

Dodatkowe informacje dotyczące procesu zatwierdzenia typu przyrządów do pomiaru prędkości pojazdów w kontroli ruchu drogowego

Proces zatwierdzenia typu przyrządu pomiarowego w Głównym Urzędzie Miar ma następujący przebieg:

1. wpływ wniosku wraz z załącznikami,
2. analiza kompletności wniosku, wezwanie do uzupełnienia wniosku (jeśli złożony wniosek ma braki),
3. analiza merytoryczna wniosku, badania techniczne przyrządu pomiarowego,
4. wyjaśnienia do wniosku (jeśli zachodzi potrzeba dodatkowych wyjaśnień),
5. zakończenie badań oraz udokumentowanie ich wyników w sprawozdaniu,
6. informacja o prawie do wglądu do akt sprawy (na tym etapie wnioskodawca ma możliwość zapoznania się z wynikami badań i pozostałymi dowodami zebranymi w sprawie, a także ustosunkowania się do zebranych dowodów i materiałów),
7. wydanie decyzji zatwierdzenia typu przyrządu pomiarowego,
8. określenie wysokości opłaty za wydanie decyzji zatwierdzenia typu przyrządu pomiarowego.

Ww. punkty pokazują standardowy przebieg procesu zatwierdzenia typu przyrządu pomiarowego. W niektórych przypadkach proces ten może odbywać się inaczej, ze względu na indywidualny charakter każdej sprawy. Zasady postępowania w procesie zatwierdzenia typu przyrządu pomiarowego określa Kodeks Postępowania Administracyjnego oraz ustawa Prawo o Miarach. Szczegółowe informacje w tym zakresie znajdują Państwo w zakładce Zatwierdzenie typu przyrządu pomiarowego na stronie Głównego Urzędu Miar.

Ze względu na konstrukcję przyrządów do pomiaru prędkości pojazdów w kontroli ruchu drogowego, a także stawiane im w przepisach prawa wymagania (rozporządzenia Ministra Gospodarki w sprawie wymagań, którym powinny odpowiadać przyrządy do pomiaru prędkości pojazdów w kontroli ruchu drogowego, oraz szczegółowego zakresu badań i sprawdzeń wykonywanych podczas prawnej kontroli metrologicznej tych przyrządów pomiarowych (Dz.U. z 2019 poz. 1081) – tekst ujednoczony akty prawne do ISAP-u (sejm.gov.pl)), badania techniczne przyrządu obejmują:

- badania metrologiczne i środowiskowe,
- badania oprogramowania,
- badania kompatybilności elektromagnetycznej.

WYTYCZNE DOTYCZĄCE PRZYGOTOWANIA DOKUMENTACJI I PRZYRZĄDÓW DO POMIARU PRĘDKOŚCI POJAZDÓW W KONTROLI RUCHU DROGOWEGO

Dane, które powinien zawierać wniosek o zatwierdzenie typu przyrządu pomiarowego, w tym także przyrządu do pomiaru prędkości pojazdów w kontroli ruchu drogowego, są wskazane w zakładce:

[Jakie dane powinien zawierać wniosek o zatwierdzenie przyrządu pomiarowego? - Zatwierdzenie typu przyrządu pomiarowego - Główny Urząd Miar \(gum.gov.pl\)](#) natomiast niezbędne załączniki do wniosku w zakładce:

[Jakie dokumenty należy dołączyć do wniosku? - Zatwierdzenie typu przyrządu pomiarowego - Główny Urząd Miar \(gum.gov.pl\)](#) oraz zakładce:

[Jakie informacje powinna zawierać dokumentacja techniczno-konstrukcyjna przyrządu? - Zatwierdzenie typu przyrządu pomiarowego - Główny Urząd Miar \(gum.gov.pl\)](#) .

Dokumenty załączane do wniosku wymienione w zakładce dotyczącej zawartości dokumentacji techniczno-konstrukcyjnej przyrządu pomiarowego winny zawierać co najmniej następujące informacje:

1. dla potrzeb badań metrologicznych, środowiskowych i kompatybilności elektromagnetycznej:
 - dokładny opis przyrządu, obejmujący sposób dokonywania pomiaru przez przyrząd z uwzględnieniem wszystkich opcji działania. Opis powinien zawierać informacje, jak działa przyrząd, jakie funkcje i właściwości są wykorzystywane podczas przetwarzania od momentu pomiaru prędkości dla wszystkich ustawień głowicy pomiarowej (w przypadku pomiaru z głowicy antenowej, która ma inną charakterystykę nadawczą i odbiorczą anteny, powinny być opisane przypadki wszystkich parametrów charakterystycznych wiązki odbiorczej), w jaki sposób następuje przetwarzanie sygnału i złożenie danych pomiarowych w dowód wykroczenia,
 - dokładny opis konstrukcji obejmujący jednoznacznie informację, które elementy wchodzi w skład przyrządu pomiarowego dla wszystkich wersji przyrządu, a które są urządzeniami dodatkowymi dla przyrządu. Opis sposobu podłączenia do przyrządu i uruchomienia wszystkich urządzeń dodatkowych. Opis wyjść z przyrządu do powszechnie dostępnych urządzeń informatycznych (typ złącza + protokół transmisji - pamięci np. USB, urządzenia komunikacyjne przewodowe np. LAN, RS232 i bezprzewodowe np. Wifi, LTE),
 - dokładny opis plików z dowodami wykroczenia, z naniesionymi charakterystycznymi wartościami, które powinny znajdować się na obrazie. Opis współpracujących programów zewnętrznych,
 - informacje o wszystkich ustawieniach dostępnych w przyrządzie wraz z opisem na co one wpływają i jaki mają wpływ na pomiar i zapis wykroczeń; podać instrukcję instalacji i ustawienia przyrządu na drodze publicznej oraz informację nt. możliwości odczytu konfiguracji programowej dla wygenerowanych danych wykroczenia (zbiorcza informacja nt. instalacji przyrządu w danej wersji w określonym czasie) wraz z zabezpieczeniem takiej instalacji przed zmianą,
 - opis sposobu wykorzystania i połączenia symulatora zgodnie z jego instrukcją obsługi, opis sposobu jego działania, dostarczenie certyfikatów potwierdzających prawidłowość działania symulatora,
 - informacje o sposobie instalacji przyrządu z uwzględnieniem elementów stanowiących przyrząd pomiarowy oraz urządzenia dodatkowe, które mogą być połączone z przyrządem (niewchodzące w skład przyrządu). W przypadku działania przyrządu w różnych ustawieniach, powinien być opisany sposób odczytania informacji w jakim ustawieniu instalacyjnym był przyrząd podczas pomiarów. Instalacja przyrządu wykonywana jest zgodnie z dokumentacją),

- dostarczenie instrukcji obsługi zawierającej informacje o których mowa w treści przepisu § 24 ust. 2 pkt 1 ÷11,
- w przypadku możliwości pracy zdalnej przyrządu dokładny opis sterowania przyrządem dla wszystkich wersji,
- w przypadku dostarczania wyników badań środowiskowych - badania powinny być opisane w sposób szczegółowy (zdjęcia ustawienia przyrządu podczas badań), łącznie ze sposobem, jak było dokonywane sprawdzanie poprawności działania przyrządu podczas trwania narażenia, zachowanie na badanym przyrządzie dowodów wykroczeń wygenerowanych podczas trwania narażeń,
- w trakcie badań środowiskowych i kompatybilności elektromagnetycznej może wystąpić konieczność dostosowania złączy i przewodów do stanowisk w laboratorium.

2. dla potrzeb badań oprogramowania:

- listę kont dostępowych na wszystkich poziomach dostępu,
- wykaz i opis przeznaczenia oprogramowania zainstalowanego w przyrządzie,
- oznaczenia oprogramowania metrologicznego i miejsce jego instalacji w przyrządzie,
- opis interfejsów użytkownika przyrządu, wraz z wykazem elementów sterujących (system menu i okien dialogowych),
- opis budowy przyrządu w postaci schematu blokowego podzespołów i opisu oprogramowania przyrządu (np. schemat budowy wewnętrznej, topografii połączeń, rodzaje sieci transmisyjnych, pamięci wewnętrznych itp.),
- sposób wyznaczania sum kontrolnych stosowanych do uwierzytelnienia transmisji danych zarejestrowanych przez przyrząd oraz wskazanie wykorzystywanych algorytmów kryptograficznych;
- w zakresie zabezpieczeń danych cyfrowych i oprogramowania w szczególności:
 - opis sposobu zabezpieczenia zarejestrowanych danych przed dostępem osób nieupoważnionych oraz przed ich zmianą i zniszczeniem,
 - opis sposobu zabezpieczenia zarejestrowanych danych podczas ich transmisji przed dostępem osób nieupoważnionych oraz przed ich zmianą i zniszczeniem,
 - opis sposobu połączenia (integracji) zarejestrowanych danych z zarejestrowanym obrazem pojazdu w celu uniemożliwienia ich zmiany,
 - opis sposobu rejestrowania danych przeznaczonych do transmisji do systemów ogólnodostępnych zawierają sumy kontrolne lub pieczęcie elektroniczne (ewentualnie podpisy elektroniczne) pozwalające potwierdzić przez przyrząd i przez oprogramowanie zewnętrzne współpracujące z przyrządem, że dane po transmisji nie uległy zmianie,
 - opis sposobu kontroli niezmienności przesłanych danych za pomocą przyrządu i za pomocą oprogramowania zewnętrznego współpracującego z przyrządem,
 - opis sposobu jednoznacznej identyfikacji oprogramowania zewnętrznego przeznaczonego do współpracy z przyrządem,
 - opis sposobu rejestracji danych przeznaczonych do przesyłania przez dostępne interfejsy do powszechnie dostępnych urządzeń informatycznych w zaszyfrowanej postaci,
 - opis sposobu potwierdzenia poprawności transmisji danych przesyłanych przez dostępne interfejsy do powszechnie dostępnych urządzeń informatycznych,

- opis możliwości usuwania z przyrządu zarejestrowanych danych,
 - opis rozwiązania technicznego zapewniającego możliwość usuwania danych pomiarowych z przyrządu wyłącznie po uzyskaniu przez przyrząd potwierdzenia poprawnej ich transmisji do systemów ogólnodostępnych, a operacja usunięcia danych z przyrządu jest zawsze rejestrowane w postaci dziennika zdarzeń zawierającego datę, czas i zakres usunięcia danych, datę i czas ich utworzenia oraz imię i nazwisko osoby dokonującej transmisji danych,
 - opis sposobu wykonania potwierdzenia sprawdzenia poprawności działania przyrządu przez wykonywanie każdorazowo przy uruchomieniu (oraz w dowolnym czasie w wyniku włączenia funkcji sprawdzania) testu prawidłowości działania urządzenia, którego działanie nie pozwala na wykonywanie pomiarów prędkości w przypadku braku potwierdzenia prawidłowości działania,
 - opis sposobu w jaki umożliwiona jest identyfikacja wersji i sum kontrolnych oprogramowania istotnego dla prawidłowego funkcjonowania przyrządu i jego charakterystyk metrologicznych, w tym opis sposobu wyznaczania sum kontrolnych oprogramowania metrologicznego wszystkich elementów składowych przyrządu oraz o zgodności zastosowanych algorytmów z § 3.2 oraz identyfikacja rodzaju i wersji systemu operacyjnego,
 - opis sposobu zabezpieczenia oprogramowania przed przypadkową i nieupoważnioną zmianą,
 - opis sposobu zabezpieczeń dostępu do wszystkich interfejsów przyrządu,
 - opis sposobu zabezpieczenia przyrządu i wszystkich jego elementów składowych za pomocą nałożenia cech zabezpieczających w celu uniemożliwienia dostępu do części przyrządu istotnych dla charakterystyk metrologicznych oraz do których naruszenie może spowodować błąd pomiaru lub spowodować błąd pomiaru wskutek zmiany konfiguracji.
- w zakresie konstrukcji i sposobu działania przyrządu w szczególności:
- oznaczenia nazwy i wersji przyrządu, przy zachowaniu zgodności danych zawartych w dokumentacji z danymi zawartymi we wniosku oraz z oznaczeniami egzemplarza przyrządu dostarczonego do badania,
 - opis sposobu działania i konstrukcji przyrządu,
 - opis wszystkich części składowych przyrządu,
 - opis wszystkich wersji oraz wszystkich trybów pracy przyrządu,
 - opis możliwych przyczyn wystąpienia błędów w działaniu przyrządu i opis komunikatów o wystąpieniu błędów,
 - opis sposobu i metody rejestracji zdarzeń przez przyrząd [np. zdarzeń rejestracji pomiarów, kasowania danych, rejestracji błędów, logowania, włączenia i wyłączenia przyrządu, transmisji danych, komunikatów i logów systemowych,
 - opis urządzeń dodatkowych, które mogą być połączone z przyrządem wraz z ich specyfikacją;

**INFORMACJE O PRZEBIEGU I ZAKRESIE BADAŃ PRZYRZĄDÓW DO POMIARU PRĘDKOŚCI
POJAZDÓW W KONTROLI RUCHU DROGOWEGO**

BADANIA METROLOGICZNE I ŚRODOWISKOWE

1. Opis przebiegu i metodyki badań

OBSZAR BADAŃ	SPOSÓB WERYFIKACJI WYMAGAŃ	OZNACZENIE PRZEPISÓW ZAWIERAJĄCYCH WYMAGANIA SZCZEGÓŁOWE
DOKUMENTACJA	Zapoznanie się z dokumentacją, analiza i sprawdzenie zgodności dokumentacji z zakresem zleconych do laboratorium badań, sprawdzenie typu przyrządu, wersji i sum kontrolnych identyfikujących przyrząd).	§1-§9, §12-§19, §21-§26
DOKUMENTACJA KONSTRUKCJA FUNKCJONALNOŚĆ MODUŁY DODATKOWE	Analiza dokumentacji technicznej (zasada działania przyrządu, zasada dokonywania pomiaru prędkości, analiza dokumentów konstrukcyjnych (jeśli dotyczy), analiza działania poszczególnych bloków wewnętrznych).	§1-§9, §12-§19, §21-§26
DOKUMENTACJA	Analiza dostarczonych przez wnioskodawcę sprawozdań z badań. (rodzaj przyrządu, który podlegał sprawdzeniu poprzez identyfikację przyrządu (numer fabryczny, wersja i suma kontrolna) sprawdzenie warunków w jakich był dokonywany pomiar prędkości podczas trwania narażenia i porównanie z wymaganiami rozporządzenia, kompletność badań).	§10-§11, §20-§26
DOKUMENTACJA KONSTRUKCJA FUNKCJONALNOŚĆ MODUŁY DODATKOWE	Sprawdzenie kompletności dostarczonego przyrządu pomiarowego. Przeprowadzenie uruchomienia przyrządu. Konfiguracja komunikacji z oprogramowaniem zewnętrznym dostarczonym przez wnioskodawcę.	§13
DOKUMENTACJA KONSTRUKCJA FUNKCJONALNOŚĆ MODUŁY DODATKOWE	Porównanie zapisów z dokumentacji i wykonanej analizy z przyrządem dostarczonym do badań. Określenie opcji działania przyrządu, możliwości przestawiania ustawień przyrządu i ocena ich wpływu na działanie przyrządu – porównanie z zapisami w dokumentacji, określenie rodzaju i zastosowanych zabezpieczeń konstrukcyjnych i programowych pod kątem funkcjonalności, określenie rodzaju wyprowadzeń oraz sposobu ich zabezpieczeń. Ocena wpływu parametrów charakterystyk promieniowania anteny na błędy pomiaru na podstawie analizy tych charakterystyk (dla przyrządów radarowych). Badanie kąta rozwarcia wiązki promieniowania laserowego (dla przyrządów laserowych).	§1-§9, §12-§19, §21-§26

DOKUMENTACJA KONSTRUKCJA FUNKCJONALNOŚĆ	Sprawdzenie dokumentacji symulatora (opis działania i dokumenty potwierdzające możliwość zastosowania symulatora do badań). Uruchomienie symulatora zgodnie z instrukcją obsługi (o ile ma zastosowanie).	
DOKUMENTACJA KONSTRUKCJA FUNKCJONALNOŚĆ	Weryfikacja pomiaru symulowanej prędkości w różnej konfiguracji sprawdzanego przyrządu.	§1-§9, §12-§19, §21-§26
DOKUMENTACJA KONSTRUKCJA FUNKCJONALNOŚĆ MODUŁY DODATKOWE	Badania metrologiczne: pomiar prędkości Porównanie wskazań przyrządu do pomiaru prędkości z wzorcami wykorzystywanymi w laboratorium GUM (min. 500 pomiarów).	§21.2, §22, § 23, § 28
KONSTRUKCJA FUNKCJONALNOŚĆ	Badania środowiskowe Zgodnie z instrukcją IB50-AUV.V oraz IB51-TH (PN-EN 60068-2-1:2009, PN-EN 60068-2-2:2009, PN-EN 60068-2-78:2013-11, PN-EN 60068-230:2008, PN-EN 60068-2-14:2009, PN-EN 60068-2-64:2008, PN-EN 60068-2-6:2008, PN-EN 60068-2-27:2009, PN-EN 60068-2-75:2015-01, PN-EN 60068-2-47:2005). Możliwość wykonywania badań w zewnętrznych akredytowanych laboratoriach.	§10-§11, §20-§26
DOKUMENTACJA	Sprawdzenie działania przyrządu zgodnie z instrukcją obsługi i wymaganiami rozporządzenia.	§26
DOKUMENTACJA	Opracowanie dokumentów końcowych, sprawozdań, opisów przeprowadzonych badań.	§1-27.

BADANIA OPROGRAMOWANIA

Badania oprogramowania przyrządów do pomiaru prędkości pojazdów w kontroli ruchu drogowego obejmują weryfikację wymagań związanych z zapewnieniem

- bezpieczeństwa, niezmienności i identyfikowalności oprogramowania przyrządu,
- bezpieczeństwa, niezmienności i odtwarzalności parametrów konfiguracyjnych odpowiedzialnych za prawidłową pracę przyrządu, w tym zachowanie poprawności pomiaru oraz bezpieczeństwa cyfrowego przyrządu,
- bezpieczeństwa, niezmienności, odtwarzalności i weryfikowalności wyników pomiarowych w postaci cyfrowej.

1. Opis przebiegu i metodyki badań

W celu zapewnienia sprawnej i rzetelnej realizacji badań oprogramowania przyrządów pomiarowych, GUM stosuje podział badań na następujące obszary merytoryczne

OBSZAR BADAŃ	SPOSÓB WERYFIKACJI WYMAGAŃ	OZNACZENIE PRZEPISÓW ZAWIERAJĄCYCH WYMAGANIA SZCZEGÓŁOWE BADAŃ
BADANIA BEZPIECZEŃSTWA OPROGRAMOWANIA (BBO)	Sprawdzenie bezpieczeństwa, niezmienności oraz identyfikowalności oprogramowania i konfiguracji przyrządu pomiarowego, mogące mieć wpływ na wiarygodność, rzetelność i bezpieczeństwo uzyskiwanych wyników pomiaru. Badania dotyczą całego oprogramowania (w tym jego konfiguracji) przyrządu, które bierze udział w procesie pomiaru i zapisu wyników pomiarowych, a także związanego z zapewnieniem bezpieczeństwa cyfrowego przyrządu i danych pomiarowych.	§ 3 pkt 2 § 12 § 13 ust. 1 § 13 ust. 2 § 14 ust. 1 § 14 ust. 2 § 24 ust. 1 § 24 ust. 2 punkty: 1, 2, 5, 7, 9, 11 § 26 ust. 1 pkt 1 § 26 ust. 1 pkt 2 § 26 ust. 1 pkt 3 § 26 ust.1 pkt 5 lit. c oraz d § 26 ust.1 pkt 5 lit. e § 26 ust.1 pkt 5 lit. g § 26 ust.1 pkt 5 lit. h

BADANIA BEZPIECZEŃSTWA DANYCH (BBD)	Sprawdzenie bezpieczeństwa, niezmienności, odtwarzalności i weryfikowalności zapisywanych w przyrządzie wyników pomiarowych w postaci cyfrowej, a także możliwości weryfikacji ich niezmienności po eksporcie z przyrządu pomiarowego. Badaniem objęte są również zagadnienia związane z zapewnieniem odtwarzalności zmian w wynikach pomiarów (np. usuwanie danych).	§ 9 ust. 1 § 9 ust. 3 § 9 ust. 5 § 9 ust. 6 § 9 ust. 8 § 26 ust.1 pkt 5 lit. f
BADANIA BEZPIECZEŃSTWA TRANSMISJI DANYCH (BBTD)		§ 26 ust.1 pkt 5 lit. f § 26 ust.1 pkt 5 lit. i
BADANIA BEZPIECZEŃSTWA TRANSMISJI DANYCH (BBTD) – INTERFEJSY I PROTOKOŁY KOMUNIKACYJNE PRZYRZĄDU	Sprawdzenie bezpieczeństwa dostępu do interfejsów komunikacyjnych w taki sposób, aby uniemożliwiały one wprowadzenie niedozwolonej ingerencji z oprogramowanie przyrządu pomiarowego, parametry konfiguracyjne przyrządu oraz rejestrowane w przyrządzie wyniki pomiarów.	§ 9 ust. 7 § 13 ust. 3
BADANIA BEZPIECZEŃSTWA TRANSMISJI DANYCH (BBTD) – TRANSMISJA DANYCH	Sprawdzenie bezpieczeństwa, niezmienności i weryfikowalności wysyłanych z przyrządu wyników pomiarowych, wraz z obsługą błędów transmisji.	§ 3 pkt 2 § 9 ust. 4 § 9 ust. 6 § 9 ust. 7 § 9 ust. 8

Sprawdzenia w poszczególnych obszarach badań obejmują:

	ZAGADNIENIE	SPOSÓB WERYFIKACJI WYMAGAŃ	OZNACZENIE PRZEPISÓW ZAWIERAJĄCYCH WYMAGANIA SZCZEGÓŁOWE
BADANIA BEZPIECZEŃSTWA OPROGRAMOWANIA			
1	Dokumentacja technicznokonstrukcyjna i instrukcja obsługi	Analiza dostarczonej dokumentacji technicznej przyrządu w celu stwierdzenia, czy zawiera wszystkie informacje umożliwiające przeprowadzenie badań (typ przyrządu, wersja i suma kontrolną identyfikująca przyrząd, opis funkcji przyrządu podlegających analizie i testom).	§ 24 ust. 1 § 24 ust. 2 pkt: 1, 2, 5, 7, 9, 11 § 26 ust. 1 pkt 1 § 26 ust. 1 pkt 2

2	Zgodność rozwiązań technicznokonstrukcyjnych z dostarczoną dokumentacją	Analiza dostarczonej dokumentacji technicznej przyrządu w celu stwierdzenia, czy opisane w niej moduły, funkcje, sterowanie, komunikacja, zabezpieczenia odpowiadają działaniu egzemplarza dostarczonego do badań. Badania weryfikujące poprawności opisu w dokumentacji sposobu działania elementów i funkcji przyrządu podlegających kontroli zleconej w badaniach.	§ 26 ust. 1 pkt 1 § 26 ust. 1 pkt 3
3	Ochrona oprogramowania cechami zabezpieczającymi	Sprawdzenie, czy cechy zabezpieczające i sposób ich nałożenia zapewniają niezmiennosc elementów przyrządu istotnych dla charakterystyk metrologicznych. Badania techniczne weryfikujące czy cechy zabezpieczające skutecznie zabezpieczają oprogramowanie przed przypadkowymi i nieupoważnionymi zmianami.	§ 26 ust.1 pkt 5 lit. e
4	Autotesty i dostępność funkcji testowych	Analiza dokumentacji opisującej zakres i sposoby wywołania wykonania autotestu przyrządu Badania techniczne weryfikujące autotest i potwierdzenie prawidłowości działania przyrządu.	§ 12 § 26 ust.1 pkt 5 lit. c oraz d

		Weryfikacja uniemożliwienia pomiarów prędkości w przypadku negatywnego wyniku autotestów.	
5	Identyfikacja wersji i sum kontrolnych oprogramowania	Badania techniczne sprawdzające <ul style="list-style-type: none"> - identyfikację modułów oprogramowania zainstalowanego w przyrządzie mogących mieć wpływ na poprawność realizacji pomiaru, zachowanie charakterystyk metrologicznych oraz bezpieczeństwo oprogramowania i konfiguracji przyrządu, - raportowanie przez przyrząd wersji i sum kontrolnych oprogramowania, - weryfikację zgodności cech identyfikacyjnych oprogramowania z dokumentacją. 	§ 3 pkt 2 § 13 ust. 1 § 26 ust.1 pkt 5 lit. g

6	Ochrona oprogramowania przed zmianą	<p>Analiza opisu sposobu zabezpieczenia oprogramowania i parametrów konfiguracyjnych przed przypadkowymi i zamierzonymi zmianami.</p> <p>Analiza wykazu chronionych parametrów konfiguracyjnych przyrządu</p> <p>Analiza opisu sposobu wyznaczania i porównania sumy kontrolnej (lub metod równorzędnych o analogicznej skuteczności) z wartością nominalną, wraz ze sposobem i ochroną przechowywania wartości nominalnej.</p> <p>Badania techniczne weryfikujące czy wyznaczana i weryfikowana przez przyrząd suma kontrolna obejmuje całe oprogramowanie związane z realizacją procedury pomiarowej, przetwarzaniem i transmisją danych przez interfejsy zewnętrzne przyrządu oraz komunikacje z użytkownikiem.</p> <p>Weryfikacja możliwości aktualizacji lub modyfikacji oprogramowania przyrządu, w tym systemu operacyjnego, oraz sposobu zabezpieczenia przed ww. zmianami.</p>	§ 13 ust. 2 § 26 ust.1 pkt 5 lit. h
7	Ochrona konfiguracji oprogramowania przed zmianą	<p>Weryfikacja wykazu parametrów chronionych wraz z opisem sposobu zabezpieczenia przed zmianą, sposobu i trybu programowania parametrów, miejsca ich przechowywania wraz ze sprawdzeniem poprawności działania zastosowanych zabezpieczeń.</p> <p>Analiza opisu sposobu przechowywania, zarządzania i zapewnienia poufności kluczy kryptograficznych.</p> <p>Weryfikacja czy parametry konfiguracyjne odpowiadające za działanie oprogramowania i zabezpieczenia przyrządu przechowywane są w pamięciach wewnętrznych przyrządu, czy można zidentyfikować pliki konfiguracyjne przyrządu, w których zdefiniowane są dane i parametry chronione przed zmianą przez użytkownika przyrządu.</p> <p>Sprawdzenie czy interfejs użytkownika przyrządu oraz protokoły komunikacyjne przyrządu nie umożliwiają dostępu do zmiany parametrów związanych z</p>	§ 13 ust. 2 § 26 ust.1 pkt 5 lit. h
		poprawnością realizacji pomiaru, bezpieczeństwa oprogramowania i przechowywania danych. Zmiany wymienianych parametrów powinny być możliwe wyłącznie po naruszeniu cech zabezpieczających przyrządu.	

8	Dostęp do części przyrządu istotnych dla charakterystyk metrologicznych	<p>Identyfikacja oprogramowania w przyrządzie, które nie ma wpływu na poprawność działania i konfigurację programu metrologicznego</p> <p>Weryfikacja czy przyrząd nie umożliwi modyfikacji oprogramowania metrologicznego zainstalowanego w urządzeniu i jego częściach bez naruszenia cech zabezpieczających.</p> <p>Sprawdzenie czy przyrząd nie umożliwi modyfikacji istotnej dla charakterystyk metrologicznych konfiguracji oprogramowania urządzenia bez naruszenia cech zabezpieczających.</p> <p>Sprawdzenie czy przyrząd ma zabezpieczony system operacyjny przed jego modyfikacją bez naruszenia cech zabezpieczających, przed zmianą konfiguracji.</p> <p>Sprawdzenie skuteczności zabezpieczeń przed możliwością modyfikacji oprogramowania bez naruszenia cech zabezpieczających dla wszystkich elementów składowych przyrządu i ich sterowników mogących spowodować błąd pomiaru.</p> <p>Sprawdzenie sposobu separacji oprogramowania metrologicznego od oprogramowania nie podlegającego prawnej ochronie (np. dodatkowego oprogramowania zewnętrznego).</p>	§ 14 ust. 1 § 14 ust. 2 § 26 ust.1 pkt 5 lit. e
BADANIA BEZPIECZEŃSTWA DANYCH			
9	Zabezpieczenie danych przed nieuprawnionym dostępem	<p>Analiza sposobu wykorzystania interfejsów i protokołów komunikacyjnych oraz możliwości nieuprawnionego dostępu, zmiany lub zniszczenia danych gromadzonych w przyrządzie w tym rejestrów zdarzeń za ich pośrednictwem.</p> <p>Sprawdzenie skuteczności funkcji zabezpieczających chronione dane. Badania techniczne weryfikujące odpowiednie dla wszystkich poziomów dostępu możliwości ingerencji przy pomocy interfejsu użytkownika, portów komunikacyjnych, interfejsów komunikacyjnych (w tym sieciowych i bezprzewodowych) bez naruszenia cech zabezpieczających.</p>	§ 3 pkt 2 § 9 ust. 3 § 26 ust.1 pkt 5 lit. f
10	Zabezpieczenie danych przed modyfikacją	<p>Analiza sposobu zabezpieczenia danych oraz sposobu oznaczenia danych uszkodzonych.</p> <p>Badania techniczne weryfikujące modyfikacje w plikach z pomiarów i poprawność działania opisanych w dokumentacji metod zabezpieczenia integralności danych. Sprawdzenie czy konstrukcja przyrządu nie pozwala na ingerencje w rejestrowane pliki.</p>	§ 3 pkt 2 § 9 ust. 3 § 9 ust. 5 § 9 ust. 6 § 26 ust.1 pkt 5 lit. f

11	Odtwarzalność danych wynikowych	<p>Analiza kompletności rekordu danych pomiarowych, zastosowanych metod zapewnienia autentyczności danych, funkcji oprogramowania umożliwiających odczyt danych, sposobu oznaczania danych zmodyfikowanych (nieautentycznych).</p> <p>Badania weryfikujące działania mechanizmów uwierzytelnienia danych poprzez potwierdzenie poprawnego odczytu zapisanych danych na nośniku w sposób umożliwiający identyfikację przyrządu pomiarowego, a w przypadku transmisji danych do systemów ogólnodostępnych potwierdzenie poprawnego działania funkcji oprogramowania umożliwiającego odtwarzanie i weryfikację integralności wyników pomiarowych.</p>	§ 9 ust. 1 § 9 ust. 3 § 26 ust.1 pkt 5 lit. f
12	Zabezpieczenie przed usunięciem lub zniszczeniem danych wynikowych	<p>Analiza sposobu zabezpieczenia danych przed nieuprawnionym usunięciem lub zniszczeniem</p> <p>Sprawdzenie poprawności działania zabezpieczeń chroniących przed przypadkowymi i nieupoważnionymi zmianami lub usunięciem zapisanych danych, oraz działaniem funkcji kasowania danych przez użytkownika. Potwierdzenie działania tych zabezpieczeń w każdej konfiguracji przyrządu na poziomie dostępu osób postronnych oraz wszystkich użytkowników poprzez interfejsy komunikacyjne dostępne bez naruszenia cech zabezpieczających. Potwierdzenie braku konfiguracji, funkcji i rozkazów umożliwiających niedozwolone działania.</p>	§ 9 ust. 3 § 26 ust.1 pkt 5 lit. f
13	Usuwanie danych i rejestracja kasowania danych w dzienniku zdarzeń	<p>Analiza mechanizmu usuwania danych z przyrządu.</p> <p>Analiza zawartości dziennika zdarzeń przyrządu i opisu rejestracji zdarzeń kasowania danych w dzienniku zdarzeń.</p> <p>Badania techniczne weryfikujące poprawność i działania i opisu mechanizmów usuwania danych z wynikami pomiarów z pamięci przyrządu po potwierdzeniu poprawnej ich transmisji do systemów ogólnodostępnych. Sprawdzenie czy zdarzenie usuwania danych z przyrządu jest każdorazowo rejestrowane w nieusuwalnym dzienniku zdarzeń oraz czy dziennik ten zawiera wszystkie niezbędne dane i możliwości jego odczytu.</p>	§ 9 ust. 8
BADANIA BEZPIECZEŃSTWA TRANSMISJI DANYCH			

14	Identyfikacja i funkcje interfejsów	<p>Identyfikacja dostępnych dla użytkownika interfejsy komunikacyjnych przyrządu.</p> <p>Analiza funkcji i komend wszystkich protokołów komunikacyjnych przyrządu i opisu ich działania, wraz z określeniem wpływu na sposób działania programu, parametry konfiguracyjne przyrządu i dane pomiarowe.</p> <p>Analiza zabezpieczeń działania oprogramowania, parametrów konfiguracyjnych i danych pomiarowych przed wpływem komend protokołów komunikacyjnych.</p>	<p>§ 3 pkt 1</p> <p>§ 13 ust. 3</p> <p>§ 26 ust.1 pkt 5 lit. i</p>
----	-------------------------------------	---	--

		<p>Badania techniczne weryfikujące funkcje protokołów komunikacyjnych i skuteczność zastosowanych zabezpieczeń.</p> <p>Sprawdzenie czy na dostępnych portach możliwe do zastosowania protokoły umożliwiają ingerencję w zawartość oprogramowania przyrządu, zmianę parametrów konfiguracyjnych, dostęp do zabezpieczeń systemu, kont i haseł użytkowników lub czy nie występują niezabezpieczone usługi umożliwiające ingerencję w dane zarejestrowane przez przyrząd.</p> <p>Weryfikacja kompletności informacji zawartych w dokumentacji i występowania niedozwolonych funkcjonalności.</p>	
15	Konfiguracja i zabezpieczenia interfejsów	<p>Analiza zabezpieczenia działania programu metrologicznego, parametrów konfiguracyjnych i danych pomiarowych przed niedozwolonym wpływem przez interfejs użytkownika.</p> <p>Weryfikacja wykazu komend protokołów komunikacyjnych przyrządu i opisu ich działania, wraz z określeniem wpływu na sposób działania programu, parametry konfiguracyjne przyrządu i dane pomiarowe.</p> <p>Analiza zabezpieczenia działania programu metrologicznego, parametrów konfiguracyjnych i danych pomiarowych przed wpływem komend protokołów komunikacyjnych.</p> <p>Sprawdzenie działania funkcji i poleceń protokołów komunikacyjnych każdego z interfejsów komunikacyjnych z opisem w dokumentacji przyrządu,</p> <p>Weryfikacja występowania niepożądanych komend i poleceń dla wszystkich dostępnych dla użytkownika protokołów komunikacyjnych</p> <p>Weryfikacja czy inne oprogramowanie poprzez interfejsy komunikacyjne nie może wpływać na poprawność działania i konfigurację programu metrologicznego przyrządu.</p>	<p>§ 3 pkt 1</p> <p>§ 13 ust. 3</p> <p>§ 26 ust.1 pkt 5 lit. i</p>

16	Sieci otwarte i sieci zamknięte	<p>Identyfikacja dostępnych dla użytkownika interfejsów komunikacyjnych przyrządu.</p> <p>Analiza opisuj złącz komunikacyjnych z wyszczególnieniem miejsc nałożenia cech zabezpieczających.</p> <p>Sprawdzenie czy przyrząd lub niektóre z jego interfejsów komunikacyjnych zostały przewidziane do pracy w sieciach otwartych i bezprzewodowych w technologiach takich jak GSM, Wi-Fi, Bluetooth, IrDA, komunikacji radiowej itp.</p> <p>Sprawdzenie zabezpieczeń zastosowanych dla komunikacji za pośrednictwem ww, rodzajów sieci telekomunikacyjnych.</p> <p>Sprawdzenie czy przyrząd lub część z jego interfejsów zostały przewidziane do pracy w sieciach zamkniętych. Dla komunikacji w sieciach zamkniętych sprawdzeniu</p>	<p>§ 3 pkt 1</p> <p>§ 13 ust. 3</p> <p>§ 26 ust.1 pkt 5 lit. i</p>
----	---------------------------------	---	--

		<p>podlega czy przewody komunikacyjne łączą bezpośrednio urządzenia pracujące w sieci zamkniętej, bez niezabezpieczonych dodatkowych złączy, przełączników, koncentratorów lub innych urządzeń pośredniczących oraz dostęp do przewodów sieciowych, złączy, portów komunikacyjnych pracujących w sieci zamkniętej został zabezpieczony mechanicznie przez nałożenie cech zabezpieczających.</p>	
17	Obsługa błędów transmisji	<p>Identyfikacja dostępnych dla użytkownika interfejsów komunikacyjnych przyrządu oraz komunikatów błędów transmisji wraz z opisem zabezpieczenia transmisji przed błędami przesyłania.</p> <p>Sprawdzenie dla każdego kanału transmisji danych na zewnątrz przyrządu oraz dla każdego bezprzewodowego interfejsu komunikacyjnego wykrywalności błędów transmisji.</p> <p>Sprawdzenie czy i w jaki sposób urządzenie na każdym z interfejsów zewnętrznych wykrywa błędy transmisji spowodowane brakiem i przerwaniem połączenia, przekłamaniami transmisji danych i odbiorem niepełnych pakietów.</p> <p>Sprawdzenie dla każdego z kanałów komunikacji czy oprogramowanie wysyłające i pobierające dane wykrywa błędy transmisji i czy zastosowano mechanizmy blokujące odczyt i dalsze przetwarzanie niepełnych lub przekłamanych danych pomiarowych.</p>	<p>§ 3 pkt 1</p> <p>§ 13 ust. 3</p> <p>§ 26 ust.1 pkt 5 lit. i</p>
18	Kompletność przesyłanych danych	<p>Identyfikacja pól rekordów danych przeznaczonych do transmisji.</p> <p>Sprawdzenie prawidłowości i kompletności zawartości danych przesłanych do urządzeń je odbierających.</p>	<p>§ 3 pkt 2</p> <p>§ 9 ust. 4</p> <p>§ 9 ust. 6</p> <p>§ 26 ust.1 pkt 5 lit. f</p>

19	Zabezpieczenie przed przypadkowymi i nieumyślnymi zmianami	<p>Analiza metody wykrywania błędów transmisji i obsługi błędów.</p> <p>Sprawdzenie czy wdrożono metody weryfikacji poprawności przesyłanych danych i wykrywania błędów transmisji danych oraz zabezpieczenia przed przypadkową zmianą i usunięciem danych.</p> <p>Sprawdzenie czy zarejestrowane dane w przyrządzie podczas ich transmisji są zabezpieczone przed dostępem osób nieupoważnionych.</p> <p>Sprawdzenie czy przyrząd, podczas transmisji zarejestrowanych danych, posiada skuteczne zabezpieczenie przed nieuprawnionym dostępem, kasowaniem albo zniszczeniem danych.</p>	<p>§ 3 pkt 2</p> <p>§ 9 ust. 4</p> <p>§ 9 ust. 6</p> <p>§ 26 ust.1 pkt 5 lit. f</p>
20	Integralność danych	<p>Analiza sposobu zabezpieczenia transmisji danych przed próbami celowej manipulacji danych.</p> <p>Sprawdzenie skuteczności i poprawności doboru metod zabezpieczania przesyłania danych pod względem możliwości celowej manipulacji przesyłanych danych.</p> <p>Sprawdzenie czy przyrząd mechanizm potwierdzenia przez przyrząd niezmienności danych, które zostały</p>	<p>§ 3 pkt 2</p> <p>§ 9 ust. 4</p> <p>§ 9 ust. 6</p> <p>§ 26 ust.1 pkt 5 lit. f</p>

		<p>przesłane do systemów ogólnodostępnych za pomocą wszystkich dostępnych w przyrządzie kanałów transmisyjnych działa prawidłowo.</p>	
21	Identyfikowalność transmitowanych danych	<p>Analiza sposobu zapewnienia uwierzytelnienia danych.</p> <p>Sprawdzenie skuteczności zastosowanych środków zapewniających uwierzytelnienie przesyłanych danych odniesienia każdego przesyłanego wyniku z konkretnym pomiarem, np. za pomocą oznaczenia czasu pomiaru i identyfikatora przyrządu dokonującego pomiar.</p> <p>Sprawdzenie poprawności jednoznacznej identyfikacji i uwierzytelnienia danych.</p> <p>Sprawdzenie działania potwierdzenia niezmienności danych, które zostały przesłane podczas transmisji danych do zewnętrznych systemów lub urządzeń przechowujących dane.</p> <p>Sprawdzenie czy zarejestrowane dane w przyrządzie, przeznaczone do transmisji z przyrządu do systemów ogólnodostępnych, zostały zabezpieczone przez sumy kontrolne lub pieczęcie elektroniczne.</p>	<p>§ 3 pkt 2</p> <p>§ 9 ust. 4</p> <p>§ 9 ust. 6</p> <p>§ 26 ust.1 pkt 5 lit. f</p>

22	Poufność kluczy kryptograficznych	<p>Analiza sposobu zarządzania bezpieczeństwem kluczy kryptograficznych i ochrony powiązanych z nimi informacji.</p> <p>Sprawdzenie czy transmisja danych do systemów ogólnodostępnych wykorzystuje się dodatkowo mechanizm podpisów elektronicznych osób dokonujących pomiarów działa prawidłowo i czy umożliwia ono dodatkowe potwierdzenie przez przyrząd i przez oprogramowanie zewnętrzne współpracujące z przyrządem niezmiennosc przesyłanych danych po ich transmisji do systemów zewnętrznych.</p>	<p>§ 3 pkt 2</p> <p>§ 9 ust. 4</p> <p>§ 9 ust. 6</p> <p>§ 26 ust.1 pkt 5 lit. f</p>
23	Odbieranie, weryfikacja i przetwarzanie przesyłanych danych pomiarowych	<p>Analiza opisu oprogramowania do odczytu, weryfikacji i przetwarzania odebranych danych pomiarowych.</p> <p>Analiza sposobu wykrywania uszkodzonych lub zmodyfikowanych danych.</p> <p>Sprawdzenie działania mechanizmów walidacji danych jednoznacznie oznaczających zmodyfikowane dane jako uszkodzone i niepodlegające dalszej obróbce.</p>	<p>§ 3 pkt 2</p> <p>§ 9 ust. 4</p> <p>§ 9 ust. 6</p> <p>§ 26 ust.1 pkt 5 lit. f</p>
24	Opóźnienie i dostępność transmisji	<p>Analiza sposobu obsługi sytuacji opóźnienia transmisji.</p> <p>Analiza obsługi sytuacji przerwania transmisji lub innych awarii związanych z dostępem do sieci komunikacyjnej.</p> <p>Sprawdzenie czy opóźnienie nie ma niedopuszczalnego wpływu na przebieg pomiaru.</p>	<p>§ 3 pkt 2</p> <p>§ 9 ust. 4</p> <p>§ 9 ust. 6</p> <p>§ 26 ust.1 pkt 5 lit. f</p>
25	Potwierdzenie i dziennik transmisji zdarzeń	<p>Identyfikacja oprogramowania do odczytu, weryfikacji i przetwarzania odebranych danych pomiarowych.</p> <p>Analiza sposobu wykrywania uszkodzonych lub zmodyfikowanych danych.</p> <p>Analiza procedury kasowania danych pomiarowych z przyrządu.</p>	<p>§ 9 ust. 7</p> <p>§ 9 ust. 8</p>
		<p>Analiza odczytu i obsługę dziennika zdarzeń.</p> <p>Sprawdzenie poprawności szyfrowania danych podczas transmisji poprzez interfejsy przyrządu.</p>	

BADANIA KOMPATYBILNOŚCI ELEKTROMAGNETYCZNEJ

1. Opis przebiegu i metodyki badań

Badania EMC to sprawdzanie wpływu jednych urządzeń elektrycznych na inne urządzenia elektryczne. Dzielimy je na pomiar emisji zakłóceń i badanie odporności na zakłócenia. Zakład Elektryczności i Promieniowania zajmuje się badaniem wpływu zakłóceń elektrycznych i magnetycznych na przyrządy pomiarowe. Opis przyrządów do wywołania zakłóceń, stanowisk badawczych i metod przeprowadzania testów zawarty jest w normach oznaczonych symbolem PN-EN. W ramach procesu zatwierdzenia typu przyrządów do pomiaru prędkości pojazdów w kontroli ruchu drogowego przeprowadzane są testy odpornościowe EMC zgodne ze wskazanymi poniżej normami.

	OPIS BADAŃ	SPOSÓB WERYFIKACJI WYMAGAŃ	OZNACZENIE PRZEPISÓW ZAWIERAJĄCYCH WYMAGANIA SZCZEGÓŁOWE
1	Oddziaływania na przyrząd promieniowanego pola elektromagnetycznego z falą nośną modulowaną amplitudowo, z głębokością modulacji 80% falą sinusoidalną o częstotliwości 1 kHz dla częstotliwości od 80 MHz do 6 GHz, przy amplitudzie natężenia pola elektrycznego 20 V/m, wartości błędów wskazania przyrządu nie przekraczają wartości błędów granicznych dopuszczalnych.	PN-EN 61000-4-3 - Kompatybilność elektromagnetyczna (EMC) -- Część 4-3: Metody badań i pomiarów -- Badanie odporności na promieniowane pole elektromagnetyczne o częstotliwości radiowej PN-EN 61000-4-20 - Kompatybilność elektromagnetyczna (EMC) -- Część 4-20: Metody badań i pomiarów -- Badanie emisji i odporności w falowodach z poprzeczną falą elektromagnetyczną (TEM)	§26 ust.1 pkt. 12a

2	<p>Oddziaływania na przyrząd zaburzeń przewodzonych, niesymetrycznych, indukowanych przez pole elektromagnetyczne z falą nośną modulowaną amplitudowo, z głębokością modulacji 80% falą sinusoidalną o częstotliwości 1 kHz dla częstotliwości od 150 kHz do 80 MHz, przy amplitudzie napięcia 20 V, na przyłączach:</p> <p>zasilania z sieci 230 V AC i uziemienia lub zerowania ochronnego, sygnałowych i sterujących, wartości błędów wskazania przyrządu nie przekraczają wartości błędów granicznych dopuszczalnych.</p>	<p>PN-EN 61000-4-6 - Kompatybilność elektromagnetyczna (EMC) -- Część 4-6: Metody badań i pomiarów -- Odporność na zaburzenia przewodzone, indukowane przez pola o częstotliwości radiowej</p>	<p>§26 ust. 1 pkt. 12b</p>
3	<p>Oddziaływania na przyrząd wyładowań elektrostatycznych o wartości napięcia probierczego:</p> <p>a) 6 kV – dla wyładowania kontaktowego, b) 8 kV – dla wyładowania w powietrzu</p> <p>– wartości błędów wskazania przyrządu nie przekraczają wartości błędów granicznych dopuszczalnych).</p>	<p>PN-EN 61000-4-2 - Kompatybilność elektromagnetyczna (EMC) -- Część 4-2: Metody badań i pomiarów -- Badanie odporności na wyładowania elektrostatyczne</p>	<p>§26 ust. 1 pkt. 13</p>
4	<p>Oddziaływania na przyrząd serii szybkich elektrycznych stanów przejściowych o polaryzacji dodatniej i ujemnej, czasie trwania impulsu 50 ns i czasie jego narastania 5 ns, o wartości szczytowej napięcia:</p> <p>a) 1 kV – na przyłączy zasilania z sieci 230 V AC i uziemienia lub zerowania ochronnego, b) 0,5 kV – na przyłączach sygnałowych i sterujących – wartości błędów wskazania przyrządu nie przekraczają wartości błędów granicznych dopuszczalnych.</p>	<p>PN-EN 61000-4-4 - Kompatybilność elektromagnetyczna (EMC) -- Część 4-4: Metody badań i pomiarów -- Badanie odporności na serie szybkich elektrycznych stanów przejściowych,</p>	<p>§26.1 pkt. 14</p>
5	<p>Oddziaływania na przyłączy zasilania DC przyrządu, zasilanego z instalacji elektrycznej pojazdu, impulsów testowych o wartościach:</p> <p>a) + 112 V, + 10 V, – 220 V, + 150 V – w przypadku instalacji elektrycznej o napięciu nominalnym 12 V DC, b) + 112 V, + 20 V, – 300 V, + 300 V – w przypadku instalacji elektrycznej o napięciu nominalnym 24 V DC</p>	<p>Wg. norm ISO 7637-2 – Road vehicles - Electrical disturbance from conducting and coupling</p>	<p>§26.1 pkt. 14a</p>
6	<p>Opracowanie dokumentów końcowych, sprawozdań, opisów przeprowadzonych badań.</p>	<p>Wg odpowiedniej normy</p>	