, ISO „kieruje swój wzrok" na działania wspólne. Na początku tego roku ISO, IEC (Międzynarodowa Komisja Elektrotechniczna) i ITU (Międzynarodowy Związek Telekomunikacyjny) zorganizowały wspólne warsztaty dotyczące norm IoT. Warsztaty odbyły się w Berlinie (Niemcy), gospodarzem był DIN (Niemiecki Instytut Normalizacyjny). Całe wydarzenie prowadzone było przez ISO/IEC JTC 1. Celem warsztatów była wymiana doświadczeń i zdobycie wiedzy na temat prac normalizacyjnych w ramach tych trzech organizacji. Prelegenci z różnych sektorów podzielili się swoimi oczekiwaniami wobec IoT i określili, jak ta technologia może wpłynąć na ich obszar działalności. Zaprezentowano kilka przypadków zastosowania, m.in. inteligentne sieci, inteligentna produkcja, zarządzanie łańcuchem dostaw oraz inteligentne urządzenia przenośne (wearable smart devices). Globalne wyzwania - takie jak oszczędzanie energii, inteligentniejsze miasta i lepsza opieka zdrowotna jako przykłady tych sektorów, w których technologia IoT miałaby odegrać znaczącą rolę, były również przedmiotem dyskusji. Podczas warsztatów poruszono także kwestie przekrojowe dla zastosowań IoT, jak np. bezpieczeństwo danych i architektury referencyjne inteligentnych sieci. Postęp prac normalizacyjnych ma niebagatelny wpływ na wprowadzenie rozwiązań technologii IoT na szeroką skalę. Warsztaty zakończono konkluzją, że Normy Międzynarodowe są niezbędne w tworzeniu globalnego rynku bezpiecznych, energooszczędnych i interoperacyjnych systemów i urządzeń działających w ramach IoT. Paneliści uznali, że rozszerzenie istniejącej już współpracy między trzema międzynarodowymi organizacjami normalizacyjnymi jest niezwykle istotne, jeśli chcemy przyspieszyć pomyślne wdrażanie IoT. Jest bardzo prawdopodobne, że potrzebne będzie więcej działań zanim stan ciągłych zmian w normach się nie ureguluje. Nie ma wątpliwości, że potrzeba wielu umysłów i ich pracy, by normy stały się kompatybilne. Jednak z praktycznego punktu widzenia pracy będzie przybywać stopniowo. Eksperci zakładają, że około 2017 roku nastąpi kompletna reorganizacja. Śledźcie więc na bieżąco nasze działania.

Dalej niż komunikacja

Szybkie zmiany w technologii IoT sprawiają, że przewidywanie przyszłości normalizacji w tej dziedzinie jest wyzwaniem nawet dla doświadczonych ekspertów. Jest jednak pewne, że możliwości będą nieograniczone. Evanhoe jako futurysta rozumie współczesne trendy w technologii i przewiduje ich możliwe ukierunkowanie. „Konwergencja jest nieunikniona" – uważa. „IoT sięga dalej niż urządzenia połączone, np. przedmioty z adresem IP; wszystkie technologie automatycznej identyfikacji, w tym RFID (Radio-frequency identification) i kody kreskowe umożliwiają IoT identyfikację urządzeń działających w jego (IoT) ramach. Wszystko to działa razem i umożliwia działanie IoT i czerpanie z niego korzyści". Czy to przez twój telefon komórkowy, urządzenie przenośne, czy przedmiot codziennego użytku, IoT połączy nas tak, jak sobie tego wcześniej nie wyobrażaliśmy.

Źródło: ISOfocus September-October 2016
Tłum. I.P.

**Urządzenie nomadyczne oznacza element komunikacji lub urządzenie do przetwarzania informacji, które kierowca może wziąć do pojazdu i używać w czasie prowadzenia pojazdu, na przykład telefon komórkowy, system nawigacji lub podręczny komputer osobisty.*

Czy jesteśmy bezpieczni w Internecie Rzeczy?

Maria Lazarte

Załóżmy, że przestępca używał twojej nanny cam (czyli kamery, dzięki której można monitorować zachowanie opiekunki), aby obserwować twój dom. Albo lodówka wysyła w twoim imieniu SPAM do osób, których nawet nie znasz. A teraz wyobraź sobie, że ktoś włamał się do twojego tostera i uzyskał dostęp do całej twojej sieci. O ile inteligentne urządzenia dzięki Internetowi Rzeczy uzyskują szerszy dostęp do danych, o tyle wzrasta ryzyko ataku dzięki tym połączeniom. Normy ISO pomogą uczynić tę rozwijającą się branżę bezpieczniejszą.

Jako konsumenci i użytkownicy technologii jesteśmy tak rozkojarzeni, podziwiając możliwości Internetu Rzeczy, że nie zauważamy, jak bardzo wpłynie to na naszą prywatność i bezpieczeństwo. Oczywiście pewne urządzenia, jak np. elektroniczna niania może nieco uspokoić rodziców, którzy mogą w dowolnej chwili sprawdzić na smartfonie, co robią ich dzieci. Kiedy jednak technologia nie jest zabezpieczona, możemy niezamierzenie narazić siebie i naszych bliskich na niebezpieczeństwo. Szpiegowanie obcych ludzi nigdy nie było aż tak proste. Potrzebne jest jedynie narzędzie wyszukujące jak np. Shodan (rodzaj wyszukiwarki Google w Internecie Rzeczy – Internet of Things, IoT), która szpera w sieci i robi zdjęcia niezabezpieczonym urządzeniom. Wnętrza naszych domów, nasze zwierzęta domowe, a nawet nasze lodówki są w zasadzie na „kliknięcie". Wielu rodziców zdało sobie sprawę, jak bardzo byli zagrożeni, gdy wyszło na jaw, że elektroniczna niania, której używali, została zaatakowana przez hakera. Nie zaskakuje fakt, że w ciągu ostatnich trzech lat liczba skarg i reklamacji związanych z technologią IoT w samej Wielkiej Brytanii wzrosła o 2000%.

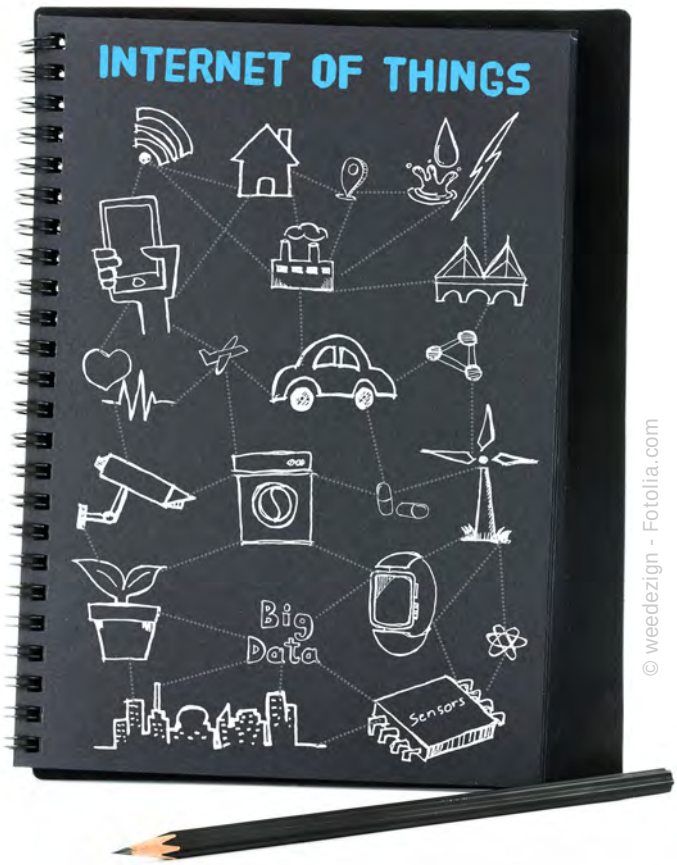
Odważny, nowy świat

Internet Rzeczy związany jest z miliardami inteligentnie powiązanych urządzeń, stale wymieniających potężne ilości danych o tym, jak żyjemy, pracujemy i spędzamy wolny czas. „Ma to ułatwić nasze życie, mamy być zdrowsi i mądrzejsi, a nasza działalność bardziej produktywna, jednak to wszystko ma swoją cenę" – uważa prof. Edward Humphreys, Przewodniczący Grupy Roboczej ISO/IEC zajmującej się systemami zarządzania bezpieczeństwem informacji. „Chcemy wierzyć w te technologie, ponieważ dzięki nim mamy więcej możliwości. Musimy jednak zdawać sobie sprawę z konsekwencji wynikających z niedostatecznej ochrony naszych danych".

Przykładowo, w ferworze ekscytacji kupujesz najnowszy aktywowany głosowo inteligentny telewizor (smart TV). Możesz wówczas zapomnieć o tym, że ta technologia musi „słuchać" wszystkiego, co mówisz, tak aby właściwe komendy zostały rozpoznane. Jeśli wszystko zostanie między tobą a telewizorem, to w czym problem, prawda? Kanały komunikacyjne umożliwiające urządzeniu wymianę informacji często nie są szyfrowane, ani w inny sposób zabezpieczone przed próbą uzyskania dostępu z zewnątrz. „To trochę jak zostawienie otwartych drzwi wejściowych; każdy może wejść w dowolnym momencie" – mówi Humphreys.

Istotą problemu jest to, że większość z nas, oprócz firm i ustawodawców, nie wzięło pod uwagę takiego ryzyka i nic w tej kwestii nie robi. Jeśli jednak konsumenci nie rozumieją albo nie wykazują zainteresowania ochroną danych, producenci również się tym nie zajmą. Oni wiedzą, że nie kierujemy się bezpieczeństwem, jesteśmy bardziej skłonni kupić kamerę internetową ze względu na jej kompatybilność, cenę czy nawet wygląd (!). Badania przeprowadzone przez Consumers International wykazały, że przeciętny użytkownik poświęca sześć sekund na przeczytanie rubryki „terms and conditions" zanim zaznaczy okienko z treścią. Dlaczego więc firmy miałyby się tym przejmować?

„Jeśli chodzi o prawodawstwo, to co robimy w domach rzadko jest chronione w takim samym stopniu, jak dane firm" – uważa Pete Eisenegger, ekspert z ramienia konsumentów zajmujący się kwestiami prywatności na szczeblach międzynarodowym i europejskim. „Weźmy takie urządzenia przenośne – śledzą i monitorują nasz ruch i wszystko co robimy, „wiedzą" więc gdzie dokładnie nas znaleźć. Jeśli połączymy to



© weedezign - Fotolia.com

z naszymi danymi osobistymi, zdjęciami, które upubliczniamy – trzeba bić na alarm. Analiza tych danych sprawia, że bardzo łatwo dowiedzieć się czegoś o ludziach".

W hiperpołączonym świecie stawka jest wysoka. Ostatni eksperyment pokazał, że możliwe jest zhakowanie pojazdu w ruchu poprzez system rozrywki dla pasażera i wyłączenie akceleratora. „Elektroniczne rozruszniki serca nadal mogą ratować życie, o ile będą zabezpieczone przed ich naruszeniem. Zakres rozwijających się i wdrażanych na nasze życie technologii cyfrowych jest przytłaczający" twierdzi Humphreys.

„Obserwujemy powstanie nowego porządku technologii Internetu Rzeczy. Teraz nie mówimy o urządzeniach, ale o całych systemach". Niezabezpieczenie jednego urządzenia będzie miało wpływ na kolejne. W roku 2013 hakerzy wykradli numery milionów kart kredytowych jednego z większych amerykańskich detalistów/sprzedawców, dzięki uzyskaniu dostępu do ich systemów poprzez ogrzewanie z dostępem do Internetu. Jedne urządzenia mogą być użyte do ataku na inne. Powinniśmy myśleć o bezpieczeństwie IoT jak o szczepionce. Jeśli nie jesteś chroniony, możesz przenieść na innych ryzyko zarażenia się. Im lepiej

będziemy chronić nasze urządzenia z użyciem silnych technologii bezpieczeństwa – tym lepiej dla nas.

„To jest powód, dla którego nie mogę wystarczająco podkreślić, jak ważne jest stosowanie norm z zakresu bezpieczeństwa informacji" – wyjaśnia Humphreys. „Mamy wiele sposobów na zminimalizowanie ryzyka ataku, trwają prace nad kolejnymi – jednak to firmy muszą je stosować".

Normy takie jak ISO/IEC 27001 i ISO/IEC 27002 tworzą wspólny język służący rozwiązywaniu problemów zarządzania ryzykiem i zgodności związanych z bezpieczeństwem informacji. ISO/IEC 27031 oraz ISO/IEC 27035 pomagają firmom skutecznie reagować na cyberataki. Istnieją również normy ISO/IEC określające sposoby szyfrowania oraz mechanizmy sygnatur, które mogą być włączone do produktów i aplikacji do ochrony transakcji online, używania karty kredytowej i przechowywanych danych.

Dla Humphreysa następne w kolejce są normy dotyczące prywatności. „Pracujemy, aby zbudować solidną podstawę normalizacyjną, która zabezpieczy nasze dane w połączonym cyfrowym świecie i zwiększy zaufanie konsumentów. Mamy nadzieję, że nasze normy będą wykorzystane do opracowania rozwiązań, które sprostają wyzwaniom związanym z Internetem Rzeczy".

Czy konsumentów to obchodzi?

Problem jest o tyle bardziej skomplikowany, o ile wielu z nas niechętnie, czasem celowo, poświęca swoją prywatność i bezpieczeństwo informacji w zamian za dostęp do, jak nam się wydaje, o wiele cenniejszej najnowocześniejszej technologii. Te urządzenia stały się obowiązkowymi elementami codziennego życia (must-have-it). Czy nasze dane są rzeczywiście aż tak cenne, aby zrezygnować z nowoczesnych rozwiązań?

Przyjrzyjmy się zachowaniom konsumentów w sieci. Ludzie regularnie wgrywają swoje zdjęcia i publikują filmiki video ze swoimi dziećmi, dzielą się swoimi poglądami politycznymi, celami podróży i swoimi ulubionymi sklepami. Kwestią nie jest to, czy powinniśmy tak bardzo upubliczniać swoją prywatność, ale jeśli taki jest nasz wybór, to czy zdajemy sobie sprawę, jaki to ma na nas wpływ i czy panujemy nad tym, jakie dane są od nas zbierane.

Internet ułatwia śledzenie i identyfikację ludzi, informacje o nas mogą wpaść w niepowołane ręce, a to jednak ryzyko. Świadomość bezpieczeństwa w sieci rośnie. Badania przeprowadzone przez National Consumers League w USA wykazały, że 76% amerykańskich nastolatków zdaje sobie sprawę, jak ważna jest prywatność w sieci i jak można zaszkodzić sobie przez aktywność on-line, jednak rzadko wiąże się te kwestie z IoT.

Komitet ISO ds. polityki konsumenckiej (ISO/COPOLCO) wpisuje te kwestie do programu prac normalizacyjnych. Niezrozumienie przez konsumentów konsekwencji niedostatecznego zabezpieczenia się w sieci nie oznacza, że nie powinni być w ogóle chronieni. „Świadomość konsumencka, nawyki i potrzeba bezpieczeństwa i prywatności są bardzo ważną częścią układanki, którą musimy się zająć" uważa Bill Dee, reprezentant ISO/COPOLCO. „W COPOLCO ukończyliśmy raport dotyczący luk w strategicznych normach z zakresu prywatności. Skupiamy się teraz na „świadomej prywatności i ochronie danych przy zakupie produktów i usług".

Świadoma prywatność

Według Eiseneggera problem tkwi w tym, że od samego początku większość przedmiotów codziennego użytku wykorzystywana przez konsumentów została wprowadzona na rynek bez dbałości o prywatność i ochronę danych. „Mimo istnienia wielu Norm Międzynarodowych, które firmy mogą wykorzystywać, by dbać o nasze raz zebrane dane osobiste, musimy stworzyć bezpieczną technologię IoT, która zapewni bezpieczeństwo w czasie rzeczywistym. Zmiana naszego podejścia nie tylko sprawi, że bezpieczeństwo będzie sprawą oczywistą, ale także ułatwi aktualizację zabezpieczeń".

Jednym z powodów, dla których firmy nie dbają o bezpieczeństwo urządzeń jest to, że projektanci pracujący nad technologiami IoT rzadko są ekspertami w dziedzinie bezpieczeństwa. „Inżynierowie powinni działać na wszystkich etapach procesów projektowych, które kładą silny nacisk na bezpieczeństwo, dzięki czemu powstanie mniej luk; obecnie zbyt wiele jest naprawiane po fakcie - uważa Eisenegger. Z nadzieją na zmianę tego stanu ISO/COPOLCO proponuje opracowanie normy, która dotyczyłaby cyfrowego projektowania zabezpieczeń prywatności w produktach i usługach".

„Gdybyśmy mogli stworzyć proces opracowywania zabezpieczeń inspirowany ciągłym doskonaleniem zgodnie z ISO 9001, tak jak ma to miejsce w ISO 10377 dotyczącej bezpieczeństwa produktów, zrobilibyśmy wielki krok do przodu" dodaje Eisenegger. „Taka norma mogłaby skupiać się na ułatwieniu znalezienia i ochronie naszych danych, zapewniać poufność analizy danych i oszacowanie bezpieczeństwa produktu".

„Zamiast zastanawiać się, czy konsumenci powinni akceptować domyślne opcje bezpieczeństwa i prywatności oferowane przez współczesne technologie, produkty i usługi, powinniśmy zapytać, co możemy zrobić, by konsumenci darzyli nas większym zaufaniem" mówi Eisenegger. „To nowa granica Norm Międzynarodowych z zakresu bezpieczeństwa i prywatności. Ta, która „zaszczepia" produkty i usługi, która chroni nasze dane i zapewnia kontrolę nad wykorzystywaniem danych w czasie rzeczywistym. Granica, która zmniejsza ilość danych zbieranych przez urządzenia, która informuje nas o działaniach strony trzeciej, wzmacniając identyfikowalność i odpowiedzialność".

Gdy te działania odniosą sukces, wówczas podobne podejście mogłoby rozwiązać wiele kwestii powiązanych, takich jak dostępność i wrażliwość cyfrowych danych oraz prywatność z jednoczesnym uwzględnieniem przystępności, uczciwości i niedyskryminowania.

Mimo istnienia wielu norm z zakresu cyberbezpieczeństwa, ISO nadal ma nad czym pracować w kwestii Internetu Rzeczy. „Grupa norm ISO/IEC 27001 jest świetnym narzędziem dla firm, które dbają o bezpieczeństwo naszych danych. Musimy jednak opracować rozwiązania, które będą odnosiły się do ryzyka związanego przede wszystkim z technologią IoT" uważa Eisenegger. Normy to świetny sposób, by wszystkie te kwestie zostały ujęte w międzynarodowym programie.

Nie możemy już zwlekać z podjęciem działań. Nasze domy, działalność i osobiste informacje są ściśle powiązane z miliardami innych osób, dzięki urządzeniom codziennego użytku. Internet Rzeczy przenosi prywatność i bezpieczeństwo na zupełnie nowy poziom. Aby nasze życie było ukryte przed oczami ciekawskich, musimy zamknąć drzwi i założyć w nich zamek.

Źródło: ISOfocus September-October 2016
Tłum. I.P.

Normy kablowe w gospodarstwie domowym

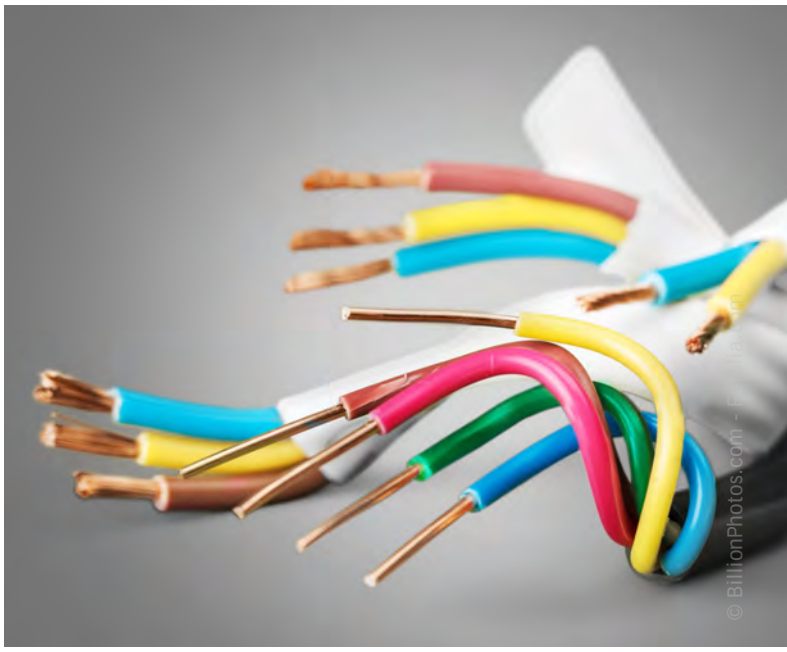
KT 53 ds. Kabli i Przewodów

W marcu 2015 roku, w KT 53 rozpoczęto prace nad normą własną. Norma ta będzie dotyczyć przewodów używanych na co dzień w każdym gospodarstwie domowym. Reprezentanci KT 53 wykazali inicjatywę normalizacji dot. osprzętu kablowego, dotychczasowe normy sięgały nawet 1986 roku. Istniała potrzeba utworzenia nowego dokumentu mającego na celu ujednolicenie nazewnictwa oraz metod badań kabli i przewodów elektrycznych do układania na stałe w budynkach.

Prace nad normą własną trwały półtora roku, co jest świetnym wynikiem , bo dotychczas prace mogły trwać prawie 3 lata. Do Grupy Projektowej 558 zgłosiło się aż 4 reprezentantów. Wykonawcą całego projektu jest Polska Izba Gospodarcza Elektrotechniki z siedzibą w Bydgoszczy. Opracowanie normalizacyjne dokumentu na konkretny produkt wymaga doskonałej znajomości Przepisów wewnętrznych CENELEC cz. 3 z 2014 roku, co też udało się osiągnąć właśnie w tej normie.

Normy opisujące produkt cechują się innymi wymaganiami formalnymi niż norma określająca metody badawcze. W niniejszej normie przywołano metody badań kabli i przewodów, jednak ze względu na potrzebę rynkową skupiono się na opisie żył przewodów i ich odpowiedniej izolacji oraz powłoce. Pamiętając o bezpieczeństwie przewodów, opisano również ich szczegółową budowę i właściwości mechaniczne oraz sposób ich oznaczania.

Ta Polska Norma zawiera wymagania odnośnie do przewodów wielożyłowych ogólnego przeznaczenia do układania na stałe o izolacji i powłoce z termoplastycznego polichlorku winylu (PVC). W tych przewodach napięcie znamionowe przewodów U_0/U nie przekracza 450/750 V. Przewody są przeznaczone do układania na stałe wewnątrz pomieszczeń. Norma dotyczy przewodów wielożyłowych o żyłach miedzianych jedno- i wielodrutowych z żyłą lub bez żyły



ochronnej. Wyjątkowo norma nie dotyczy przewodów okrągłych na napięcie znamionowe 300/500 V (U_0/U).

17 października 2016 roku została opublikowana norma własna PN-E-90068:2016-10 Przewody elektryczne - Przewody elektroenergetyczne na napięcie znamionowe 300/500V oraz 450/750V (U_0/U) - Przewody wielożyłowe ogólnego przeznaczenia do układania na stałe o izolacji z termoplastycznego polichlorku winylu (PVC)

Opublikowano PN-EN 60794-3-21:2016-06 Kable światłowodowe - Część 3-21: Kable zewnętrzne - Wymagania wyrobu dotyczące telekomunikacyjnych kabli napowietrznych samonośnych stosowanych do okablowania zabudowań

Opublikowana norma należy do wieloczęściowej normy PN-EN 60794 dotyczącej kabli światłowodowych. Światłowody to niewątpliwie jedne z najnowocześniejszych rozwiązań elektrotechnicznych ostatnich lat.

W ww. części IEC 60794 podano wymagania dotyczące wyrobu. Podano szczegółowe wymagania dotyczące telekomunikacyjnych, samonośnych, napowietrznych kabli światłowodowych stosowanych do okablowania obiektów. Wymagania zapewniają zgodność z ISO/IEC 11801 i ISO/IEC 24702. Do kabli objętych niniejszą normą stosowane są wymagania zawarte w specyfikacji grupowej IEC 60794-3-20 oraz w IEC 60794-3.

Opublikowano trzy części normy PN-EN 62631-3:
PN-EN 62631-3-1:2016-10 Właściwości dielektryczne stałych materiałów elektroizolacyjnych - Część 3-1: Wyznaczanie właściwości rezystancyjnych (pomiary przy prądzie stałym) - Rezystancja skrośna i rezystywność skrośna - Metoda ogólna
PN-EN 62631-3-2:2016-04 (...) – Rezystancja powierzchniowa i rezystywność powierzchniowa
PN-EN 62631-3-3:2016-08 (...) – Rezystancja izolacji

W opublikowanej normie w 2011 roku podano ogólne wytyczne dotyczące wyznaczania własności dielektrycznych stałych materiałów elektroizolacyjnych. W pierwszej części IEC 62631 opublikowanej w tym roku podano metodę wyznaczania rezystancji i rezystywności skrośnej materiałów elektroizolacyjnych przy zastosowaniu napięcia prądu stałego. W drugiej części tej normy podano metodę wyznaczania rezystancji i rezystywności powierzchniowej materiałów elektroizolacyjnych przy tych samych zastosowaniach. Natomiast w części trzeciej tej normy podano metody wyznaczania rezystancji izolacji albo rezystancji układów elektroizolacyjnych przy zastosowaniu napięcia prądu stałego.

Opublikowano PN-EN 50577:2016-02 Kable i przewody elektryczne - Badanie odporności na ogień kabli i przewodów bez ochrony specjalnej (klasyfikacja P)

W niniejszej Normie Europejskiej opisano metodę badań służącą do oceny utrzymania ciągłości zasilania dla kabli i przewodów elektrycznych posiadających cechę ognioodporności zgodnie z wymaganiami EN 13501-3. Na podstawie tych badań określa się czas utrzymania ciągłości obwodu kabli lub przewodów narażonych na działanie ognia w warunkach opisanych przez znormalizowaną krzywą czas/temperatura w EN 1363-1. Niniejszą normę powinno stosować się łącznie z EN 1363-1.

Niniejsza Norma Europejska dotyczy kabli i przewodów zasilających i sterowniczych na napięcie znamionowe do 600/1000 V włącznie. Kable lub przewody są badane w znormalizowanych, reprezentatywnych warunkach instalacji. Badania nie służą do oceny jakości pracy systemu kablowego. W niniejszej normie, w Załączniku A zawarto zakres bezpośredniego stosowania i zasady rozszerzenia zakresu stosowania wyników badań (EXAP) (Anex B). Wybór kabli do badań, w celu zakwalifikowania do odpowiedniej rodziny, znajduje się w Załączniku B. W przypadku, jeśli wybór przewodów nie jest zgodny z załącznikiem B wyniki badań mają zastosowanie jedynie do kabli testowanych.

Sektor Elektrotechniki

Substancje niebezpieczne w pracy

W bieżącym roku w KT 159 ds. Zagrożeń Chemicznych i Pyłowych w Środowisku Pracy opracowano dziewięć Polskich Norm własnych dotyczących oznaczania niebezpiecznych dla zdrowia człowieka substancji emitowanych do powietrza na stanowiskach pracy:

1. Triazotan(V)-propano-1,2,3-triyl (potocznie nitrogliceryna) (PN-Z-04466:2016-10) stosowany jest do produkcji materiałów wybuchowych, np. dynamitu i paliwa rakietowego, w przemyśle chemicznym, a także w produkcji leku stosowanego w leczeniu pacjentów z chorobą wieńcową. Triazotan(V)-propano-1,2,3-triyl jest dla człowieka toksyczny i wywołuje szereg dolegliwości. Do organizmu człowieka dostaje się w postaci par przez drogi oddechowe, doskonale wchłania się przez skórę, jest substancją działającą bardzo toksycznie na organizm człowieka po połknięciu.

2. Cyjanoakrylan etylu (PN-Z-04467:2016-10) stosowany jest w przemyśle chemicznym do produkcji klejów i polimerów. Kleje zawierające cyjanoakrylan etylu są bardzo popularne. Stosowane są do sklejania szkła, elementów metalowych, drewnianych, skórzanych, gumowych oraz elementów z tworzyw sztucznych. Cyjanoakrylan etylu po przekroczeniu dopuszczalnego stężenia w powietrzu na stanowisku pracy działa drażniąco na oczy, błony śluzowe dolnych i górnych dróg oddechowych, może powodować alergiczne zapalenie skóry. Związek wchłania się do organizmu podczas oddychania.

3. Nitropropan (PN-Z-04474:2016-10) jest mieszaniną izomerów (1-nitropropanu i 2-nitropropanu). Oba stosowane są w przemyśle chemicznym. 1-Nitropropan stosowany jest jako dodatek do farb i klejów. 2-Nitropropan jest wykorzystywany jako rozpuszczalnik do lakierów i polimerów. Może być także stosowany jako dodatek do paliwa w samochodach wyścigowych. Mieszanina izomerów nitropropanu wchłaniana jest do organizmu głównie przez drogi oddechowe. 1-Nitropropan wykazuje toksyczność ostrą przy wdychaniu, po naniesieniu na skórę i po połknięciu. 2-Nitropropan jest substancją rakotwórczą, wykazuje toksyczność ostrą przy wdychaniu i po

połknięciu.

4. 4-Chloro-3-metylofenol (PN-Z-04475:2016-10) stosowany jest jako środek bakteriobójczy i konserwujący kleje, gumy, farby, tusze, wyroby tekstylne i skórzane. Używany jest także do produkcji preparatów stosowanych przeciwko pasożytom zwierząt. 4-Chloro-3-metylofenol po przekroczeniu dopuszczalnego stężenia w powietrzu na stanowisku pracy działa drażniąco na oczy i może spowodować poważne ich uszkodzenie. Może powodować reakcje alergiczne skóry.

5. Metanol (PN-Z-04476:2016-10) stosowany jest w przemyśle chemicznym do produkcji formaldehydu, kwasu octowego i glikolu etylenowego, tworzyw sztucznych i włókien syntetycznych, barwników, środków ochrony roślin i płynów do mycia i odmrażania szyb samochodowych. Metanol jest substancją toksyczną, pary metanolu w bardzo dużych stężeniach w powietrzu mogą spowodować uszkodzenie nerwów wzrokowych. Skutkiem zatrucia drogą pokarmową jest utrata wzroku, uszkodzenie mięśnia sercowego oraz ostre uszkodzenie nerek.

6. Tellur (PN-Z-04477:2016-10) stosowany jest jako dodatek do stali, stopów ołowiu oraz stopów magnezu i miedzi. Składnik ten w stopach zwiększa ich elastyczność, wytrzymałość, twardość i odporność chemiczną. Tellur stosuje się także w elektrotechnice. Stosuje się go także do barwienia szkła i porcelany oraz w przemyśle chemicznym jako katalizator reakcji chemicznych. Używany jest także przy procesie wulkanizowania gumy i jako przeciwstukowy składnik benzyn. Przy stężeniach telluru w powietrzu na stanowisku pracy powodujących ostre zatrucie tellurem, może dojść do uszkodzenia wątroby, układu nerwowego i naczyniowo-sercowego. Przewlekłe narażenie na tellur wywołuje ból głowy, zaburzenia żołądkowo-jelitowe oraz alergiczne reakcje skórne. Tellur jest bardzo niebezpieczny dla kobiet w ciąży.

7. Tal (PN-Z-04478:2016-10) stosowany jest jako składnik niektórych stopów. Stosowany jest do produkcji szkieł optycznych, elementów półprzewodnikowych, fotoogniw, katalizatorów i pestycydów. Tal wchłania się do organizmu przez przewód pokarmowy, drogi oddechowe i skórę. Po przekroczeniu dopuszczalnego stężenia talu w powietrzu na stanowisku pracy, może dojść do uszkodzenia tkanki nerwowej, gruczołów skórnych i korzeni włosów oraz nerek i wątroby.

8. Hydrochinon (PN-Z-04479:2016-10) stosowany jest w przemyśle chemicznym przede wszystkim jako przeciwutleniacz oraz jako inhibitor polimeryzacji. Stosowany jest także do produkcji farb i olejów, do produkcji rozpuszczalników do farb, jest składnikiem tuszy i tonerów. Stosowany jest w fotografice. Hydrochinon jest substancją rakotwórczą, mutagenną, toksyczną i uczulającą, może powodować poważne uszkodzenie oczu. Jest bardzo toksyczny po połknięciu.

9. Tiuram (PN-Z-04480:2016-10) stosowany jest w przemyśle gumowym oraz ze względu na swoje grzybobójcze właściwości, jako składnik środków myjących, leków oraz chemicznych środków ochrony roślin. Tiuram po przekroczeniu dopuszczalnego stężenia w powietrzu na stanowisku pracy działa drażniąco na górne drogi oddechowe. W dużych dawkach działa toksycznie na płód. Jest też substancją o działaniu uczulającym.

Normy te można kupić na www.pkn.pl

Elżbieta Sosnowska – sekretarz KT 159

Moduły fotowoltaiczne

KT 54 ds. Chemicznych Źródeł Prądu

25 października br. opublikowano normę PN-EN 61215-1-1:2016-10 Moduły fotowoltaiczne (PV) do zastosowań naziemnych - Kwalifikacja konstrukcji i aprobata typu -- Część 1-1: Wymagania szczególne dotyczące badań naziemnych modułów fotowoltaicznych (PV) wykonanych z krzemu krystalicznego

Wyżej wymieniona część normy z IEC 61215 ustanawia wymagania IEC dla kwalifikacji konstrukcji i aprobaty typu modułów fotowoltaicznych do zastosowań naziemnych odpowiednich dla długookresowej eksploatacji w typowych warunkach klimatycznych, takich jak zostały zdefiniowane w normie IEC 60721-2-1. Zastosowanie normy przewidziane jest dla wszelkiego typu płaskich modułów wykonanych z krzemu krystalicznego.

Norma nie jest przeznaczona do modułów stosowanych w systemach z koncentratorami światła, chociaż może być wykorzystana do modułów w układach z niskim stopniem koncentracji (1 do 3 słońc). Dla takich modułów wszystkie testy są przeprowadzane w zakresie wartości prądu, napięcia i mocy spodziewanych przy planowanym stopniu koncentracji światła.

Celem opisanej sekwencji testów jest wyznaczenie elektrycznych i cieplnych charakterystyk modułu i wykazanie, najlepiej jak to jest możliwe w rozsądnych ramach czasowych i kosztów, że moduł będzie w stanie wytrzymać wydłużoną ekspozycję w warunkach klimatycznych, jak te wspomniane wcześniej. Aktualny oczekiwany czas życia w ten sposób kwalifikowanych modułów zależeć będzie od ich konstrukcji oraz środowiska i warunków w jakich będą one pracować.

Norma definiuje technologie modyfikacji PV procedur testowania i wymagań zgodnie z IEC 61215-1:2016 i IEC 61215-2:2016.

Sektor Elektryki

Komitety Techniczne
Komitety Zadaniowe
Podkomitety Techniczne
październik 2016

Komitety Techniczne

Zmiany zakresu tematycznego Komitetów Technicznych

- **KT 20 ds. Skóry i Obuwia** rozszerzył zakres współpracy o CEN/TC 382 PFOS, współpraca przejęta od KT 249 ds. Analizy Chemicznej.

Nowi Przewodniczący Komitetów Technicznych

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

- w KT 35 ds. Mleka i Przetworów Mlecznych **mgra inż. Marka Murawskiego** reprezentującego Krajowy Związek Spółdzielni Mleczarskich - Związek Rewizyjny
- w KT 132 ds. Silników Spalinowych **dra inż. Tomasza Lusa** reprezentującego Akademię Marynarki Wojennej im. Bohaterów Westerplatte
- w KT 210 ds. Armatury Przemysłowej i Rurociągów Przemysłowych **mgra inż. Krzysztofa Grzesiaka** reprezentującego Urząd Dozoru Technicznego
- w KT 242 ds. Informacji i Dokumentacji **dr Jolantę Szulc** reprezentującą Uniwersytet Śląski
- w KT 312 ds. Robót Ziemnych **dra inż. Zdzisława Skutnika** reprezentującego Szkołę Główną Gospodarstwa Wiejskiego w Warszawie.

Nowi Sekretarze Komitetów Technicznych

W październiku Prezes PKN powołał do pełnienia funkcji Sekretarza:

- w KT 51 ds. Pomiarów Przemysłowych Wielkości Nieelektrycznych **mgra inż. Piotra Szymańskiego** z Polskiego Komitetu Normalizacyjnego
- w KT 128 ds. Projektowania i Wykonawstwa Konstrukcji Metalowych i Konstrukcji Zespolonych **mgr inż. Barbarę Pałczyńską** z Polskiego Komitetu Normalizacyjnego
- w KT 213 ds. Projektowania i Wykonawstwa Konstrukcji z Betonu **mgr inż. Barbarę Pałczyńską** z Polskiego Komitetu Normalizacyjnego
- w KT 252 ds. Projektowania Konstrukcji Murowych **mgr inż. Barbarę Pałczyńską** z Polskiego Komitetu Normalizacyjnego
- w KT 257 ds. Metrologii Ogólnej **mgra inż. Piotra Szymańskiego** z Polskiego Komitetu Normalizacyjnego
- w KT 297 ds. Informacji Geograficznej **mgra inż. Sławomira Maciejewskiego** z Polskiego Komitetu Normalizacyjnego
- w KT 298 ds. Geodezji **mgra inż. Piotra Szymańskiego** z Polskiego Komitetu Normalizacyjnego.

Nowi członkowie Komitetów Technicznych

W październiku Prezes PKN powołał na członków KT następujące podmioty:

- **Cert Partner Sp. z o.o. Sp.k.** do KT 281 ds. Bezpieczeństwa Maszyn pod Względem Elektrycznym
- **EXPRAN Sp. z o.o.** do KT 321 ds. Elektronicznych Inhalatorów Nikotyny oraz Płynów do ich Uzupełniania
- **Politechnikę Poznańską** do KT 104 ds. Kompatybilności Elektromagnetycznej
- **Politechnikę Wrocławską** do KT 130 ds. Aparatury Chemicznej, Zbiorników i Butli do Gazów
- **Polwax SA** do KT 222 ds. Przetworów Naftowych i Cieczy Eksploatacyjnych
- **PULSAR K. Bogusz Spółka jawna** do KT 264 ds. Systemów Sygnalizacji Pożarowej
- **STAL-PRODUKT Spółka jawna, Kornelia Zaława, Dariusz Zaława** do KT 145 ds. Stali Jakościowych i Specjalnych
- **Uniwersytet Łódzki** do KT 297 ds. Informacji Geograficznej
- **Związek Banków Polskich** do KT 271 ds. Bankowości i Bankowych Usług Finansowych.

Odwołania członków Komitetów Technicznych

W październiku Prezes PKN odwołał z członka KT:

- Akademię Obrony Narodowej z KT 306 ds. Bezpieczeństwa Powszechnego i Ochrony Ludności
- BAYER Sp. z o.o. z KT 179 ds. Ochrony Cieplnej Budynków, KT 180 Bezpieczeństwa Pożarowego Obiektów, KT 211 Wyrobów do Izolacji Cieplnej w Budownictwie, KT 307 ds. Zrównoważonego Budownictwa i KT 308 ds. Oceny Uwalniania Substancji Niebezpiecznych
- Centrum Badań i Dozoru Górnictwa Podziemnego Sp. z o.o. z KT 6 ds. Systemów Zarządzania
- ELTEST M. Jewtuch Sp.J. z KT 104 ds. Kompatybilności Elektromagnetycznej
- Glaspol Sp. z o.o. z KT 198 ds. Szkła
- Polski Związek Inżynierów i Techników Budownictwa Oddział Warszawski z KT 108 ds. Kruszyw i Kamienia Budowlanego
- PRZERÓBKĘ PLASTYCZNĄ NA ZIMNO-BAILDON Sp. z o.o. z KT 145 ds. Stali Jakościowych iSpecjalnych.

Podkomitety Techniczne

Nowi Przewodniczący Podkomitetów Technicznych

W październiku Prezes PKN powołał do pełnienia funkcji Sekretarza:

- w KT 176/PK 3 ds. Środków Uzbrojenia i Wyposażenia Inżynieryjnego **dra hab. inż. Adama Januszko** reprezentującego Wojskowy Instytut Techniki Inżynieryjnej im. Profesora Józefa Kosackiego.

Nowi członkowie Podkomitetów Technicznych

W październiku Prezes PKN powołał na członków PK następujące podmioty:

- **PIT–RADWAR SA** do KT 176/PK 5 ds. Sprzętu Radiotechnicznego, Środków Łączności, Specjalnych Urządzeń Elektrotechnicznych, Techniki Świetlnej oraz Systemów i Środków Informatyki
- **Polwax SA** do KT 222/PK 1 ds. Paliw Płynnych i KT 222/PK 3 ds. Olejów Smarowych.

POLSKI KOMITET NORMALIZACYJNY

E-DOSTĘP

Polskie Normy w jednym miejscu!

Oferujemy

- dostęp z licencją jednoroczną lub trzyletnią (stała opłata roczna)
- możliwość przeglądania norm oraz ich wydruk dla celów wewnątrzzakładowych użytkownika
- automatyczną aktualizację
- możliwość wyszukiwania normy po numerze lub jego fragmencie, tytule, stanie aktualności oraz wyróżniku ICS
- możliwość umieszczenia w zbiorze nowo zakupionych, aktualnych norm

Łatwy dostęp

E-dostęp do zakupionego, wybranego przez użytkownika zbioru norm (minimum 25 norm)

Bezpieczeństwo

uwierzytelnianie w systemie poprzez unikalny login i hasło

Aktualizacja

na bieżąco aktualizowany zbiór PN 24 h/7 dni w tygodniu

W celu uzyskania wyceny usługi prosimy o przesyłanie listy norm na adres: wsmsekr@pkn.pl