

# wiadomości

• N O R M A L I Z A C J A •

# PKN

5/2018



# DZIEŃ

NORMALIZACJI

# POLSKIEJ

# 5/2018

- 3 OD REDAKCJI
- 4 DZIEŃ NORMALIZACJI POLSKIEJ
- AKTUALNOŚCI
- 12 Normy Międzynarodowe to narzędzie zgodności z wymaganiami RODO
- 16 Bezpieczeństwo pożarowe obiektów
- Z PRAC NORMALIZACYJNYCH
- 18 Ochrona sieci kolejowych przed cyberatakami
- 24 Gazownictwo
- 28 **ORGANY TECHNICZNE** - kwiecień 2018

„WIADOMOŚCI PKN” to miesięcznik elektroniczny publikowany cyklicznie na stronie internetowej PKN [www.pkn.pl](http://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

Piotr Jotel - tel. 22 556 75 98

#### REDAKCJA:

00-950 Warszawa, skr. poczt. 411

ul. Świętokrzyska 14

e-mail: [redakcja@pkn.pl](mailto:redakcja@pkn.pl)

#### WYDAWCA:

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

Materiały publikowane w miesięczniku „Wiadomości PKN” są chronione prawami autorskimi. Ich kopiowanie i rozpowszechnianie (w całości lub części) wymaga zgody wydawcy, a cytowanie powołania się na źródło.

Artykuły publikowane w miesięczniku przedstawiają punkt widzenia Autorów i nie zawsze są tożsame z poglądami wydawcy. Redakcja zastrzega sobie prawo do adyustacji tekstów i zmiany tytułów. Materiałów niezamówionych redakcja nie zwraca.

Redakcja nie ponosi odpowiedzialności za treść ogłoszeń.

© Copyright by Polski Komitet Normalizacyjny

Zdjęcia © Adobe Stock

Okładka © Adobe Stock



## Szanowni Czytelnicy!

Producenci pasz, środków żywnościowych, operatorzy transportu, producenci maszyn i urządzeń, materiałów opakowaniowych, środków czystości etc. – oni wszyscy mają wpływ na jakość naszej żywności. Dlatego tak istotne jest bezpieczeństwo całego łańcucha rolno-spożywczego – zapobieganie skażeniu żywności, promowanie higieny żywności, zdrowia roślin i dobrostanu zwierząt.

Mikroorganizmy patogenne, zanieczyszczenia procesowe, organizacje łańcucha żywnościowego, system zarządzania bezpieczeństwem żywności, ochrona konsumenta – te zagadnienia poruszone zostały na konferencji zorganizowanej z okazji Dnia Normalizacji Polskiej. Więcej o tym wydarzeniu można przeczytać w bieżącym numerze.

Joanna Skalska



# DZIEŃ NORMALIZACJI POLSKIEJ

## Konferencja

### Jakość i bezpieczeństwo żywności



Czy wiesz, co jesz? Nieznajomość przepisów prawa i zaleceń zawartych w normach stwarza ogromne ryzyko dla nas wszystkich. Może to prowadzić do poważnych konsekwencji – zanieczyszczeń procesowych żywności. Dlatego tak ważne jest nie tylko wczesne rozpoznawanie zagrożeń, lecz także opracowanie wspólnych metod ich minimalizowania. Potrzebne są wskazówki, najlepsze praktyki i testy w celu promowania i zwiększenia bezpieczeństwa, jakości i wydajności w całym przemyśle spożywczym. W osiągnięciu tych celów pomocne są Polskie Normy.

Tegoroczny Dzień Normalizacji Polskiej obchodziliśmy pod hasłem: „Jakość i bezpieczeństwo żywności”. PKN zorganizował 23 maja konferencję, podczas której mówiliśmy o wymaganiach i kryteriach, które muszą być spełnione, byśmy mieli pewność, że kupujemy zdrową żywność. Wszystko po to, żeby być świadomym konsumentem, producentem i dystrybutorem.

Konferencję otworzył **Tomasz Schweitzer**, Prezes PKN, który powitał przybyłych gości. Następnie **Jolanta Kochańska** i **Teresa Sosnowska** powiedziały o normalizacji dla bezpieczeństwa żywności. Omówiły system normalizacyjny w Polsce, Europie i na świecie. Wskazały, które Organy Techniczne



Tomasz Schweitzer



Jolanta Kochańska



Teresa Sosnowska

zajmują się normalizacją w zakresie żywności. Następnie skupiły się na normach odnoszących się do poszczególnych aspektów związanych z żywnością, czyli: systemu zarządzania bezpieczeństwem żywności, oznaczania zanieczyszczeń procesowych w żywności, alergenów czy pierwiastków śladowych. Podkreśliły, że rolą normalizacji w bezpieczeństwie żywności jest m.in.:

- opracowanie znormalizowanego systemu zarządzania bezpieczeństwem żywności z uwzględnieniem wymagań prawnych, ukierunkowanego na dostarczanie bezpiecznych wyrobów;
- opracowywanie znormalizowanych metod badań dotyczących określania zawartości składników istotnych z punktu widzenia bezpieczeństwa żywności;
- ochrona konsumentów – wykrywanie zafałszowania żywności.

**Profesor Krzysztof Kwiatek** z Państwowego Instytutu Weterynaryjnego – Państwowego Instytutu Badawczego przedstawił prezentację nt. wymagań i kryteriów mikrobiologicznych dla żywności, omówił stare i nowe podejście z wykorzystaniem oceny ryzyka, norm i normalizacji. Podał definicję bezpieczeństwa żywności, czyli pewności, że żywność nie zaszkodzi konsumentowi, jeżeli jest przygotowana i/lub spożyta zgodnie z jej przeznaczeniem. Podkreślił, że bezpieczeństwo mikrobiologiczne to ważny element w działalności firm spożywczych. Zakłada ono nieobecność lub akceptowalne poziomy: zanieczyszczeń mikroorganizmami patogennymi i saprofitycznymi, towarzyszącym im toksyn, które czynią żywność szkodliwą dla zdrowia poprzez ostre lub chroniczne oddziaływanie.

Ponadto podał zasady, które zapewnią wiarygodne wyniki badań, akceptowane przez zainteresowanych, np. stosowanie zharmonizowanych procedur badawczych we wszystkich laboratoriach i krajach, normy metodyczne opracowane w wyniku międzynarodowych prac normalizacyjnych. Na zakończenie podkreślił, że normalizacja i normy – to ważny dział prawa żywnościowego oraz wskazał na wzrastające znaczenie przedmiotowych norm zakładowych w zapewnieniu mikrobiologicznego bezpieczeństwa żywności.

**Krzysztof Kwiatek**, reprezentant Ministerstwa Rolnictwa i Rozwoju Wsi, powiedział o wykorzystaniu norm w regulacjach prawnych w obszarze bezpieczeństwa żywności. Stwierdził, że źródłami prawa powszechnie obowiązującego



*Krzysztof Kwiatek*



*Krzysztof Popławski*

według art. 87 Konstytucji RP są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe, rozporządzenia, akty prawa miejscowego. Normy natomiast to czynnik służący zapewnieniu jednolitego przeprowadzenia kontroli oraz ich stałej, wysokiej jakości (preambuła rozporządzenia 882/2004).

Na konferencji omówiono także normę ISO 22000 w kontekście korzyści dla organizacji należącej do łańcucha żywnościowego. **Katarzyna Rokosa** z Polskiego Centrum Akredytacji przedstawiła najważniejsze zmiany znowelizowanej normy, odpowiadające współczesnym potrzebom rynku. Korzyści wynikające z nowelizacji normy dotyczą:

- aktualizacji terminów i definicji;
- uproszczonej treści, łatwiejszej do zrozumienia przez wszystkie zainteresowane strony;
- dostosowania wymagań normy do możliwości ich spełnienia przez małe i średnie przedsiębiorstwa.

Koncentrują się one m.in. na podejściu do ryzyka, ujednoczeniu formatu i zapewnieniu spójności między normami, co powoduje uproszczenie ich zintegrowanego wykorzystania oraz sprawia, że są one bardziej czytelne i bardziej zrozumiałe dla użytkowników. W znowelizowanej normie zaktualizowano także terminy, które dotychczas uznane były za potencjalnie mylące i zastosowano wyjaśnienia dotyczące różnic pomiędzy Krytycznymi Punktami Kontroli, Programami Wstępnymi oraz Operacyjnymi Programami Wstępnymi.



*Katarzyna Rokosa*



*Hanna Mojska*

**Profesor Hanna Mojska** z Instytutu Żywności i Żywienia im. prof. dra med. Aleksandra Szczygła przybliżyła trendy zmian w zawartości zanieczyszczeń procesowych w żywności, ze szczególnym uwzględnieniem akryloamidu.

Akryloamid powstaje w żywności w wyniku reakcji Maillarda zachodzącej w wysokiej temperaturze, np. podczas smażenia, pieczenia. Potwierdzono jego obecność w termicznie przetwarzanych produktach zbożowych i ziemniaczanych oraz w kawie. Międzynarodowa Agencja Badań nad Rakiem (IARC) w 1994 r. zaliczyła akryloamid do związków „prawdopodobnie rakotwórczych dla ludzi”. W Polsce rozpoczęto prowadzenie badań monitoringowych zawartości akryloamidu w żywności już w 2004 r.

H. Mojska podała przepisy prawne dotyczące zawartości akryloamidu w żywności, tj. Rozporządzenie Komisji (UE) z dnia 20 listopada 2017 r. ustanawiające środki łagodzące i poziomy odniesienia służące ograniczeniu obecności akryloamidu w żywności (2017/2158) – obowiązuje od 11 kwietnia 2018 r. Zwróciła także uwagę na normy metodyczne, tj. PN-EN 16618:2015-06 - Analiza żywności - Oznaczanie akryloamidu w żywności metodą chromatografii cieczowej sprzężonej z tandemową spektrometrią mas (LC-ESI-MS/MS). Opublikowanie normy powinno przyczynić się do ujednoczenia metodyki oznaczania akryloamidu i zapewnienia miarodajności uzyskiwanych wyników badań.



Anna Bugajewska

O walidacji ryzyka wzrostu bakterii patogennych, w tym *Listeria monocytogenes* w żywności gotowej do spożycia (RTE) mówiła **doktor Anna Bugajewska** z Silliker Polska Sp. z o.o. Prelegentka omówiła najważniejsze drobnoustroje wywołujące zakażenia i zatrucia pokarmowe, wśród których *Listeria monocytogenes* jest jednym z najbardziej zjadliwych patogenów przenoszonych przez żywność. Przedstawiła również wymagania dla laboratoriów przeprowadzających badanie obciążeniowe, wśród których znalazły się m.in.: wiedza i doświadczenie eksperckie, akredytacja laboratorium, odpowiednie warunki i zdolność przechowywania oraz właściwy poziom biobezpieczeństwa.



Andrzej Starski

Monitorowanie biologicznych i chemicznych czynników ryzyka w żywności omówił **Andrzej Starski** z Narodowego Instytutu Zdrowia Publicznego – Państwowego Zakładu Higieny, podając podstawowe definicje i zakres monitorowania, dane ilościowe nt. prowadzonego monitoringu w wybranych obszarach oraz badania w kierunku: kryteriów mikrobiologicznych żywności, dodatków do żywności, zanieczyszczeń chemicznych żywności. Prelegent przedstawił dwa podejścia do definicji monitorowania czynników ryzyka:

- urzędowa kontrola – oznaczająca każdą formę kontroli, którą właściwy organ lub wspólnota wykonuje do celów sprawdzenia zgodności z prawem paszowym i żywnościowym, regułami dotyczącymi zdrowia zwierząt i ich dobrostanu;
- monitorowanie – oznaczające prowadzenie zaplanowanej sekwencji obserwacji i pomiarów w celu uzyskania obrazu stanu zgodności z prawem paszowym i żywnościowym, regułami dotyczącymi zdrowia zwierząt i ich dobrostanu.



Końcowy referat dotyczący relatywizmu bezpieczeństwa żywności wygłosił **doktor Antoni Pluta**, przewodniczący KT 35 ds. Mleka i Przetworów Mlecznych. Zwrócił uwagę, że żywność, sposoby jej wytwarzania i konsumpcja są ważnym składnikiem kulturowym, religijnym, turystycznym itp. każdego społeczeństwa. W swojej prezentacji poruszył problem fałszowania żywności, podał też przykłady niebezpiecznej żywności, odwołując się m.in. do szkodliwego wpływu ołowiu i innych metali ciężkich na organizm człowieka. Podjął także kwestie związane z GMO. W uprawie roślin GMO nie chodzi o wydajność tylko o korzyści ekonomiczne, konkurencję i „chwilową” przewagę. Prelegent zaapelował, żeby pogoń za zyskiem nie przesłaniała wartości naszego zdrowia. Wymienił także nadrzędne kategorie determinant zdrowia, z których największe znaczenie dla kształtowania zdrowia ma styl życia ludzi (55%).

W prezentacji przytoczył cytat, który może być całościowym podsumowaniem rozważań i zagadnień poruszanych podczas konferencji: „Bezpieczeństwo żywności to pojęcie relatywne; nie jest nierozzerwalną biologiczną cechą żywności. Żywność może być bezpieczna dla niektórych osób, ale dla innych być niebezpieczną, bezpieczną na pewnym poziomie spożycia, ale nie na innym, oraz bezpieczną w pewnym punkcie czasowym, w pewnym wieku człowieka, a w innym – nie. Zamiast tego definiujemy bezpieczną żywność jako taką, w której pewien poziom ryzyka nie został przekroczony. Decyzje, co do akceptowalności tego poziomu, powiązane są z opiniami, wartościami, jak również stanem wiedzy (...)” – Nestle M., *Safe food: bacteria, biotechnology, and bioterrorism*.



Antoni Pluta

## Nagroda PKN – Kompas Normalizacji

Obchody Dnia Normalizacji Polskiej są okazją do uroczystego uhonorowania osiągnięć w zakresie wspierania normalizacji, w tym m.in. zaangażowania w promocję normalizacji lub szczególny wkład w promowanie systemu normalizacji dobrowolnej. Nagroda PKN może być przyznana osobom fizycznym, prawnym oraz jednostkom organizacyjnym nieposiadającym osobowości prawnej, polskim i zagranicznym.

W tym roku nagrodą wyróżniono Władysława Moronia i Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy.

Władysław Moroń jest związany z zagadnieniem normalizacji od samego początku swojej kariery zawodowej. Już w latach 1964-69, będąc pracownikiem Instytutu łączności we Wrocławiu, został powołany do pracy w departamencie elektrotechniki w Instytucie Normalizacyjnym Rady Wzajemnej Pomocy Gospodarczej w Moskwie. Zainicjował tam program prac nad normami dotyczącymi kompatybilności elektromagnetycznej bloku wschodniego, które były oparte na normach międzynarodowych IEC i CISPR.

W 1994 r. został powołany przez prezesa Polskiego Komitetu Normalizacyjnego na przewodniczącego Normalizacyjnej Komisji Problemowej nr 104, a następnie od 2002 r. Komitetu Technicznego nr 104 ds. Kompatybilności Elektromagnetycznej, którą to rolę pełni po dzień dzisiejszy.

Zagadnienia rozpatrywane na posiedzeniach, związane z tematyką KT 104, dotyczą projektów norm międzynarodowych i europejskich regulujących oddziaływanie elektromagnetyczne między różnorodnymi urządzeniami i systemami oraz ustalających metody pomiarów energii elektromagnetycznej oddziałującej na człowieka.

Komitet tłumaczy istotne Normy Europejskie na język polski, starając się zachowywać jednolitą i przejrzystą polską terminologię co, przy braku jakichkolwiek działań w zakresie terminologii dziedzinowej gdziekolwiek indziej, jest sprawą kluczową. Od początku swojego istnienia Komitet przetłumaczył około 150 norm.



Władysław Moroń



*Daniel Podgórski, Tomasz Schweitzer, Danuta Koradecka*

Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy jest jednym z najważniejszych partnerów PKN, uczestniczącym w działalności normalizacyjnej w dziedzinie bezpieczeństwa i higieny pracy oraz ergonomii. Współpracę CIOP z PKN datuje się od początku utworzenia Instytutu, tj. od lat 50. ubiegłego wieku, kiedy to w Instytucie powoływano Komisje Normalizacyjne opracowujące poszczególne Polskie Normy – wówczas dokumenty o charakterze techniczno-prawnym.

CIOP-PIB, jako ośrodek wiodący w kraju w zakresie licznych aspektów bezpieczeństwa i higieny pracy oraz ergonomii, jest członkiem 22 organów technicznych PKN: KT 1, 21, 22, 104, 143, 157, 158, 159, 161, 206, 248, 268, 276, 280, 281, 291, 299, 305, 308, 314, 317 oraz KT 176/PK 4. Za pośrednictwem swoich reprezentantów Instytut aktywnie uczestniczy w pracach i posiedzeniach wymienionych KT/PK. Uczestniczy w pracach Grup Projektowych, opiniuje projekty Polskich Norm, Norm Europejskich i Norm Międzynarodowych oraz innych dokumentów normalizacyjnych, uczestniczy w głosowaniach, a także

deleguje ekspertów do Grup Roboczych organizacji normalizacyjnych międzynarodowych i europejskich. Warto dodać, że w siedmiu KT reprezentanci Instytutu zostali wybrani na Przewodniczących, co potwierdza autorytet, jakim cieszy się CIOP-PIB w środowisku zajmującym się normalizacją zagadnień związanych z bezpieczeństwem, ochroną pracy i ergonomią.

Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy odznacza się zaangażowaniem i profesjonalizmem zarówno jako jednostka prowadząca sekretariaty KT, jak i uczestnik międzynarodowych i europejskich prac normalizacyjnych oraz autor projektów Polskich Norm.

Mamy nadzieję, że „Kompas Normalizacji” będzie dla nagrodzonych nie tylko uwieńczeniem dotychczasowej działalności normalizacyjnej i zaangażowania w jej popularyzację, lecz także motywacją do jej dalszego współtworzenia i doskonalenia.

*Red.*



# Normy Międzynarodowe to narzędzie zgodności z wymaganiami RODO

Organizacje z całego świata mają podporządkować się nowym europejskim regulacjom dotyczącym ochrony danych osobowych.

Michael A. Mullane

25 maja br. wejdzie w życie Ogólne Rozporządzenie o Ochronie Danych Unii Europejskiej (RODO) i będzie mieć ogromny wpływ na własności internetowe na całym świecie oraz na wszystkie organizacje, bez względu na to, gdzie mają swoje serwery, jeśli tylko dostarczają obywatelom Unii Europejskiej różnego rodzaju informacji, treści lub usługi online.

Właściciele zasobów sieciowych będą potrzebowali jednoznacznie wyrażonych przez użytkowników zgód, aby móc dalej zbierać, przechowywać, analizować dane osobowe czy dzielić się nimi z firmami analitycznymi, partnerami reklamowymi, grupami marketingowymi i innymi podmiotami zewnętrznymi, tak jak było to możliwe dotychczas. Prawdopodobnie zmieni to sposób traktowania danych osobowych wszędzie, ponieważ firmy będą chciały uniknąć dodatkowych kosztów związanych z różnymi sposobami zarządzania danymi.

RODO nakłada poważne ograniczenia na przekazywanie danych poza Unię Europejską, bez względu na to, czy odbiorcą są inne kraje czy organizacje międzynarodowe. Tylko pełna zgodność z obowiązkowymi przepisami stanowi warunek uniknięcia surowych sankcji, w tym kar pieniężnych do wysokości nawet 20 milionów euro albo 4% całkowitego obrotu, jeśli kwota jest wyższa.

Organizacje na całym świecie ścigają się z czasem, aby zapewnić przestrzeganie praw użytkowników, zwiększyć ochronę danych i zagwarantować prywatność na swoich stronach internetowych. Normy Międzynarodowe dostarczają narzędzia w postaci wypróbowanych i sprawdzonych technologii, które pomogą osiągnąć zgodność z nowym prawem UE.

## Wyzwania

RODO obejmuje szeroki zakres danych osobowych, w tym identyfikatory sieciowe takie jak np. adres IP i pliki cookie, a także dane kart kredytowych i informacje o stanie zdrowia. To zasadniczo zmieni sposób, w jaki organizacje zbierają dane osobowe, jak je przechowują i jak z nich korzystają.

Na przykład, aby zapewnić użytkownikowi „prawo do bycia zapomnianym” organizacje będą musiały mieć możliwość wykasowania czyichś danych personalnych w każdej chwili. RODO wprowadza również prawo do „przenoszenia danych”; chodzi o to, aby obywatele mogli swobodnie przenosić swoje dane osobowe od jednego usługodawcy do innego.

RODO zagwarantuje, że dane osobowe będą przechowywane tylko za wyraźną zgodą klienta, wykorzystywane tylko w celu, dla którego zostały pozyskane i przechowywane nie dłużej niż to konieczne. Zgoda na wykorzystanie danych osobowych powinna być jasna i zwięzła i w każdej chwili użytkownicy będą mogli ją wycofać.

Organizacje będą musiały przestrzegać ścisłych wytycznych po to, żeby dane były zawsze poprawne i przetwarzane zgodnie z zasadami w jednolity sposób. Jeśli dojdzie do jakichkolwiek naruszeń bezpieczeństwa, organizacje będą miały obowiązek poinformować właściwe organy nadzorcze w ciągu 72 godzin.

W miarę jak zbliża się 25 maja, informatycy przebudowują witryny internetowe w taki sposób, aby te nie gromadziły już automatycznie danych, kiedy tylko ktoś wejdzie na stronę. Ściągają każdy rodzaj oprogramowania zaprojektowanego tak, aby od początku domyślnie zapewniało prywatność. Jednak mimo to wielu dostawców usług internetowych jest zaniepokojonych wymaganiami, tym bardziej że oficjalne wytyczne są skomplikowane i niekiedy trudne do zastosowania.

## Przydatne normy

Normy Międzynarodowe zawierają solidny i niezawodny model, przydatny przy gromadzeniu, przechowywaniu i przetwarzaniu wrażliwych danych w warunkach zróżnicowanych wymagań regulacyjnych, oparty na najlepszych praktykach określonych przez wiodących ekspertów branżowych i technologicznych z całego świata. Normy opracowane przez ekspertów z Podkomitetu (SC) 27: *IT Security techniques* – będącego częścią ISO/IEC JTC 1, który jest Wspólnym Komitetem Technicznym IEC i ISO zajmującym się technologią informacyjną – dostarczają nie tylko kompletny zestaw narzędzi i metodologię zarządzania bezpieczeństwem danych, lecz także udostępniają najlepsze praktyki, sprawdzone w realnych warunkach.



© YB / Adobe Stock

Najlepsze praktyki obejmują kwestie bezpieczeństwa danych, wymiany informacji, bezpieczeństwa przechowywania i przetwarzania. Rodzina norm ISO/IEC 27000, obejmująca techniki bezpieczeństwa w technologiach informacyjnych, odnosi się do obszernej tematyki, co umożliwia zainteresowanym porównywanie najlepszych praktyk w zakresie wdrażania, modernizacji i ciągłego udoskonalania nadzoru.

W tym kontekście trzeba wspomnieć o normie ISO/IEC 27001 *Information technology – Security techniques – Information security management systems – Requirements*. Zdaniem międzynarodowych specjalistów zajmujących się ochroną danych (IT Governance): „firma, która wdrożyła ISO/IEC 27001 wykonała przynajmniej połowę pracy do osiągnięcia zgodności z wymaganiami RODO, dzięki minimalizacji ryzyka naruszeń”.

ISO/IEC 27001 identyfikuje potencjalne zagrożenia dotyczące danych klientów i interesariuszy i gwarantuje, że organizacje wdrażają właściwe środki minimalizujące ryzyko. Norma obejmuje szyfrowanie, testowanie na bieżąco, ocenę ryzyka oraz zdolność szybkiego przywrócenia dostępu do danych osobowych w sytuacji incydentu.

Obecnie opracowywana jest ISO/IEC CD 27552, która będzie rozszerzeniem ISO/IEC 27001 w zakresie wymagań dotyczących zarządzania prywatnością. Norma obejmuje procesy mające na celu ochronę przed przechwyceniem danych, a także zachowanie ich zgodności, dostępności, integralności i poufności.

Normy ISO/IEC 19592-1 and ISO/IEC 19592-2 *Information technology – Security techniques – Secret sharing*, w zakresie wymagań ogólnych i mechanizmów podstawowych, opisują najlepsze praktyki w technikach kryptograficznych, jakich używa się do zabezpieczenia poufności wiadomości (*secret sharing*). Te techniki mogą być wykorzystane do bezpiecznego przechowywania wrażliwych danych w systemach rozproszonych.

Norma ISO/IEC 29100 *Information technology – Security techniques – Privacy framework* opisuje model ochrony danych osobowych w technologiach informacyjno-komunikacyjnych (TIK) ISO/IEC 27018 umożliwiający użytkownikom zarządzanie bezpieczeństwem danych osobowych w publicznie dostępnych chmurach.

Norma ISO/IEC 29101 *Information technology – Security techniques – Privacy architecture framework* określa strukturę i powiązane z nią środki kontroli w zakresie ochrony prywatności w systemach TIK, które przechowują i przetwarzają dane osobowe.

Przydatna w nauce, edukacji i szkoleniach norma ISO/IEC 29187-1 *Information technology – Identification of privacy protection requirements pertaining to learning, education and training* uwzględnia te wymagania publiczne, które regulują tworzenie, używanie i wymianę danych osobowych, a także zarządzanie cyklem życia informacji. Obejmuje między innymi przepisy dotyczące ochrony konsumentów, prywatności i dostępności indywidualnej.

## Ocena zgodności

Ponieważ nie każde ryzyko jest związane z zastosowaniem technologii, ważne jest, aby odpowiedzialni za zarządzanie danymi posiadali wymagane szkolenia, wiedzę i umiejętności. Prace Komitetu ds. Oceny Zgodności (*Committee on Conformity Assessment – CASCO*) – stworzonego wspólnymi siłami przez IEC i ISO – mają kluczowe znaczenie dla procesu ustalania, czy organizacja spełnia wymagania związane z jej kompetencjami technicznymi również w innych dziedzinach.

Norma ISO/IEC 17024 określa ogólne wymagania dotyczące certyfikacji personelu, natomiast ISO/IEC 17065 obejmuje wymagania dotyczące certyfikowania produktów, procesów i usług.

Przestrzeganie odpowiednich Norm Międzynarodowych zapewnia skuteczne wdrażanie najlepszych praktyk mających na celu ochronę danych osobowych i ograniczanie ryzyka. Organizacje mogą wykorzystywać normy do budowania nowych cyfrowych relacji z klientami, a to jest kamień węgielny wymogów RODO.

Normy Międzynarodowe mogą odgrywać ważną rolę w ochronie reputacji marki i minimalizacji niepożądanych skutków wizerunkowych, zapewniając zaufanie klientów co do niezawodności systemów, którym powierzyli swoje dane. W tym kontekście daleko idące zmiany regulacyjne zapewniają narzędzia wdrażania solidnych systemów zarządzania bezpieczeństwem danych, które i sprawnie, i skutecznie obchodzą się z wrażliwymi informacjami.

Tłum. P. M.

Źródło: <https://ieccetech.org/issue/2018-02/International-Standards-provide-toolkit-for-GDPR-compliance>

# Bezpieczeństwo pożarowe obiektów

## Prace PKN/KT 180

Dzięki pracom podjętym w KT 180 z inicjatywy Komendy Głównej Państwowej Straży Pożarnej w kwietniu 2017 r. została opublikowana długo oczekiwana znowelizowana wersja normy [PN-B-02857:2017-04 Ochrona przeciwpożarowa budynków - Przeciwpożarowe zbiorniki wodne - Wymagania ogólne](#).

Na nowo określono w niej wymagania ogólne dla przeciwpożarowych zbiorników wodnych przeznaczonych do magazynowania wody do celów zewnętrznego gaszenia pożaru. Norma obejmuje naziemne, półpodziemne, podziemne, kryte i otwarte przeciwpożarowe zbiorniki wodne. Przesłanką do jej opracowania była potrzeba ujednoczenia wymagań dla przeciwpożarowych zbiorników wodnych, szczególnie na potrzeby Państwowej Straży Pożarnej, a jej wdrożenie miało na celu dostosowanie wymogów w niej zawartych do obecnych rozwiązań.

KT 180 w 2017 r. roku prowadził również prace nad kilkoma projektami norm. 31 sierpnia 2017 r. została opublikowana norma [PN-EN 1364-1:2015-08 Badania odporności ogniowej elementów nienośnych - Część 1: Ściany](#) zastępująca normę z 2001 roku, przedstawiająca metodę ustalania odporności ogniowej ścian nienośnych wewnętrznych oraz zewnętrznych. Norma jest przeznaczona do stosowania łącznie z PN-EN 1363-1:2012 i odnosi się zarówno do elementów przeszklonych, jak i ścian nienośnych zawierających przeszklenia.



Opublikowano również kolejne części normy 13501, w których zaktualizowano i ujednolicono terminologię, tak aby dokument był bardziej przejrzysty dla odbiorców:

- **PN-EN 13501-4:2016-07 Klasyfikacja ogniowa wyrobów budowlanych i elementów budynków - Część 4: Klasyfikacja na podstawie wyników badań odporności ogniowej elementów systemów kontroli rozprzestrzeniania dymu** - określająca procedurę klasyfikacji elementów systemów kontroli rozprzestrzeniania w oparciu o badania odporności ogniowej oraz klasyfikacji na podstawie rozszerzonego zastosowania wyników badań. Norma dotyczy przewodów wentylacyjnych, klap odcinających, kurtyn dymowych oraz mechanicznych urządzeń wentylacyjnych do systemów kontroli rozprzestrzeniania dymu, elementów przyłączeniowych oraz grawitacyjnych urządzeń wentylacyjnych do odprowadzania dymu i ciepła.
- **PN-EN 13501-5:2016-07 Klasyfikacja ogniowa wyrobów budowlanych i elementów budynków - Część 5: Klasyfikacja na podstawie wyników badań oddziaływania ognia zewnętrznego na dach** - zawierająca procedury klasyfikacji ogniowej zarówno dachów, jak i pokryć dachowych poddawanych oddziaływaniu ognia zewnętrznego, w zakresie ich właściwości użytkowych, na podstawie czterech metod badań podanych w CEN/TS 1187:2012 i właściwych reguł rozszerzonego zastosowania.
- **PN-EN 13501-6:2014-04 Klasyfikacja ogniowa wyrobów budowlanych i elementów budynków - Część 6: Klasyfikacja na podstawie wyników badań reakcji na ogień kabli elektrycznych** - przedstawiająca procedurę klasyfikacji ogniowej w zakresie reakcji na ogień kabli elektrycznych, za które należy rozumieć wszystkie kable zasilające, sterujące i komunikacyjne, łącznie z kablami światłowodowymi.

- **PN-EN 13501-2:2016-07 Klasyfikacja ogniowa wyrobów budowlanych i elementów budynków - Część 2: Klasyfikacja na podstawie wyników badań odporności ogniowej, z wyłączeniem instalacji wentylacyjnej** - opisująca procedurę klasyfikacji wyrobów budowlanych i elementów budynku na podstawie wyników badań odporności ogniowej i dymoszczelności. Norma obejmuje również klasyfikację na podstawie rozszerzonego zastosowania wyników badań. Ma zastosowanie do elementów nośnych, wyrobów i systemów do zabezpieczeń elementów lub części obiektów, elementów nienośnych lub nienośnych części obiektów oraz do okładzin ściennych i sufitowych.

Wszystkie wyżej wymienione normy są dostępne w sklepie PKN.

*Katarzyna Maciejczyk*

A photograph of a railway station at night. The scene is illuminated by warm yellow lights from street lamps and station buildings, contrasting with the cool blue tones of the twilight sky. In the foreground, a tall metal pole supports overhead power lines and two signal lights, both of which have their red lights lit. The tracks lead into the distance, where more tracks and station structures are visible. The overall atmosphere is quiet and industrial.

# Ochrona sieci kolejowych przed cyberatakami

Morand Fachot

Sieci kolejowe, będące integralną częścią infrastruktury krytycznej, nadal są narażone na cyberataki

W ostatnich latach systemy kolei i metra stały się przedmiotem serii cyberataków. Mimo że dotychczas nie zgłoszono żadnych poważnych awarii czy wypadków, prawdopodobnie problem ten będzie narastał i znacznie wpłynie na bezpieczeństwo. W miarę przechodzenia systemów sygnalizacji i sterowania pociągami z systemów zasadniczo zamkniętych na otwarte, oparte na technologiach komunikacji mobilnej i IP (protokół internetowy), bezpieczeństwo cybernetyczne staje się coraz ważniejsze. Normy Międzynarodowe IEC odegrają w tym sektorze bardzo ważną rolę.

### Zmiana technologiczna i kulturowa

Systemy kolejowe stanowią integralną część systemu transportowego i są postrzegane jako część infrastruktury krytycznej w wielu krajach. Cyberzagrożenia sieci kolejowych nabierają coraz większego znaczenia, ponieważ wzrasta poziom cyfryzacji systemów sterowania ruchem kolejowym.

Systemy sterowania sygnalizacją i pociągami przez długi czas opierały się na różnego typu przełącznikach. Zasadniczo, są to zamknięte zastrzeżone systemy, chronione przez tzw. luki powietrzne.

Tradycyjne systemy chronione lukami powietrznymi nie są odporne na ataki. W 2008 r. czternastolatek z Polski użył zmodyfikowanego pilota do telewizora, aby ingerować w torowisko tramwajowe w Łodzi. Cztery pojazdy wykoleiły się, a 12 osób zostało rannych.

Sektor kolejowy wprowadza obecnie systemy otwarte oparte na technologiach, takich jak usługi GPRS (General Packet Radio Service) i LTE dla komunikacji mobilnej oraz IP. Systemy te, będąc otwarte, stanowią przesunięcie technologiczne, a także kulturowe.

Jednak systemy komputerowe wprowadziły dodatkowy wymiar cyberzagrożeń. Oznacza to, że cyberbezpieczeństwo staje się sprawą bardzo istotną i musi być uwzględniane od samego początku.

W listopadzie 2016 r. Miejski Urząd Transportu w San Francisco (San Francisco Municipal Transportation Authority - SFMTA) był celem ataku *ransomware*. Jego systemy informacyjne zostały zaszyfrowane, a operator musiał odłączyć bramki biletowe i automaty biletowe, co spowodowało straty finansowe.

W maju 2017 r. niemiecki operator kolejowy Deutsche Bahn został zaatakowany *ransomware* – WannaCry. W wyniku tego ataku na niektórych stacjach wyłączono tablice elektroniczne, jednak usługi przewozowe nie zostały zakłócone.

Rosnąca świadomość cyberzagrożeń dla sektora kolejowego została podkreślona na wielu międzynarodowych konferencjach. Specjalna sesja na temat cyberbezpieczeństwa w kolejach w ramach Intelligent Rail Summit 2017, zorganizowana w Wiedniu w listopadzie 2017 r. przez RailTech (globalną platformę dla specjalistów z branży kolejowej), obejmowała wiele aspektów. Mówiono o zagadnieniach ze sfery cyberzagrożeń oraz środkach mających na celu ich rozwiązanie, w tym wykorzystanie norm IEC.

### Wielu potencjalnych atakujących

Głównym zagrożeniem dla systemów kolejowych (i innych systemów transportowych) nie są tzw. skryptowe dzieciaki (*script-kiddies*) – jak wspomniany już polski nastolatek, który włamał się do łódzkiego systemu tramwajowego – ale cztery różne grupy sprawców podzielonych na dwie kategorie:

1. Przestępcy, którzy próbują wyłudzić pieniądze, przy czym głównym narzędziem jest oprogramowanie *ransomware*. Stało się to modelem biznesowym, w którym opracowywane są różne typy złośliwego oprogramowania, które można sprzedawać lub wypożyczać.
2. Inne osoby zdecydowane by przerwać lub zakłócić działalność (w tym fizyczną). Ta grupa obejmuje:
  - niezadowolonych lub zwolnionych pracowników mających dostęp (w tym fizyczny) do systemów komputerowych;
  - terrorystów i grupy umotywowane politycznie;
  - podmioty państwowe.

Ataki fizyczne nie powinny być pomijane. We wrześniu 2016 r. centrum kontroli ruchu lotniczego w Chicago zostało zamknięte przez ogromny pożar zaprószonego przez niezadowolonego wykonawcę. Tysiące lotów na terenie USA zostało zakłóconych. Ataki mogą także przybrać postać hybrydową, łączącą ataki fizyczne i cybernetyczne.

Zapobieganie atakom fizycznym, będącym zazwyczaj wynikiem nieautoryzowanego dostępu, jest możliwe dzięki zastosowaniu Norm Międzynarodowych opracowanych przez IEC/TC 79: *Alarm and electronic security systems* oraz ISO/IEC JTC 1/SC 17: *Cards and personal identification*.

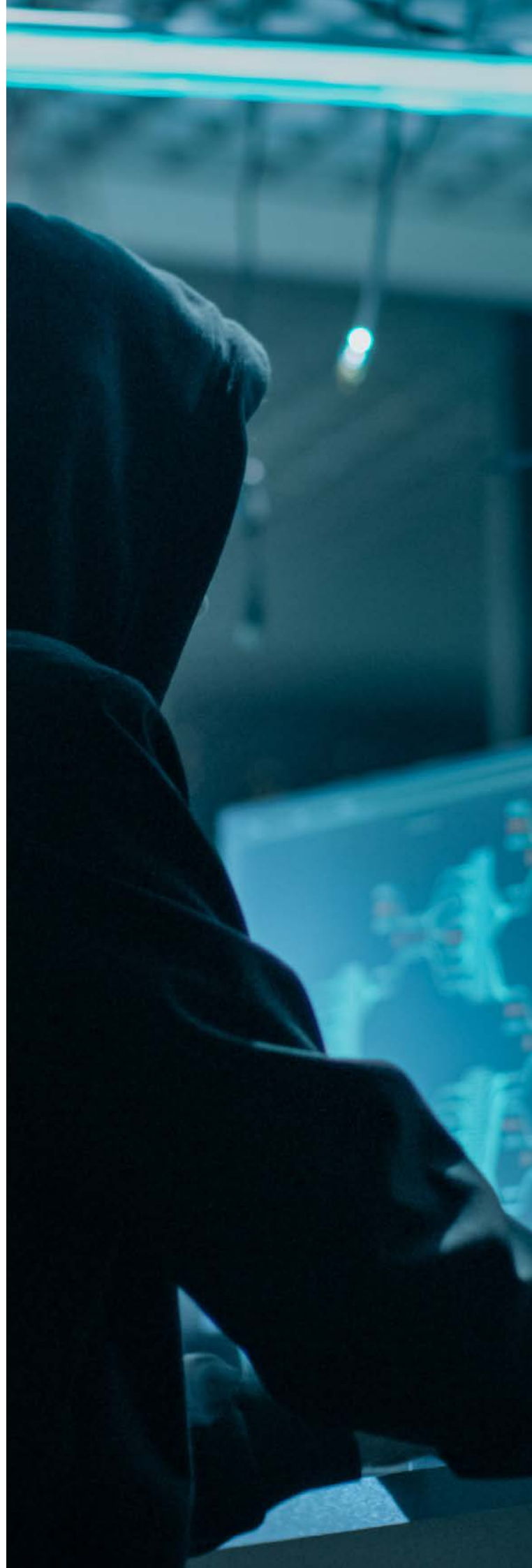
Obudowy zawierające sprzęt elektroniczny i kontrolny zainstalowane w odległych miejscach wzdłuż torów, wykazują podatność na ataki fizyczne i cybernetyczne.

### Ochrona infrastruktury kolejowej przed cyberatakami

Cyfryzacja sektora kolejowego i przejście od technologii elektromechanicznej do cyfrowej technologii IP są wspierane przez Unię Europejską poprzez Europejski System Zarządzania Ruchem Kolejowym (European Rail Traffic Management System - ERTMS).

ERTMS to system norm obejmujących zarządzanie i współdziałanie sygnalizacji dla kolei, który przyjął się w Europie i poza nią: w kilku krajach afrykańskich, w Brazylii, Meksyku, wielu krajach Bliskiego Wschodu i Azji, w tym w Chinach i Indiach, a także w Australii.

Przemysłowe automatyczne systemy sterowania (*industrial automated control systems* - IACS) nie są już odizolowane od zewnątrz, a systemy kolejowe są w coraz większym stopniu wzajemnie połączone dzięki automatycznej obsłudze pociągu (*automatic train operation* - ATO) i jako część inteligentnych systemów transportowych, jak powiedział podczas konferencji François Hausman, kierownik ds. ochrony cybernetycznej głównej linii Alstom i lider WP ds. cyberbezpieczeństwa w Shift2Rail.



Powiedział też, że cyberataki na przemysłowe systemy kontroli wzrosły o ponad 600% w latach 2012-2014, przynosząc poważne obawy w zakresie finansów i bezpieczeństwa.

Specyfika kolei, np. elementy elektroniczne rozproszone wzdłuż torów lub pociągów, bardzo długi cykl życia (przekraczający 25 lat), różnorodność łańcucha dostaw i technologii oraz inne cechy sprawiają, że jest to złożona dziedzina.

### Zautomatyzowane, bezprzewodowe sygnały bardziej efektywne, ale podatne na nowe zagrożenia

„Branża motoryzacyjna znalazła się w poważnej potrzebie ochrony cybernetycznej. Najwyższy czas, aby branża kolejowa również weszła na pokład” – mówi Amir Levintal, dyrektor generalny izraelskiej firmy Cylus specjalizującej się w bezpieczeństwie na kolei. „Obecne podejście do cyberbezpieczeństwa nie pasuje do dzisiejszej architektury sieci kolejowych”, powiedział Levintal przedstawicielowi Global Railway Review.

Levintal uważa, że nowe systemy sygnalizacyjne są szczególnie podatne na ataki hakerów. Te systemy „są kluczowe dla bezpieczeństwa ruchu kolejowego. W ciągu ostatnich kilku lat stały się one również bardziej zautomatyzowane – a teraz są obsługiwane bezprzewodowo” – wyjaśnia.

„W najgorszym przypadku hakerzy mogliby wysłać do pociągu komendy, aby pojazd zwolnił, zatrzymał się lub przyspieszał na zakrętach tak, że pociąg mógłby nie utrzymać się na torach. Wszystkie te scenariusze prowadzą do katastrofy” – ostrzega Levintal.



## Normy IEC obejmujące IACS kluczowe dla sieci kolejowych

Shift2Rail, inicjatywa, która skupia kluczowe europejskie podmioty kolejowe w celu stworzenia jednolitego europejskiego obszaru kolejowego, analizuje, w jaki sposób różne aspekty cyberbezpieczeństwa powinny być stosowane w sektorze kolejowym. Oceniono aktualne normy i wybrano serię IEC 62443, ponieważ:

- jest przeznaczona dla IACS;
- obejmuje cykl życia produktów i systemów;
- obejmuje procesy oceny ryzyka bezpieczeństwa;
- definiuje poziomy bezpieczeństwa na podstawie wymagań bezpieczeństwa funkcjonalnego;
- jest wykorzystywana w innych infrastrukturach krytycznych.

Wybór IEC 62443 został również podkreślony przez inżyniera ds. Cyberbezpieczeństwa ERTMS Sharvind Appiaha podczas warsztatów organizowanych przez Railway Gazette. „Nie ma powodu, aby opracowywać nowe normy dla kolei. Istnieje już wiele norm dot. cyberbezpieczeństwa, bez

względu na to, czy są to normy NIST (Amerykański Narodowy Instytut Standardów i Technologii), czy normy ISO/IEC (...). Wyzwaniem jest sprawdzenie, które z nich pasują do kontekstu kolejowego – to właśnie robimy w Shift2Rail, patrzymy na normy branżowe, co oznacza, że IEC 62443 to kompletny zestaw norm opracowanych dla IACS, ale stosujemy je w kontekście kolei”.

„Uważam, że to sprytny sposób na wypełnienie luki. Unika się przejścia przez fazę badań i rozwoju (R&D), gdzie musielibyśmy przepisać normy. Mamy już normy; to kwestia ich zastosowania i nauczenia się, jak je wykorzystywać”.

Fakt, że IEC 62443 pojawia się jako podstawowy zestaw norm dla sektora kolejowego, został podkreślony przez innych prelegentów na konferencji w Wiedniu, w szczególności przez Davida Rogersa z firmy Siemens w jego prezentacji: „IEC 62443: Norma cyberbezpieczeństwa zbliżająca się do Kolejowego Internetu Rzeczy”.

„Zestaw norm obejmuje trzech głównych interesariuszy w ochronie zakładów przed cyberatakami: właścicieli aktywów, integratorów systemów i dostawców produktów”, uważa Rogers. Kluczową koncepcją normy IEC 62443 jest to, że bezpieczeństwo wymaga przyjęcia zestawu skoordynowanych działań, podejścia ogólnie opisanego jako *defence-in-depth* (dosł. obrona w głębi).

Fakt, że norma IEC 62443 jest szeroko stosowana, ilustruje niemiecka norma DIN VDE V 0831-104; VDE V 0831-104:2015-10: *Electric signalling systems for railways – Part 104: IT Security Guideline* oparta na zapisach normy IEC 62443 (62443-3-3:2013).

### Wszystkie kraje wprowadzają środki cyberbezpieczeństwa w sektorze kolejowym

Brytyjski Departament Transportu wydał dokument z wytycznymi, który ma pomóc przemysłowi kolejowemu w zmniejszeniu jego podatności na cyberataki. Dokument ten określa zasady i ogólne podejście do cyberbezpieczeństwa jako dobrą praktykę, nie zawiera jednak szczegółowych instrukcji.

Normy wymienione w niedawno opublikowanych wynikach konsultacji publicznych opracowanych przez Australian Standard Rail Industry Safety and Standards Board (RISSB) obejmują, oprócz serii IEC 62443, grupę ISO/IEC 27000 dot. bezpieczeństwa IT, a także Raport Techniczny ISO/IEC (TR) 15443-1:2012 i ISO/IEC TR 15443-2:2012, *Information technology – Security techniques – Security assurance framework*.

W Stanach Zjednoczonych firma NIST opublikowała dokument dotyczący oceny działania bezpiecznego projektu systemu sterowania przemysłowego dla systemu sterowania kolejowego.

Ponieważ systemy kolejowe będą coraz częściej opierać się na komunikacji mobilnej, urządzeniach połączonych i sieciach IP, częstotliwość cyberataków ze strony różnych podmiotów prawdopodobnie wzrośnie.

Normy Międzynarodowe, w szczególności normy IEC, takie jak IEC 62443, zapewnią kompleksowe podejście do bezpieczeństwa technologii informacyjnej (IT) i technologii operacyjnej (OT) oraz będą kluczowe dla ochrony IACS przed cyberzagrożeniami.

Oprac. I.P.

Źródło: IEC e-tech magazine, Issue 2/2018

Wieloczęściowa norma IEC 62443 zostanie wdrożona do zbioru PN jako PN-EN 62443 Bezpieczeństwo w systemach sterowania i automatyki przemysłowej dzięki pracy KT 50 ds. Automatyki i Robotyki Przemysłowej.

# Gazownictwo

PKN/KT 277

W 2018 r. zostały opublikowane polskie wersje językowe pięciu Norm Europejskich z zakresu gazownictwa, w ramach prac na zamówienie. Cztery Normy Europejskie zostały opracowane na podstawie mandatów udzielonych CEN przez Komisję Europejską i Europejskie Stowarzyszenie Wolnego Handlu.





### Podkomitet 3 ds. Przesyłu Paliw Gazowych

W styczniu 2018 r. została opublikowana polska wersja językowa [PN-EN 12480:2015-07](#) *Gazomierze – Gazomierze rotorowe*.

Norma EN 12480:2015 została opracowana na podstawie mandatów udzielonych CEN przez Komisję Europejską i Europejskie Stowarzyszenie Wolnego Handlu:

- M/071 *Mandate to CEN for standardization in the field of Pressure equipment,*
- M/374 *Mandate to CEN and CENELEC for standards in the field of measuring instruments,*
- M/541 [C(2015)8558] *Standardization request in support of the implementation of Directive 2014/32/EU on measuring instruments.*

Norma ta jest związana z dyrektywami: 2014/32/UE Przyrządy pomiarowe oraz 97/23/WE Urządzenia ciśnieniowe (PED).

Określono w niej zakresy, budowę, wymagania, charakterystyki wyjściowe i badania gazomierzy rotorowych (zwanymi gazomierzami RD lub po prostu gazomierzami) do pomiaru objętości gazu.

Ma zastosowanie do gazomierzy rotorowych stosowanych do pomiaru objętości paliw gazowych przynajmniej 1., 2., i 3., rodziny gazowej, których skład podano w EN 437:2003+A1:2009, przy maksymalnym ciśnieniu pracy mniejszym lub równym 20 barów powyżej ciśnienia otoczenia i zakresie temperatur gazu przynajmniej od -10°C do +40°C.

Norma ma zastosowanie do gazomierzy, które są instalowane w miejscach z wibracjami i wstrząsami o niewielkim natężeniu oraz w:

- zamkniętych lokalizacjach (wewnątrz lub na zewnątrz przy zastosowaniu ochrony określonej przez wytwórcę), z kondensacją lub bez kondensacji wilgoci lub, jeżeli określone jest to przez wytwórcę,
- otwartych lokalizacjach (na zewnątrz, bez jakiegokolwiek osłony), z kondensacją lub bez kondensacji wilgoci.

Norma ma również zastosowanie do gazomierzy o iloczynie najwyższego dopuszczalnego ciśnienia PS i objętości V mniejszym od 6 000 bar · litr lub iloczynie PS i DN mniejszym od 3 000 barów.

W marcu 2018 r. została opublikowana polska wersja językowa [PN-EN 1776:2016-04 Infrastruktura gazowa – Układy pomiaru gazu – Wymagania funkcjonalne](#).

Norma EN 1776:2015 została opracowana na podstawie mandatu M/017 *Standardization mandate to CEN in the field of equipment and installation for the transmission and distribution of gas*, udzielonego CEN przez Komisję Europejską i Europejskie Stowarzyszenie Wolnego Handlu.

Norma ta częściowo została opracowana jako odpowiedź na prace europejskich organizacji normalizacyjnych (CEN/CENELEC/ETSI) na podstawie mandatu Komisji M/441. Zaleca się, aby niniejsza norma była stosowana w powiązaniu z CEN/CLC/ETSI TR 50572, *Functional Reference Architecture for Communications in Smart Metering Systems* oraz EN 16314 *Gas meters – Additional functionalities* (gdzie gazomierz często określany jest jako gazomierz inteligentny).

Dyrektywa 2009/73/WE dotycząca wspólnych zasad dla wewnętrznego rynku gazu ziemnego i powiązana z Rozporządzeniem (WE) Nr 715/2009 w sprawie warunków dostępu do sieci przesyłowych gazu ziemnego ma także na celu bezpieczeństwo techniczne łącznie z niezawodnością techniczną europejskiego systemu gazowego. Względy te mieszczą się także w zakresie normalizacji CEN/TC 234 *Gas infrastructure*. CEN/TC 234 ocenił pod tym względem prawodawstwo UE i odpowiednio zmodyfikował niniejszą normę.

Norma obejmuje aspekty środowiskowe odnoszące się do projektowania, budowy, działania i utrzymania, a także odbioru/unieruchomienia układów pomiaru gazu zgodnie z CEN Guide 4 i CEN/TR 16388.

W normie określono wymagania funkcjonalne dotyczące projektowania, budowy, badania, odbioru/unieruchomienia, działania, utrzymania i, gdzie jest to odpowiednie, wzorcowania łącznie z odpowiednimi udokumentowanymi postanowieniami dla wszystkich nowych układów pomiaru i wszelkich poważnych zmian układów istniejących.

Infrastruktura gazowa jest skomplikowana i ważność bezpieczeństwa jej budowy i użytkowania doprowadziła do opracowania w krajach członkowskich bardzo szczegółowych przepisów i instrukcji operatorskich. Te szczegółowe wymagania obejmują uznane normy inżynierii gazowniczej oraz specjalne przepisy nałożone przez struktury prawne krajów członkowskich.

## Podkomitet 2 ds. Dystrybucji Paliw Gazowych

W marcu 2018 r. została opublikowana polska wersja językowa normy [PN-EN 12007-3:2015-09 Infrastruktura gazowa – Rurociągi o maksymalnym ciśnieniu roboczym do 16 barów włącznie – Część 3: Szczegółowe wymagania funkcjonalne dla stali](#).

EN 12007-3:2015 została opracowana na podstawie mandatu M/017 *Standardization mandate to CEN in the field of equipment and installation for the transmission and distribution of gas*.

W normie opisano szczegółowe wymagania funkcjonalne dla rur stalowych w uzupełnieniu do ogólnych wymagań funkcjonalnych w EN 12007-1, dla maksymalnego ciśnienia roboczego do 16 barów włącznie. W normie określono wspólne podstawowe zasady dotyczące infrastruktury gazowej. Zaleca się, aby użytkownicy niniejszej normy mieli świadomość, że w państwach członkowskich CEN mogą występować bardziej szczegółowe normy krajowe i/lub kodeksy postępowania.

W kwietniu 2018 r. została opublikowana polska wersja językowa normy [PN-EN 331:2016-04 Kurki kulowe i kurki stożkowe z zamkniętym dnem uruchamiane ręcznie, przeznaczone dla instalacji gazowych budynków](#).

EN 331:2015 została opracowana na podstawie mandatu M/131 *Mandate to CEN/CENELEC concerning the execution of standardization work for harmonized standards on pipes, tanks and ancillaries, not in contact with water intended for human consumption*.

Jeżeli niniejsza Norma Europejska jest powołana w Dzienniku Urzędowym Unii Europejskiej (OJEU), rozdziały niniejszej normy, podane w Załączniku ZA do normy, spełniają postanowienia ww. mandatu, w ramach rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 305/2011 z dnia 9 marca 2011 r. ustanawiającego zharmonizowane warunki wprowadzania do obrotu wyrobów budowlanych i uchylającego dyrektywę Rady 89/106/EWG.

W niniejszej normie podano charakterystyki budowy, właściwości użytkowych i bezpieczeństwa kurków kulowych i kurków stożkowych z zamkniętym dnem. Uszczegółowiono także metody badań oraz postanowienia dotyczące oznakowania.

Norma ma zastosowanie do metalowych kurków niezakopanych bezpośrednio, przeznaczonych dla instalacji domowych i komunalnych, wewnątrz lub na zewnątrz budynków.

„Niezakopany bezpośrednio” w kontekście niniejszej normy oznacza, że kurki stosowane pod ziemią nie są w bezpośrednim kontakcie z ziemią lub innymi materiałami, np. że są one w osłonie ochronnej.

## **Podkomitet 1 ds. Pomiarów i Oceny Jakości Paliw Gazowych**

W styczniu 2018 r. została opublikowana polska wersja językowa normy [PN-EN ISO 6141:2015-07 Analiza gazu – Zawartość certyfikatów dla gazowych mieszanin wzorcowych](#).

W normie określono minimalne wymagania dotyczące zawartości certyfikatów dla jednorodnych mieszanin gazowych w butlach gazowych, do stosowania jako gazowe mieszaniny wzorcowe. Gazy czyste, gdy są stosowane jako gazowe mieszaniny wzorcowe, są również objęte postanowieniami niniejszej normy. Gazy i mieszaniny gazowe sporządzane w innych celach, nie są brane pod uwagę.

Wymagania określone w niniejszej normie dotyczą metrologicznych aspektów gazowych mieszanin wzorcowych. Inne aspekty, takie jak bezpieczeństwo i aspekty prawne, nie zostały uwzględnione.

Ponadto w normie zamieszczono dodatkowe informacje (dane opcjonalne) zalecane do opisanja jedno-

rodnej mieszaniny gazowej dostarczonej pod ciśnieniem w butli lub innym pojemniku. Nie uwzględniono obszaru danych dotyczących etykietowania butli związanego z bezpieczeństwem.

*Ryszard Rybaltowski  
Sektor Maszyn i Inżynierii*

# ORGANY TECHNICZNE

## kwiecień 2018

## Komitety Techniczne

### Nowi Przewodniczący Komitetów Technicznych

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

- w **KT 87 ds. Chowu i Hodowli Zwierząt** dra hab. **Jacka Walczaka** reprezentującego Instytut Zootechniki - Państwowy Instytut Badawczy
- w **KT 126 ds. Rur Stalowych** mgra inż. **Dariusza Chromika** reprezentującego TÜV SÜD Polska Sp. z o.o.
- w **KT 141 ds. Tworzyw Sztucznych** dr hab. inż. **Reginę Jeziorską** reprezentującą Instytut Chemii Przemysłowej im. prof. Ignacego Mościckiego
- w **KT 185 ds. Ochrony Drewna i Materiałów Drewnopochodnych** prof. nadzw. **IDT Andrzeja Fojutowskiego** reprezentującego Instytut Technologii Drewna
- w **KT 230 ds. Małych Statków** mgra inż. **Adama Dunikowskiego** reprezentującego Polski Rejestr Statków S.A.
- w **KT 246 ds. Ochrony Radiologicznej** dra **Pawła Krajewskiego** reprezentującego Centralne Laboratorium Ochrony Radiologicznej
- w **KT 256 ds. Terminologii, Innych Zasobów Językowych i Zarządzania Treścią** mgr **Monikę Popiołek** reprezentującą Polskie Stowarzyszenie Biur Tłumaczeń
- w **KT 285 ds. Górniczych Maszyn i Urządzeń Dołowych** dra inż. **Edwarda Pieczorę** reprezentującego Instytut Techniki Górniczej KOMAG
- w **KT 290 ds. Technik Specjalnych w Elektryce** prof. dra hab. **Jacka Sosnowskiego** reprezentującego Instytut Elektrotechniki
- w **KT 302 ds. Zastosowania Informatyki w Ochronie Zdrowia** mgra inż. **Edwarda Byczyńskiego** reprezentującego Stowarzyszenie HL7 Polska



## Nowi Zastępcy Przewodniczącego Komitetów Technicznych

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

- w **KT 285 ds. Górniczych Maszyn i Urządzeń Dołowych** mgr inż. **Romanę Zajęc** reprezentującą Instytut Techniki Górniczej KOMAG
- w **KT 290 ds. Technik Specjalnych w Elektryce** dra inż. **Wojciecha Sokólskiego** reprezentującego Specjalistyczne Przedsiębiorstwo Zabezpieczeń Przeciwkorozyjnych CORRPOL Sp. z o.o.

## Nowi Sekretarze Komitetów Technicznych

W kwietniu Prezes PKN powołał do pełnienia funkcji Sekretarza:

- w **KT 87 ds. Chowu i Hodowli Zwierząt** mgra **Krzysztofa Palecznego** reprezentującego Instytut Zootechniki - Państwowy Instytut Badawczy
- w **KT 108 ds. Kruszyw i Kamienia Budowlanego** mgra inż. **Roberta Mularzuka** reprezentującego Instytut Badawczy Materiałów Budowlanych Sp. z o.o.
- w **KT 128 ds. Projektowania i Wykonawstwa Konstrukcji Metalowych i Konstrukcji Zespoleonych** mgra inż. **Jerzego Kaweckiego** z Polskiego Komitetu Normalizacyjnego
- w **KT 213 ds. Projektowania i Wykonawstwa Konstrukcji z Betonu** mgra inż. **Jerzego Kaweckiego** z Polskiego Komitetu Normalizacyjnego
- w **KT 252 ds. Projektowania Konstrukcji Murowych** mgra inż. **Jerzego Kaweckiego** z Polskiego Komitetu Normalizacyjnego

## Nowi członkowie Komitetów Technicznych

W kwietniu Prezes PKN powołał na członków KT następujące podmioty:

- **4Kraft Sp. z o.o. do KT 237** ds. Artykułów dla Niemowląt i Małych Dzieci oraz Bezpieczeństwa Zabawek
- **AkustiX Sp. z o.o. do KT 253** ds. Akustyki Architektonicznej
- **Barlinek Inwestycje Sp. z o.o. do KT 100** ds. Wyrobów z Drewna i Materiałów Drewnopochodnych
- **Barlinek S.A. do KT 100** ds. Wyrobów z Drewna i Materiałów Drewnopochodnych
- **Centrum Badań i Dozoru Górnictwa Podziemnego Sp. z o.o. do KT 269** ds. Bezpieczeństwa Chemicznego
- **CryptoProtect Sp. z o.o. do KT 170** ds. Terminologii Informatycznej, Kodowania Informacji i Techniki Biurowej

- **Epson Europe B.V. Sp. z o.o. Oddział w Polsce do KT 60** ds. Energoelektroniki i Przyrządów Półprzewodnikowych
- **Fabrykę Sprzętu Ratunkowego i Lamp Górniczych FASER S.A. do KT 21** ds. Środków Ochrony Indywidualnej Pracowników
- **Grupę Lambda Sp. z o.o. Dystrybucja Sp.k. do KT 212** ds. Budowy i Utrzymania Dróg
- **ICR Polska Sp. z o.o. do KT 64** ds. Urządzeń Elektrycznych w Przestrzeniach Zagrożonych Wybuchem
- **Imperial Tobacco Polska S.A. do KT 321** ds. Elektronicznych Inhalatorów Nikotyny oraz Płynów do ich Uzupelniania
- **Lift Components Sp. z o.o. do KT 131** ds. Dźwigów, Schodów i Chodników Ruchomych
- **Pancerpol Galewski, Trzopek sp. j. do KT 316** ds. Ciepłownictwa i Ogrzewnictwa
- **Politechnikę Krakowską im. Tadeusza Kościuszki do KT 7** ds. Badań Nieniszczących
- **Politechnikę Rzeszowską im. Ignacego Łukasiewicza do KT 207** ds. Obróbki Ubytkowej i Przyrostowej oraz Charakterystyki Warstwy Wierzchniej
- **Politechnikę Warszawską do KT 104** ds. Kompatybilności Elektromagnetycznej
- **SGS Polska Sp. z o.o. do KT 100** ds. Wyrobów z Drewna i Materiałów Drewnopochodnych, do **KT 108** ds. Kruszyw i Kamienia Budowlanego i **KT 144** ds. Koksu i Przetworzonych Paliw Stałych

## Odwołania członków Komitetów Technicznych

W kwietniu Prezes PKN odwołał z członka KT:

- **ENEA Operator Sp. z o.o. z KT 53** ds. Kabli i Przewodów, **KT 70** ds. Przekazników Elektrycznych i Elektroenergetycznej Automatyki Zabezpieczeniowej, **KT 74** ds. Aparatury Rozdzielczej i Sterowniczej Wysokonapięciowej, **KT 77** ds. Aparatury Rozdzielczej i Sterowniczej Niskonapięciowej i **KT 304** ds. Aspektów Systemowych Dostawy Energii Elektrycznej
- **Zakład Aparatury Elektrycznej ERGOM Sp. z o.o. z KT 77** ds. Aparatury Rozdzielczej i Sterowniczej Niskonapięciowej
- **Zakład Elektroniki COMPAS inż. Jacek Szewczyk z KT 52** ds. Systemów Alarmowych Włamania i Napadu

## Komitety Zadaniowe

### Nowy Przewodniczący Komitetu Zadaniowego

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

- w KZ 505 ds. **Procesów Kryminalistycznych** Pana **Artura Dębskiego** reprezentującego Centralne Laboratorium Kryminalistyczne Policji

## Podkomitety Techniczne

### Nowy członek Podkomitetu Technicznego

- **Dowództwo Generalne Rodzajów Sił Zbrojnych**  
- Inspektorat Sił Powietrznych do KT 176/PK 6 ds. Uzbrojenia i Sprzętu Lotnictwa Wojskowego

**OFERUJEMY:**

**Szkolenia tradycyjne**

- Urządzenia techniczne. Dyrektywy i normy
- Certyfikacja personelu badań nieniszczących
- Ochrona danych osobowych - RODO
- Przygotowanie miast do procesu certyfikacji
- ISO 9001:2015 - zmiany
- Podstawy normalizacji, Polskie Normy
- System Zarządzania Bezpieczeństwem Informacji
- Przegląd norm w obszarze Smart Cities
- Przetwórstwo materiałów biodegradowalnych

**Szkolenia e-learningowe**

- Podstawy prac normalizacyjnych
- ISO 9001:2015
- Bezpieczny plac zabaw
- Wprowadzanie do obrotu wyrobów budowlanych
- Ocena zgodności i certyfikacja

**PKN**  
POLSKI KOMITET  
NORMALIZACYJNY

Więcej szczegółów pod adresem [wiedza.pkn.pl](http://wiedza.pkn.pl)