wiadomości PKN

• NORMALIZACJA •

6/2017

WYDAWCA

POLSKI KOMITET NORMALIZACYJNY

www.pkn.pl

wiadomości PKN
NORMALIZACJA
6/2017

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

ZESPÓŁ REDAKCYJNY
Redaktor prowadzący:
Joanna Skalska - tel. 22 556 74 62

Marta Hejduk - tel. 22 556 77 09

Skład:
Oskar Sztajer – tel. 22 556 77 62

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

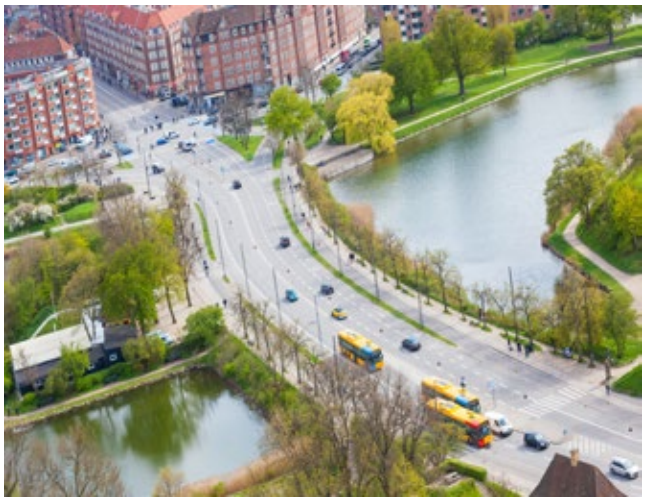
WYDAWCA:
Polski Komitet Normalizacyjny
ul. Świętokrzyska 14
00-050 Warszawa

Szanowni Czytelnicy

Wycieraczki, które same się włączają, bo „wiedzą" kiedy pada, lusterka wsteczne, które same się przyciemniają, alarmy informujące o tym, że nie zapięliśmy pasów bezpieczeństwa... Codzienność, prawda? Ale technologia idzie dalej. Samochody zaczęły aktywnie „łączyć się" z internetem. Z pomocą mobilnych aplikacji można teraz uzyskać współrzędne lokalizacji pojazdu czy dane dotyczące jego trasy, a także otworzyć drzwi, uruchomić silnik oraz sterować dodatkowym wyposażeniem wewnątrz niego. Czy zdajemy sobie sprawę z tego, że połączenie samochodu z internetem to coś więcej niż asystent parkowania? To dostęp do informacji zapisanych w portalach społecznościowych, poczcie e-mail, smartfonie (jeżeli jest połączony z samochodem), danych z nawigacji, aplikacji działających w ramach systemu operacyjnego samochodu itp. Technologie te oferują kierowcom wiele udogodnień, jednak stawiają także nowe wyzwania w kwestii bezpieczeństwa. Cyberprzestępcy mogą wykraść dane, zlokalizować samochód, przejąć nad nim kontrolę. To nowe zagrożenia, którym trzeba stawić czoła.

O cyberatakach, biometrii, samochodach połączonych, a także o aktualnościach w pracach normalizacyjnych można przeczytać w bieżącym numerze miesięcznika.

Joanna Skalska



SMART CITY – zagrożenia i perspektywy

28 marca 2017 roku w Warszawie odbyła się X edycja Ogólnopolskiego Kongresu „SMART CITY – założenia i perspektywy". Uczestniczyli w nim włodarze polskich miast, liczni przedstawiciele urzędów marszałkowskich, administracji lokalnej i biznesu. Jako przykłady dobrych praktyk w zakresie inteligentnych miast podano przede wszystkim Opalenicę (inteligentne zarządzanie energią), Płock (Integrująca Platforma Geoinformacyjna systemów miejskich) i Słupsk (integracja komunikacji publicznej z innymi gminami).

Zwrócono szczególną uwagę na rolę mieszkańców – liderów zmian – w procesie rozwoju miasta i jego przestrzeni. Zdaniem Daniela Larssona, Radcy Ambasady Szwecji w Warszawie, miasto powinno uławiać mieszkańcom podjęcie właściwych społecznie decyzji, np. poprzez umożliwienie dostępu do systemu Veturilo (Warszawski Rower Publiczny) czy szerokopasmowego Internetu. Wspomniano o kosztownej i zarazem perspektywicznej idei stworzenia możliwości wypożyczania niewielkich samochodów elektrycznych na terenie miast.

W czasie konferencji podkreślono rolę normy PN-ISO 37120 Zrównoważony rozwój społeczny – Wskaźniki usług miejskich i jakości życia w proc sie zarządzania miastem. Norma zawiera listę 100 wskaźników – z czego 46 to wskaźniki podstawowe, a 54 dodatkowe – przyporządkowanych do 17 grup tematycznych. Jest to pierwszy tego typu ustalony zestaw wskaźników, służący do raportowania stanu rozwoju miasta i planowania zrównoważonego rozwoju. Ponadto podczas konferencji poruszono tematykę WCCD (World Council on City Data), oBEMS (Office Building Energy Management System) oraz tworzenia infrastruktury internetowej na podstawie 230V, tzw. Eternet.

Przeprowadzone sesje oraz panele dyskusyjne zaowocowały wieloma nowymi pomysłami oraz perspektywami dla rozwoju polskich miast.

W najbliższym czasie - 29 czerwca 2017 r. we Wrocławiu odbędzie się XII edycja Ogólnopolskiego Kongresu „SMART CITY – założenia i perspektywy". Podczas Kongresu poruszona zostanie tematyka możliwości rozwoju polskich miast i regionów oraz nowych technologii jako istotnego elementu dynamicznego rozwoju jednostek miejskich. Ponadto przeprowadzone zostaną dwa panele dyskusyjne dotyczące efektywnego wytwarzania i wykorzystywania energii w aglomeracjach miejskich oraz zarządzania zasobami miejskimi, przede wszystkim poprzez inteligentną infrastrukturę miast oraz ekologiczny i zrównoważony transport.

Katarzyna Rabęda
Joanna Mandziuk

Bitwa o połączone samochody

Producenci samochodów i operatorzy telekomunikacyjni nie są zgodni co do przyszłości samochodów połączonych

Catherine Bischofberger

Giganci motoryzacji i specjaliści od telekomunikacji muszą pracować razem, jeżeli chcą utorować drogę samochodom połączonym. Jednak obie strony mają inny pogląd na to, jak ta współpraca powinna wyglądać. Jednym z punktów spornych jest cyberbezpieczeństwo.

Przemysły motoryzacyjny i telekomunikacyjny charakteryzują się odmiennymi kulturami pracy. Producenci samochodów zrewolucjonizowali XX w ., natomiast przemysł telekomunikacyjny zapoczątkował wiek Internetu. Jedną z głównych różnic jest pojęcie „odpowiedniego" czasu. Produkty telekomunikacyjne są unowocześniane co miesiąc, w przemyśle motoryzacyjnym potrzeba kilku lat na stworzenie nowego modelu samochodu. Nie jest więc zaskoczeniem, że „samochodziarze" podejrzliwie przyglądają się „nowicjuszom" z telekomunikacji, zwłaszcza, że branża motoryzacyjna jest ściśle związana z pojęciem bezpieczeństwa. Rozbij swój telefon - stracisz zapisane w nim kontakty; rozbij swój samochód – zaryzykujesz swoje życie. Stawki nie są takie same, a przedsiębiorstwa z branży motoryzacyjnej nie są całkowicie przekonane, że operatorzy telekomunikacyjni w pełni zrozumieli tę kwestię.

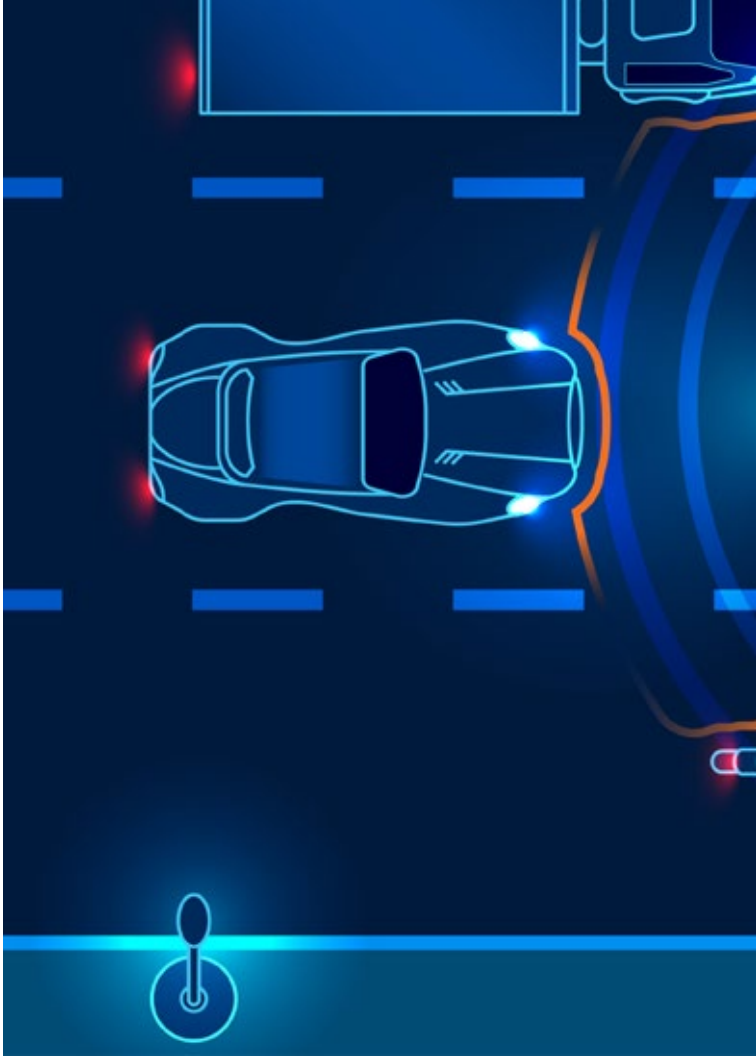
Próby, próby...

Kilka europejskich inicjatyw zmusza ich do podjęcia współpracy, szczególnie, że wszystko wskazuje na to, iż przyszłością motoryzacji jest automatyzacja i autonomiczność. Jedną z inicjatyw jest brytyjski projekt CITE (Connected Intelligent Transport Environment), który zebrał wielu producentów samochodów i operatorów telekomunikacyjnych razem z Radą Miasta Coventry, władzami Coventry University i przedstawicielami firmy Highways England. Projekt ma na celu stworzenie zaawansowanego środowiska do testowania pojazdów połączonych i autonomicznych. Obejmuje również wyposażenie dróg miejskich i autostrad (odcinki o długości do 40 mil) w cztery różne „mówiące technologie samochodowe". Jednym z celów projektu jest sprawdzenie, jak, dzięki lepszej łączności, technologie pomagają zmniejszyć korki drogowe, zapewniając jednocześnie inne standardowe usługi w zakresie rozrywki i bezpieczeństwa.

Podobny projekt uruchomiono we Francji. Projekt pilotażowy pod nazwą Scoop@F obejmuje 3000 pojazdów poruszających się po 2000 km dróg w różnych rejonach Francji: Ile-de-France i Korytarzem Wschodnim (East Corridor) biegnącym z Paryża do Strasburga, a także w Bretanii, Bordeaux i Isère. Druga część programu Scoop@F jest poświęcona w szczególności testom transgranicznym przeprowadzanym z innymi państwami członkowskimi UE (Hiszpania, Portugalia i Austria). Jego celem jest opracowanie hybrydowego rozwiązania komunikacyjnego działającego w sieciach 3G, 4G i ITS G5.

Główną ideą przyświecającą testom jest stymulacja współpracy pomiędzy producentami samochodów, operatorami telekomunikacyjnymi oraz zarządcami dróg, a ponadto wymiana doświadczeń, innowacyjnych rozwiązań i najlepszych praktyk. Program Scoop@F ma na celu sprawdzenie wspieranej przez UE platformy C-ITS (Cooperative Intelligent Transport Systems) uruchomionej w lipcu 2014 r. Platforma ta ma za zadanie budować interoperacyjność pewnej liczby usług na szczeblu europejskim. Mowa tu m.in. o powiadomieniach o miejscach niebezpiecznych, informacjach dotyczących stacji ładowania/tankowania pojazdów wykorzystujących paliwa alternatywne itd.

Podczas wspólnej konferencji ITU-UNECE dotyczącej przyszłości samochodów połączonych, zorganizowanej podczas tegorocznego Geneva Motor Show,



szef Connected Car w Orange Business Services Car Julien Masson wyjaśniał: „Komunikacja pomiędzy pojazdami jest jednym ze sposobów pomagania pojazdom autonomicznym w zmianie pasa ruchu na autostradzie, co dla technologii samojezdnej stanowi nadal spory problem. Kwestie skalowalności, podobnie jak problemy z interoperacyjnością, muszą zostać rozwiązane jak tylko przekroczymy granice".

Trzecie przedsięwzięcie nosi nazwę Nordic Way. Jest to projekt pilotażowy, który ma umożliwić pojazdom przekazywanie zabezpieczonych informacji o zagrożeniach bezpieczeństwa przez sieci komórkowe na korytarzu drogowym biegnącym przez Finlandię, Norwegię, Szwecję i Danię. Podobnie jak Scoop@f jest połączony z platformą C-ITS. W ten projekt jest bardzo zaangażowana Fińska Agencja Transportowa (Finnish Transport Agency), podobnie jak wiele firm telekomunikacyjnych i samochodowych.

Dwa konkurujące poglądy

W ramach samej platformy C-ITS producenci samochodów i operatorzy telekomunikacyjni prezentują różne opinie na temat wdrażania nowych systemów. Reprezentanci branży motoryzacyjnej mają tendencje do wspierania rozszerzonych rozwiązań dla pojazdów,

na przykład zewnętrzne dodatki do oprogramowania i sprzętu, opracowane i zarządzane przez samych producentów samochodów. Interfejsy są zaprojektowane w taki sposób, aby nie zagrażać bezpieczeństwu oraz chronić prywatność danych.

Operatorzy telekomunikacyjni opowiadają się za wbudowaną platformą aplikacyjną i rozwiązaniem serwerowym, które umożliwią wykorzystanie większej liczby danych, a tym samym zwiększą innowacyjność. Producenci samochodów twierdzą, że takie podejście jest podatne na włamania i może zagrozić bezpieczeństwu kierowców.

Pomimo dużych rozbieżności między stronami, ich przedstawiciele zgodzili się, że istnieje konieczność opracowania brakujących norm dotyczących zaawansowanych interfejsów fizycznych/ elektrycznych i logicznych, które obejmą minimalny poziom bezpieczeństwa, w tym minimalne zestawy danych i ujednolicone protokoły danych uaktywniające usługi IT.

IEC na pierwszym planie walki z cyberatakami

Kwestia bezpieczeństwa związanego z cyberatakami i włamaniami od dawna pozostaje w sferze zainteresowań IEC na różnych płaszczyznach. Można przywołać tu np. normę IEC 62645: 2014 dotyczącą bezpieczeństwa elektrowni jądrowych, opracowaną specjalnie w celu zapobiegania cyberatakom, wykrywania ich i reagowania na nie.

Powstające zagrożenia związane z cyberbezpieczeństwem napotykane przez połączone i autonomiczne pojazdy są rozpatrywane wspólnie przez IEC i ISO, przez różne podkomitety Wspólnego Komitetu Technicznego, ISO/IEC JTC 1.

IEC zachęca do adaptacji norm, zwłaszcza tych z zakresu technologii czujników już teraz wykorzystywanych przez przemysł motoryzacyjny do jazdy autonomicznej. Dzięki IEC/TC 47 *Semiconductor devices* powstają Normy Międzynarodowe obejmujące użytkowanie i ponowne wykorzystanie czujników, a także urządzenia do testowania. Powstają także normy obejmujące bezprzewodowe ładowanie elektrycznych pojazdów autonomicznych, nad którymi czuwa IEC/TC 69 *Electric road vehicles and industrial trucks*.

Źródło: IEC e-tech magazine April 2017
I.P.

OCHRONA pojazdów drogowych przed CYBERATAKAMI

Morand Fachot

Najważniejsze systemy infrastruktury coraz częściej są celem wyrafinowanych cyberataków. Sesja corocznego sympozjum Future Networked Car – organizowana przez Międzynarodowy Związek Telekomunikacyjny (International Telecommunication Union – ITU) oraz Europejską Komisję Gospodarczą (United Nations Economic Commission for Europe – UNECE) w ramach Geneva Motor Show – dokonała przeglądu środków podejmowanych dla cyberbezpieczeństwa systemów motoryzacyjnych. W wydarzeniu wzięli udział przedstawiciele władz, producenci samochodów oraz osoby zajmujące się opracowywaniem rozwiązań z zakresu cyberbezpieczeństwa w motoryzacji.

Troska o bezpieczeństwo

Instytucje rządowe i władze lokalne są zaniepokojone zagrożeniami związanymi z systemami transportu drogowego.

Darren Handley, Departament Transportu (Department for Transport – DoT), wyjaśnił uczestnikom, że przed przemysłem motoryzacyjnym stoją trzy rodzaje wyzwań:

- kulturalne: cyberbezpieczeństwo jest nowym zjawiskiem dla branży, potrzebuje więc odpowiednich struktur i organizacji;
- techniczne: trudność wynikająca z długiego czasu rozwoju i cyklu życia pojazdów, zarządzania ryzykiem w łańcuchu dostaw i interakcji z osobami trzecimi (trudności jak po wprowadzeniu na rynek urządzeń telematycznych);
- rządowe: nie ma żadnych regulacji, które precyzowałyby, co producenci powinni robić.

Jednak D. Handley zwraca uwagę, że organizacje normalizacyjne takie jak ISO, ITU, Stowarzyszenie Inżynierów Motoryzacji (Society of Automotive Engineers – SAE) oraz IEC i ISO w ramach Wspólnego Komitetu Technicznego ISO/IEC JTC 1 *Information technology*, pracują nad wstępnymi wytycznymi w tym obszarze.

Podejście brytyjskiego Departamentu Transportu ma sprawić, że „sektor transportu w UK będzie bezpieczny i odporny na cyberzagrożenia, a także zdolny do dalszego rozwoju w coraz bardziej połączonym, cyfrowym świecie". DoT chce zapewnić odpowiedni poziom ochrony pojazdów i infrastruktury drogowej z jaką pojazdy się komunikują przed nieautoryzowanym dostępem, przejęciem kontroli czy zakłóceniami.

Według D. Henley'a , DoT będzie wspierać to podejście poprzez:

- rozumienie zagrożeń dla cyberbezpieczeństwa i wrażliwość sektora transportu;
- zmniejszanie ryzyka wystąpienia cyberataku i podejmowanie odpowiednich działań, by chronić kluczowe zasoby;
- szybkie i efektywne reagowanie na incydenty cybernetyczne;
- promocję zmiany kulturowej, zwiększenie świadomości i budowę potencjału cybernetycznego.

Podejmowane w tej materii działania obejmują:

- promocję – dzięki inicjatywom takim jak wymiana informacji motoryzacyjnych prowadzona przez brytyjskie Centrum Bezpieczeństwa Cybernetycznego (National Cyber Security Centre (NCSC)) oraz Centre for the Protection of National Infrastructure (CPNI) w lutym 2017 r.; promocja zasad cyberbezpieczeństwa połączonych pojazdów autonomicznych (connected autonomous vehicles – CAV) w kwietniu 2017 r.;
- łagodzenie – poprzez współpracę w zakresie bezpieczeństwa cybernetycznego dla połączonych korytarzy* z partnerami z UE; przewodnictwo Grupy zadaniowej ds. bezpieczeństwa internetowego w ramach światowego forum UNECE w sprawie harmonizacji przepisów dotyczących pojazdów (projekt dokumentu 2018);
- reagowanie – zapewnienie mechanizmów raportowania i reagowania na incydenty poprzez system NCSC/CPNI Cyber Incident Response (CIR) (2017 r.).

Perspektywa jednostek badawczych i certyfikujących

Dirk Schlesinger, Dyrektor ds. Technologii w TÜV SÜD, (międzynarodowa firma świadcząca usługi w zakresie badań, kontroli, audytów i certyfikacji), podkreślił, jakie, wyzwania stoją przed branżą: „samochodem jutra jest komputer na kółkach, tylko bardziej skomplikowany". D. Schlesinger wspomniał o systemie Windows 10, który zawiera 27 – 50 milionów linii kodu, włączając w to płytę główną, kartę graficzną i aplikacje takie jak Office. Zauważył też, że Windows 10 nie ma żadnych czujników, a wszystko pozostaje w jednym miejscu. Dla porównania: supersamochód Ford GT ma 50 różnych czujników w zestawach 28 mikroprocesorów, 6 sieci CAN (communication area network), 3 000 różnych sygnałów dostarczających ekwiwalent 100 GB danych na godzinę (100 GB/h).

Wyzwaniem jest zebranie wszystkich sygnałów i ich skomunikowanie, mając przy tym pewność, że „gdy jeden czujnik zawiedzie to nie padnie cały system". Zauważa też, że samochód ma 10 milionów linii kodu „do zastosowań w sytuacjach krytycznych", czyli o 3 miliony więcej niż Boeing 787 i o 8 milionów więcej niż myśliwiec F-22, a „restart podczas jazdy jest wykluczony".

„Zawsze zakładaj, że jesteś w niebezpiecznej sieci, gdzie jesteś narażony na wiele ataków z różnych źródeł", uważa D. Schlesinger. Źródłem ataku mogą być wg niego „pokładowe" systemy audio, aplikacje na smartfony, przechwycenie komunikacji, (np. przy zdalnym otwieraniu drzwi, czujnikach ciśnienia opon oraz bezpośrednim dostępie do sieci przez tylną kamerę) lub zerwanie lusterka. Niedługo źródłem zagrożeń może być infrastruktura IT sprzedawcy lub zakładu naprawczego, dane od producentów oryginalnego wyposażenia albo inne elementy cyfrowego łańcucha dostaw.

Jak podkreślił D. Schlesinger, ochrona oprogramowania i kontrola jakości są coraz istotniejsze, jednak istniejące normy nie są wystarczające. Ostrzegał, że poleganie wyłącznie na bramach sieciowych i programach antywirusowych nie rozwiązuje wszystkich problemów, a całościowe spojrzenie na cyberbezpieczeństwo powinno uwzględniać technologię informatyczną i operacyjną (IT and Operational Technology – OT) podobną do tej w automatyce przemysłowej.

W poszukiwaniu rozwiązań informatycznych

Arnaud Taddei, Dyrektor ds. Architektury Systemów Bezpieczeństwa i główny technolog w Symantec, zaprezentował podejście firmy polegające na wyposażaniu samochodów w kompleksowe systemy bezpieczeństwa. To podejście zostało krótko opisane w Białej Księdze.

Według firmy Symantec „technologia istnieje po to, aby rozwiązywać wiele problemów związanych z bezpieczeństwem; trudności związane z wdrażaniem takiej technologii w samochodach są znacznie większe niż podobne działania w tradycyjnych systemach informatycznych. W nich większość problemów może zostać rozwiązana dzięki szybkiej instalacji, aktualizacji, zmianie konfiguracji" lub przy wykorzystaniu bardziej radykalnych środków mających na celu walkę z wyrafinowanymi zagrożeniami. Ale „samochody nie działają w ten sposób", ponieważ nie otrzymują „tygodniowych, codziennych i bieżących aktualizacji zabezpieczeń".

Firma Symantec zaleca „skalowalne podejście do wbudowanego systemu zabezpieczeń". Wymaga ono dyscypliny i współpracy w stosowaniu następujących podstawowych zasad bezpieczeństwa:

- ochrona całej komunikacji (całej łączności);
- ochrona każdego czujnika, siłownika, mikrokontrolera (MCU) i mikroprocesora;
- bezpieczne i efektywne zarządzanie całym pojazdem za pomocą OTA***;
- łagodzenie zaawansowanych zagrożeń.

Branża motoryzacyjna stoi w obliczu poważnych wyzwań, jak zauważa Symantec - aby bezpiecznie wprowadzać nowe technologie, potrzeba jest długiego czasu na przeprowadzanie certyfikacji. Ale sytuacja jest pilna, zaniedbanie tej kwestii może spowodować wzrost liczby ofiar śmiertelnych, podobnie jak zbyt szybkie zmiany w technologii.

Rozwiązanie tego „dużego i złożonego problemu wymaga zrozumienia i starań zarówno ze strony firm motoryzacyjnych, jak i firm zajmujących się bezpieczeństwem IT i OT. Projektowanie samochodów, które są bezpieczne od początku do końca, będzie wymagało czasu, a oba przemysły muszą zacząć rozwiązywać kwestie związane z bezpieczeństwem na każdym poziomie motoryzacyjnego łańcucha wartości".

Ochrona samochodów przed zagrożeniami cybernetycznymi wymaga dyscypliny i współpracy w stosowaniu podstawowych zasad bezpieczeństwa na każdym poziomie.

Symantec wskazuje „cztery podstawy" takiego działania:

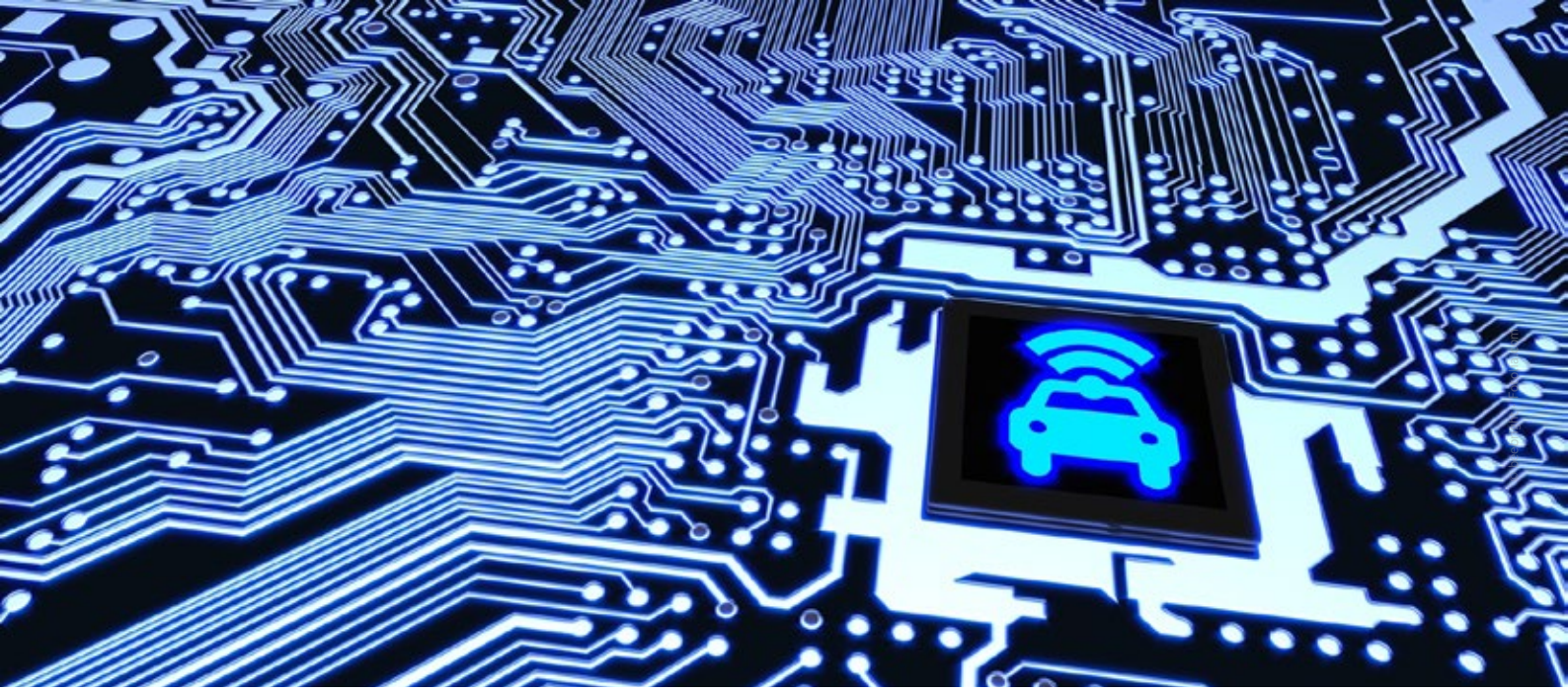
- ochrona łączności: w szczególności modemów wykorzystywanych w ramach platform IVI (in-vehicle infotainment) lub w diagnostyce pokładowej pojazdu (on-board diagnostics – OBD);
- ochrona każdego modułu: czujników, siłowników i wszystkiego z MCU;
- zarządzanie z pomocą OTA: z chmury do każdego samochodu;
- łagodzenie zaawansowanych zagrożeń: analiza w samochodzie i w chmurze.

„Długoterminowe, kompleksowe bezpieczeństwo wymaga zbudowania bezpieczeństwa w każdej warstwie samochodu. Dzisiejsze samochody mają wiele warstw. (...). Zabezpieczenie całego „stosu" od góry do dołu w pełni i kompleksowo potrwa wiele lat, biorąc pod uwagę złożoność relacji z rozproszonymi dostawcami", zauważa Symantec, który oferuje zestaw technologii, mających sprostać tym wyzwaniom.

Bezpieczne pojazdy połączone

Yoram Berholtz, Dyrektor ds. Rozwoju Biznesowego w firmie Argus (firma zajmująca się bezpieczeństwem cybernetycznym w motoryzacji), która zapewnia bezpieczeństwo sieciowe całego pojazdu dzięki wykrywaniu ataków, podejrzanych działań i zmian standardowych zachowań w sieci pojazdu. Pojazdowa Ochrona Sieci firmy Argus, dzięki scentralizowanemu ośrodkowi sterowania, bada całą sieć komunikacyjną pojazdu i powstrzymuje pojawiające się w niej zagrożenia.

Według Y. Berholtza, w przyszłym roku na drogach będzie się poruszać 100 milionów samochodów.



Możliwe scenariusze ataku obejmują cyberokup, kradzieże samochodów, ataki ukierunkowane na prowokowanie wypadków, kradzież danych, naruszenia prywatności i wypadki.

Dyrektor Berholtz zauważa, że prawie wszystkie główne marki samochodów były już celem ataków. Podał przykłady takich sytuacji i wspomniał o pojazdach, które miały luki w zabezpieczeniach.

Opisał krótko „Filozofię cyberbezpieczeństwa wg firmy Argus", która polega na:

- zapobieganiu: utrudnienie dokonania ataku;
- zrozumieniu: identyfikacja ataku i jego rodzaju w czasie rzeczywistym;
- reakcji: ograniczanie szkód i uodpornianie floty pojazdów w ciągu kilku godzin.

Zapobieganie polega na:

- ochronie wewnętrznej: poprzez ochronę elektronicznego sterownika wtrysku (engine control unit – ECU), ochronę sieci pojazdu oraz ochronę łączności;
- ochronie zewnętrznej pojazdu przez cały okres użytkowania i ochronie części zamiennych.

Wiele zależy od monitorowania flot pojazdów w czasie rzeczywistym w celu wykrycia luk w zabezpieczeniach zaatakowanych podzespołów, blokowania ataków i zabezpieczenia dostępu osób nieupoważnionych.

Bezpieczeństwo zapewnia bezprzewodowe dostarczanie aktualizacji zabezpieczeń.

Długoterminowe zadanie wymagające ścisłej współpracy pomiędzy organizacjami

Ochrona pojazdów drogowych przed zagrożeniem cybernetycznym jest trudnym zadaniem, niemożliwym do osiągnięcia w krótkim czasie. Będzie ono wymagało ścisłej i stałej współpracy między wieloma organizacjami, producentami samochodów i OEM, firmami dostarczającymi oprogramowanie i dostawcami systemów zabezpieczających.

IEC, działając w ramach ISO/IEC JTC 1, odgrywa swoją rolę w ogólnej strukturze, jak pokazuje to dokument UNECE dotyczący Zasad Systemu Bezpieczeństwa w Systemach Inteligentnego Transportu oraz Pojazdach Autonomicznych i Połączonych.

Wspomniany dokument wymienia ponad 11 norm i innych publikacji ISO/IEC JTC 1, dwie normy SAE (SAE J3061, *Cybersecurity guidebook for cyber-physical vehicle systems and SAE J3101, Requirements for hardware protected security for ground vehicle applications*) oraz cztery dokumenty NIST.

**connected corridors*
***original equipment manufacturer/service provider – (OEM/SP)*
****OTA (Over the Air) - Funkcja oferowana przez niektóre modele telefonów komórkowych pozwalająca na pobranie np. danych konfiguracyjnych. Niektóre aparaty umożliwiają w ten sposób szybkie i łatwe skonfigurowanie przeglądarki WAP lub usługi GPRS. Przy pomocy funkcji OTA możliwe jest również pobieranie do pamięci telefonu programów napisanych w języku Java 2 Microediton.*

Źródło: IEC etech magazine, Issue 03/2017
I.P.

Biometria dla konsumentów

Elektroniczny DNA ułatwia dostęp do pojazdów i zwiększa bezpieczeństwo

Antoinette Price

Odcisk palców, dłoń, tęczówka, głos, rozpoznawanie twarzy i gestu pomogą w rozwoju systemów wspomagania kierowcy i bezpieczeństwa pojazdów.

Biometria jest stosowana od dziesięcioleci przez organy ścigania oraz w systemach służących identyfikowaniu osób i kontrolowaniu dostępu, które wymagają wysokiego poziomu zabezpieczeń. Systemy te porównują dane behawioralne i fizyczne.

Niedawno ten zasięg rozszerzył się. Już teraz możemy zabezpieczyć dostęp do smartfonów lub tabletów odciskiem palca lub używać aplikacji rozpoznawania głosu do uwierzytelniania internetowych kont bankowych.

Działać z normami

Komitety techniczne IEC i ich podkomitety tworzą Normy Międzynarodowe w celu zapewnienia niezawodności, jakości i interoperacyjności.

Wspólny Komitet Techniczny ISO/IEC JTC 1 zajmuje się technologiami informacyjnymi. Zakres ISO/IEC JTC 1/SC 37 *Biometrics* obejmuje specyfikacje dotyczące bezpieczeństwa, testowania i raportowania różnych aspektów, takich jak format wymiany danych, rozpoznawanie twarzy, rozpoznawanie komend głosowych.

Odcisk palca - klucz do Twojego samochodu

W miarę jak samochody stają się bardziej połączone i zmierzają do pełnej samodzielności, przemysł motoryzacyjny również zmierza w tym kierunku. Raport Frost i Sullivan mówi, że do roku 2025 jeden na trzy samochody (prawie 34 miliony samochodów osobowych) będzie używać biometrii do identyfikacji i personalizacji.

Zabezpieczenia dla pojazdów

W 2016 r. rekordowa liczba firm technologicznych współpracowała z producentami samochodów, które coraz częściej włączają inteligentne funkcje do swoich najnowszych pojazdów. W badaniach przeprowadzonych przez firmę Gartner szacuje się, że do 2020 r. po drogach będzie poruszać się ćwierć miliarda samochodów połączonych. Jednak jednym z największych wyzwań będzie zabezpieczenie ogromnej liczby danych, które takie samochody tworzą, i ochrona pasażerów przed ich zhakowaniem.

Wiele nowych samochodów ma systemy wykorzystujące biometrię - są one albo wbudowane, albo prowadzone przez zewnętrzne usługi, takie jak chmura.

W przyszłości zwiększy się liczba funkcji, które będą zawierać dodatkowe zabezpieczenia:

- Uruchamianie i obsługa przyszłych samochodów będzie wymagała identyfikacji kierowcy za pomocą czujnika linii papilarnych, będącego uzupełnieniem klucza.
- Inne systemy będą rozpoznawać twarz kierowcy przed wejściem do pojazdu; włączenie silnika będzie możliwe tylko wtedy, gdy będzie aktywny profil kierowcy.
- Rozpoznawanie tęczówki zostanie użyte do odblokowania zapłonu, identyfikowania użytkowników pojazdu i spersonalizowanych ustawień (np.foteli czy lusterek).

Bezpieczeństwo kierowcy na nowym poziomie

Sektory: samochodowy, ubezpieczeniowy i zdrowotny będą współdziałać, ponieważ zaawansowana biometria sprawi, że przyszłe samochody będą bardziej bezpieczne. Mimo że miną jeszcze lata zanim samochody będą jeździć autonomicznie, a ludzie nie będą musieli nimi kierować, przemysł motoryzacyjny już opracowuje sposoby monitorowania czujności kierowcy. Na przykład czujniki w pasach i osłonach będą monitorować uderzenia rytmu serca kierowcy i ostrzegać przed zawałem, podczas gdy sensory śledzące oczy wykryją senność prowadzącego pojazd. Praca IEC/TC 47 *Semiconductor devices* obejmuje projektowanie, produkcję i użytkowanie czujników.

Pojawienie się innowacyjnych urządzeń do zarządzania zdrowiem w połączeniu ze starzeniem się populacji, zwiększenie świadomości zdrowotnej i rosnąca potrzeba zarządzania chorobami przewlekłymi, doprowadza do wzrostu popularności medycznych nośników (medical wereables). Według raportu Global Industry Analysts oczekuje się, że do 2020 r. światowy rynek wyrobów medycznych do użytku domowego wyniesie 4,5 miliona dolarów.

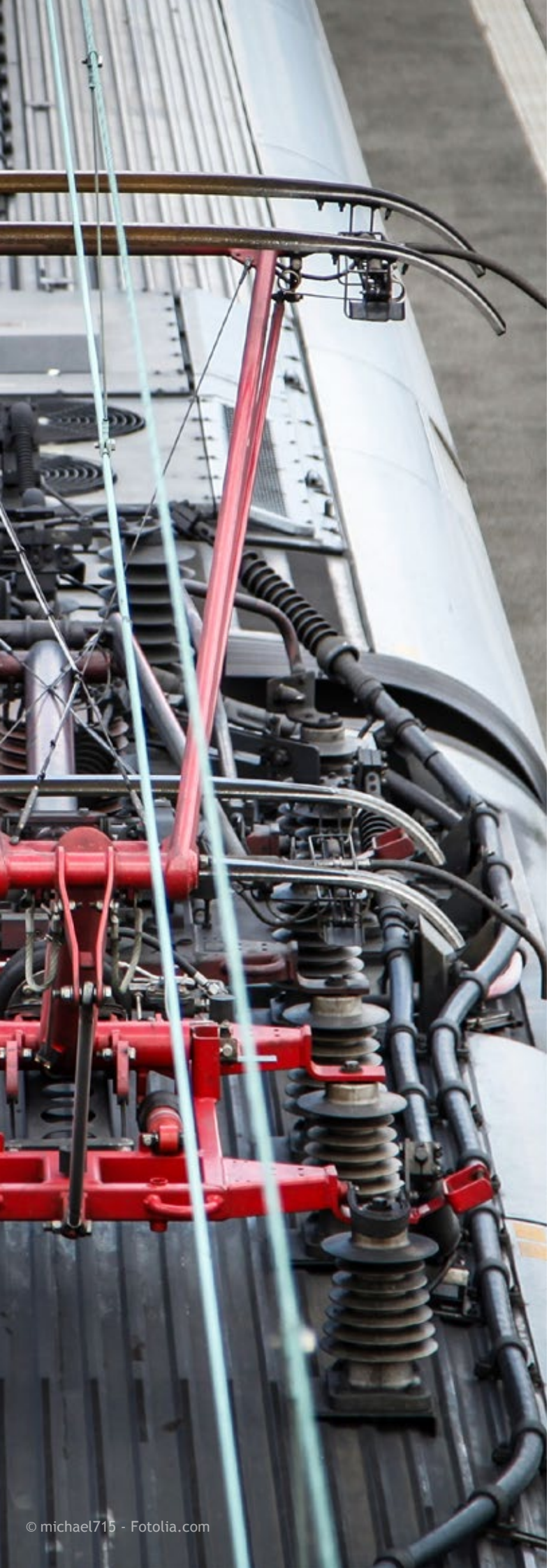
Z tego względu powołano IEC/TC 124, który rozpocznie prace nad normalizacją nośników medycznych i technologii z nimi związanej.

A co z kradzieżą tożsamości?

Choć dane biometryczne są unikalne dla osób fizycznych i są logicznym wyborem jeśli chodzi o bezpieczeństwo dostępu i kontroli, to jednak niczego nie można uznać za 100% bezpieczne. Karty, hasła i osobiste numery identyfikacyjne można anulować lub zmienić w przypadku utraty, zagubienia lub kradzieży, podczas gdy z odciskami palców, które zostały skopiowane i niewłaściwie wykorzystane, już tak postąpić się nie da. Ponadto informacje biometryczne są przechowywane w bazach, które muszą być chronione przed wszelkimi potencjalnymi naruszeniami bezpieczeństwa. Jeśli ta technologia ma się rozpowszechnić, to kwestie problematyczne muszą zostać rozwiązane.

Oprogramowanie i sprzęt w samochodzie będzie wymagał ochrony. Wiele podkomitetów ISO/IEC JTC 1 przyczynia się do zmniejszenia takich zagrożeń, na przykład ISO/IEC JTC 1/SC 27 *IT Security techniques*. Duża liczba danych będzie wymieniana między aplikacjami na smartfonach a inteligentnymi panelami samochodowymi, które również będą integralną częścią Internetu rzeczy. Praca ISO/IEC JTC 1/SC 6 *Telecommunications and information exchange between systems* przyczynia się również do poprawy bezpieczeństwa danych.

Źródło: IEC etech magazine, Issue 03/2017
J.S.



Pantografy

W sektorze Elektryki trwają obecnie prace normalizacyjne nad polską wersją językową normy: *PN-EN 50206-1 Zastosowania kolejowe – Tabor – Pantografy: Charakterystyki i badania – Część 1: Pantografy pojazdów linii głównych*.

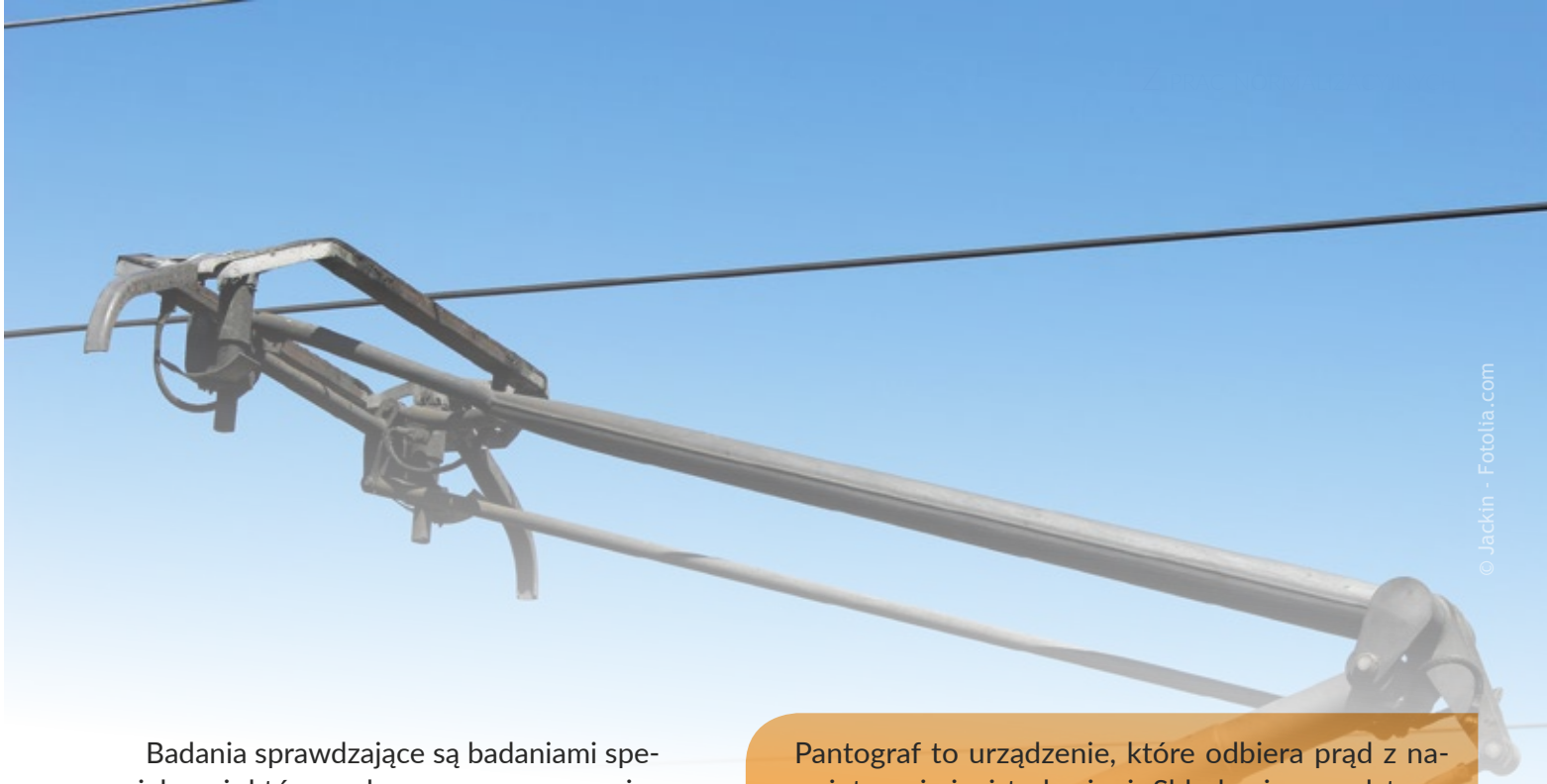
Norma PN-EN 50206-1:2010 zawiera podstawowe charakterystyki montażowe, które powinny być stosowane do pantografów w celu umożliwienia prawidłowego odbioru prądu z systemu sieci jezdnej górnej. Norma określa także badania, którym powinien zostać poddany pantograf przed eksploatacją oraz w jej trakcie.

Wyróżniono cztery kategorie wykonywanych badań:

1) badania typu;
2) badania wyrobu;
3) badania sprawdzające;
4) badania złożone.

Badania typu przeprowadzane są na pojedynczym urządzeniu danej konstrukcji. Urządzenie będące w bieżącej produkcji powinno być uznane za spełniające wymagania badań typu i powinno być zwolnione z tych badań, jeżeli producent dostarczy podpisane raporty z wykonanych już badań typu na identycznym urządzeniu skonstruowanym wcześniej. Badania wyrobu należy wykonywać w celu sprawdzenia, czy właściwości wyrobu odpowiadają parametrom zmierzonym podczas badania typu.

Jednym z przykładów obrazujących zarówno badanie typu, jak i badanie wyrobu jest sprawdzanie funkcjonowania systemu ADD (Automatic Drop Device). System ten wyłącza z użycia niesprawny pantograf, zabezpieczając go przed poważniejszym uszkodzeniem oraz chroniąc sieć trakcyjną przed ewentualnym zerwaniem.



Badania sprawdzające są badaniami specjalnymi, które wykonywane są na pojedynczym egzemplarzu w celu uzyskania dodatkowych informacji. Obejmują badania działania (np. pomiar średniej statycznej siły stykowej w temperaturze otoczenia) oraz badania wytrzymałościowe (np. badania drgań pionowych).

Badania złożone są badaniami specjalnymi i uzupełniającymi, mogą być przeprowadzane tylko w środowisku eksploatacyjnym. Powinny one uwzględniać typ pojazdu, który ma być stosowany, jego prędkość i kierunek jazdy. Za przykład badania złożonego może posłużyć badanie terenowe, którego celem jest ustalenie, że ślizgacz odbieraka prądu wytrzyma bez uszkodzeń prąd znamionowy z pojazdem w warunkach jazdy. Badanie to powinno być przeprowadzone z pantografem zamontowanym na dachu lokomotywy ciągnącej pociąg na linii i z obciążeniem prądowym podanym w warunkach technicznych odbiorcy. Podczas tego badania temperatura i prąd w funkcji czasu powinny być rejestrowane na nakładkach stykowych i w krytycznych sekcjach ślizgacza odbieraka prądu. Kryterium przyjęcia wyników badania jest brak oznak nadmiernego nagrzewania się jakiejkolwiek części ślizgacza odbieraka prądu.

Pantograf to urządzenie, które odbiera prąd z napowietrznej sieci trakcyjnej. Składa się z podstawy ramy, systemu działania, ramy przegubowej i ślizgacza zwanego potocznie kołyską. Podstawa ramy to stała część pantografu, która jest przymocowana do dachu pojazdu za pośrednictwem izolatorów. Pod pojęciem system działania rozumie się urządzenie, które zapewnia siłę do podnoszenia lub opuszczania pantografu oraz utrzymywania go w pozycji złożenia. Ruchoma rama składa się z układu ramion połączonych przegubowo. Układ ten służy do regulacji pionowej wysokości ślizgacza oraz zapewnia jego odpowiedni docisk na skutek działania układu napędowego. Ślizgacz to część, która jest podtrzymywana przez ramę i obejmuje nakładki stykowe, nabieżniki („wąsy”) oraz może zawierać zawieszenie. Nakładki stykowe realizują bezpośredni styk z przewodem jezdnym sieci trakcyjnej i ślizgając się wzdłuż przewodu jezdnego, umożliwiają przekazywanie energii.

Badania przedstawione w normie nie obejmują badań izolatorów. Norma nie uwzględnia także badań dielektrycznych pantografów, które powinny być przeprowadzone na pantografie zainstalowanym na dachu pojazdu. Nie dotyczy ona również pantografów używanych w wyodrębnionych systemach metra i kolei z taborem o lekkiej konstrukcji. Takie pantografy są przedmiotem rozważań w PN-EN 50206-2:2010.

Właściwe utrzymanie i diagnostyka pantografów ma duże znaczenie dla prawidłowej współpracy z siecią trakcyjną. Stosowanie nowoczesnych urządzeń diagnostycznych i zwrócenie uwagi na zagrożenia związane z wprowadzaniem nowych rozwiązań konstrukcyjnych może zmniejszyć liczbę zdarzeń wynikających z uszkodzeń ślizgacza odbieraka prądu bądź sieci jezdnej.

Sektor Elektryki

Metale - próba udarności

KT 123 ds. Badań Własności Metali

W 2017 r. zostały opublikowane angielskie wersje językowe norm:
PN-EN ISO 148 Metale - Próba udarności sposobem Charpy'ego:
- Część 1: Metoda badania
- Część 2: Sprawdzanie młotów wahadłowych
- Część 3: Przygotowanie i charakterystyka próbek wzorcowych Charpy-V do pośredniego sprawdzania młotów wahadłowych

Próba udarności jest próbą dynamiczną, określającą zdolność materiału do przenoszenia gwałtownych obciążeń typu uderzeniowego. Charakteryzuje ona te własności mechaniczne materiału, których nie można wykryć przy pomocy prób statycznych. Badanie to ma szczególne znaczenie dla stali ulepszanych cieplnie, gdy wraz z korzystnym wzrostem wytrzymałości i twardości zachodzi szkodliwy wzrost kruchości materiału. Próba pozwala w tym przypadku ustalić najlepsze warunki obróbki cieplnej.

Jedną ze stosowanych prób udarności jest próba udarności sposobem Charpy'ego, opisana w wieloczęściowej normie PN-EN ISO 148.

Część 1. zawiera opis próby udarności sposobem Charpy'ego z karbem V lub karbem U. Omówiono tu metodę polegającą na pomiarze energii pochłoniętej w trakcie badania udarności metali, z użyciem młotów wahadłowych Charpy'ego.

W części 2. opisano sprawdzanie elementów młotów wahadłowych stosowanych w próbie udarności zarówno pod względem konstrukcji, jak również wydajności i dokładności wyników. Norma ta ma zastosowanie dla młotów wahadłowych o różnych konstrukcjach i wydajności. Zawarto w niej dwie metody sprawdzania: metodę bezpośrednią i pośrednią. Metoda bezpośrednia obejmuje pomiar części krytycznych maszyny w celu zapewnienia, że spełnia wymagania tej części normy. Przyrządy służące sprawdzaniu i kalibracji są zgodne z normami krajowymi. Metoda pośrednia wykorzystuje próbki wzorcowe do badań w celu sprawdzania punktów na skali pomiarowej dla zaabsorbowanej energii. Wymagania dotyczące próbek odniesienia znajdują się w PN-EN ISO 148-3. Aby młot wahadłowy stosowany w próbie udarności był zgodny z tą częścią normy, powinien być sprawdzony obiema metodami. W tej części normy zawarto również opis sposobu oceny poszczególnych składowych energii całkowitej pochłoniętej w złamaniu próbki do badań.

W części 3. określono wymagania oraz metody przygotowania dla próbek do badań stosowanych do pośredniego sprawdzania młotów wahadłowych. Próbki wzorcowe do badań kwalifikuje się na wzorcowych młotach wahadłowych (stosowanych w próbie udarności), również opisanych w tej części normy.

Wieloczęściowa norma PN-EN ISO 148 to jedna z podstawowych norm z zakresu KT 123 ds. Badań Własności Metali. Ma zastosowanie w przemyśle, laboratoriach czy na uczelniach.

Urszula Niedźwiedzka
Sektor Hutnictwa

Sporty walki – atak i obrona z maksymalną gwarancją bezpieczeństwa współzawodników

Boks, karate, kick-boxing, taekwondo, jiu-jitsu, judo, sumo, zapasy, wrestling, kendo, aikido… itp. Długo by wymieniać, prawdopodobnie każdy z nas zetknął się w swoim życiu z którąś z tych nazw bądź sam uprawiał którąś z wymienionych dyscyplin. Chodzi oczywiście o sporty walki. We współczesnym świecie znalazły one już swoje stałe miejsce jako dyscyplina sportowa bądź sposób samoobrony. Wprawdzie w tym drugim przypadku mowa raczej o sztukach walki, które połączone są najczęściej z dążeniem do psychofizycznego samodoskonalenia, ale one także oparte są na określonych technikach walki. Znaczenie sportów walki podkreśla fakt, że szereg z nich znalazło się wśród dyscyplin olimpijskich.

Walka jest stara jak historia ludzkości, wiąże się z zachowaniem sprawności, siły i sprytem, towarzyszy ludzkości na całym świecie. Walczono w celu obrony przed napaścią, jak również z chęci zdobycia pożywienia i przetrwania. Prymitywne formy walki praktykowano już od czasów prehistorycznych, a w czasach starożytnych rozgrywano zawody w walkach bokserskich, zapaśniczych oraz innych, w których wykorzystywano uderzenia, kopnięcia, chwyty i rzuty.

Sztuki walki pochodzą z Dalekiego Wschodu (Azja Wschodnia); nigdzie walka wręcz lub z wykorzystaniem akcesoriów takich jak kije, miecze, pałki (tonfa), łuki nie zyskała tak wielkiej skuteczności i rangi. Do Ameryki i Europy sztuki walki dotarły dopiero w połowie XIX wieku wraz z falą chińskich emigrantów, a prawdziwe zainteresowanie tym sposobem skutecznego unieszkodliwiania przeciwnika wzbudziły filmy z Azji Wschodniej, głównie z Hong Kongu, dając motywację do pogłębiania wiedzy z tego zakresu.

Wraz ze wzrastającym zainteresowaniem tą dziedziną życia zrodziła się konieczność ujednolicenia zasad i dopracowywania technik walki, a z czasem wiele sztuk walki przekształciło się w dyscypliny sportowe. I jak to w wielu innych sportach tego typu, w konkurencjach związanych z walką wręcz trzeba liczyć się z powstaniem urazów w trakcie starcia z przeciwnikiem. To z kolei wymusza konieczność zagwarantowania zawodnikom maksymalnej ochrony przy jednoczesnym zapewnieniu, że ich możliwości wykazania zręczności i znajomości techniki nie zostaną ograniczone.

Nad rozwiązaniem tego problemu pracują specjaliści z CEN/TC 162 „Odzież ochronna, ochrona rąk i ramion oraz kamizelki ratunkowe", którzy od wielu lat dokładają starań, aby ujednolicić wymagania dotyczące ochraniaczy dla sportowców

trenujących sporty walki. Norma opisująca takie środki ochrony – EN 13277 – powstała już ponad 15 lat temu. Składała się z kilku części, które dotyczyły wymagań ogólnych i dodatkowych oraz metod badań w odniesieniu do sprzętu ochronnego dla uprawiających sztuki walki. Przez lata norma ta była wielokrotnie nowelizowana, powstawały kolejne części, dotyczące już konkretnych fragmentów ciała (głowy, tułowia, śródstopia itp.). Do chwili obecnej opublikowano następujące części normy EN 13277:

PN-EN 13277 Środki ochrony dla uprawiających sztuki walki
- Część 1: Ogólne wymagania i metody badań
- Część 2: Dodatkowe wymagania i metody badań dotyczące ochraniaczy śródstopia, ochraniaczy goleni i ochraniaczy przedramion
- Część 3: Dodatkowe wymagania i metody badań dotyczące ochraniaczy tułowia
- Część 4: Dodatkowe wymagania i metody badań dotyczące ochraniaczy głowy
- Część 6: Dodatkowe wymagania i metody badań dotyczące ochraniaczy na piersi kobiet
- Część 5: Dodatkowe wymagania i metody badań dotyczące ochraniaczy narządów płciowych i brzucha
- Część 7: Dodatkowe wymagania i metody badań dotyczące ochraniaczy dłoni i stóp

Wszystkie części tej normy zostały przetłumaczone na język polski przez specjalistów z Komitetu Technicznego 22 ds. Odzieżownictwa. Istnieje możliwość ich zakupu w sklepie PKN, dodatkowo jest także szansa zapoznania się z angielską wersją każdej z tych norm.

Nie oznacza to, że CEN/TC 162 zakończył prace nad EN 13277. Już powstaje kolejna jej część, dotycząca ochraniaczy twarzy w karate:

prPN-prEN 13277-8 Środki ochrony dla uprawiających sztuki walki - Część 8: Dodatkowe wymagania i metody badań dotyczące ochraniaczy twarzy w karate

Projekt opracowywany jest w trzech oficjalnych wersjach językowych (angielskiej, francuskiej i niemieckiej), z jego treścią można było zapoznać się w trakcie ankiety powszechnej pod koniec ubiegłego roku.

Jak więc widać normy już są, ich znaczenie zostało docenione przez wpisanie ich na listę norm zgodnych z wymaganiami dyrektywy Nowego podejścia 89/686/EWG odnoszącej się do środków ochrony indywidualnej.

Ważne jest, aby uprawiający sporty walki byli świadomi konieczności użytkowania specjalistycznego sprzętu ochronnego i sięgali po ochraniacze wysokiej jakości, oznaczone znakiem CE[1]). Pozwoli to na zwiększenie bezpieczeństwa podczas uprawiania sportów walki, przy zachowaniu niewątpliwej widowiskowości tych dyscyplin sportowych.

Anna Steidel
Sektor Produktów Powszechnego Użytku

1) Znak oznaczający potwierdzenie zgodności wyrobu z wymaganiami określonymi w dyrektywie europejskiej.

Komitety Techniczne
Komitety Zadaniowe
Podkomitety Techniczne

maj 2017

Komitety Techniczne

Zmiany zakresu tematycznego Komitetów Technicznych:

- **KT 62 ds. Sprzętu Elektroinstalacyjnego** rozszerzył zakres o CLC/TC 23H, Plugs, Socket-outlets and Couplers for industrial and similar applications, and for Electric Vehicles; CLC/SR 23K, Electrical energy efficiency products; IEC/TC 23/SC 23K, Electrical Energy Efficiency products
- **KT 80 ds. Ogólnych w Sieciach Elektroenergetycznych** rozszerzył zakres o CLC/SR 115, High Voltage Direct Current (HVDC) Transmission for DC voltages above 100kV (Provisional)
- **KT 171 ds. Sieci Komputerowych i Oprogramowania** rozszerzył zakres o CEN/TC 445, Digital information Interchange in the Insurance Industry

Nowi członkowie Komitetów Technicznych

W maju Prezes PKN powołał na członków KT następujące podmioty:

- **Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego - Państwowy Instytut Badawczy** do KT 6 ds. Systemów Zarządzania
- **GRYFITLAB Sp. z o .o .** do KT 273 ds. Mechanicznych Urządzeń Zabezpieczających.
- **ICR Polska Sp. z o.o.** do KT 11 ds. Telekomunikacji
- **Krajowe Forum Chłodnictwa Związek Pracodawców** do KT 63 ds. Elektrycznego Sprzętu Powszechnego Użytku
- **PPG Deco Polska Sp. z o.o.** do KT 175 ds. Farb i Lakierów
- **Szajna Laboratorium Optyczne** do KT 49 ds. Optyki i Przyrządów Optycznych
- **Urząd Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych** do KT 284 ds. Sprzętu, Narzędzi i Urządzeń Medycznych Mechanicznych.

Odwołania członków Komitetów Technicznych

W maju Prezes PKN odwołał z członka KT:

- eCall Polska Sp. z o.o. z KT 17 ds. Pojazdów i Transportu Drogowego
- Elgór+Hansen SA z KT 5 ds. Chłodnictwa, Pomp Ciepła, Klimatyzatorów i Sprężarek
- Instytut Energetyki - Instytut Badawczy z KT 303 ds. Materiałów Elektroizolacyjnych
- Lhoist Polska Sp. z o.o. z KT 196 ds. Cementu i Wapna

RODO - OCHRONA DANYCH OSOBOWYCH OD PODSTAW

SZKOLENIE

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

Zagadnienia:

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

Miejsce szkolenia:

Polski Komitet Normalizacyjny
ul. Świętokrzyska 14
Warszawa

Cena szkolenia:

390,00 zł netto + 23% VAT/osobę

Więcej szczegółów na stronie wiedza.pkn.pl

PKN POLSKI KOMITET NORMALIZACYJNY

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