Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej Nr 59

L Międzyuczelniana Konferencja Metrologów

MKM 2018

Szczecin - Kopenhaga, 10-12 września 2018

doi: 10.32016/1.59.30

OCHRONA OPROGRAMOWANIA METROLOGICZNEGO

Michał MOSIĄDZ, Janusz SOBIECH, Jacek WÓJCIK

Główny Urząd Miar, Zakład Metrologii Interdyscyplinarnej
tel.: (+48) 22 681 93 93 e-mail: zmi@gum.gov.pl

Streszczenie: Podstawowym celem metrologii jest zapewnienie rzetelności i wiarygodności pomiarów. Nowoczesne technologie ICT znajdują powszechne zastosowanie w przyrządach pomiarowych. Konieczne jest określenie zasad ich stosowania, aby nie utracić podstawowych wartości procesu pomiarowego – powtarzalności, wiarygodności i odtwarzalności – definiujących jakość procesu pomiarowego. W pracy dokonano przeglądu regulacji dotyczących technologii ICT w przyrządach pomiarowych, poddano dyskusji ich zastosowanie w przykładowych rozwiązaniach technicznych oraz znaczenie dla bezpieczeństwa pomiaru.

Słowa kluczowe: cyfryzacja, ICT, bezpieczeństwo, jakość pomiaru.

1. METROLOGIA A BEZPIECZEŃSTWO IT

Podstawową cechą pomiaru jest wiarygodność wyniku. Spełnienie oczekiwań w tym zakresie jest warunkowane przez kontrolę środowiska pomiarowego, powtarzalność przebiegu procesu pomiarowego oraz zapewnienie odtwarzalności i bezpiecznego przetwarzania wyników pomiarowych. Wskutek cyfryzacji przyrządów pomiarowych, niewystarczające okazują się dotychczasowe rozwiązania związane z kontrolą warunków środowiskowych, okresowym serwisowaniem i sprawdzaniem działania układów pomiarowych, czy tradycyjne zarządzanie przetwarzaniem danych. Zasady zaufania oparte na doświadczeniu i wiedzy pracowników są zastępowane przez wytyczne tworzące zaufanie dla cyfrowego przetwarzania danych. Nowoczesne środowisko pomiarowe składa się nie tylko z warunków środowiskowych kontrolowanych automatycznie, ale również z cyfrowych przyrządów pomiarowych wraz z oprzyrządowaniem, za których poprawność działania odpowiada oprogramowanie. Bezpieczeństwo danych cyfrowych gwarantowane jest w szczególności metodami kryptograficznymi. Niezbędne zarządzanie wersjami i zmianami oprogramowania odbywa się z wykorzystaniem narzędzi informatycznych.

Potrzeba zapewnienia wysokiej jakości pomiaru w świecie technologii ICT została dostrzeżona przez środowisko metrologiczne i znalazła wyraz w regulacjach dotyczących przyrządów pomiarowych stosowanych w rozliczeniach handlowych, pomiarach przemysłowych czy pracy laboratoryjnej. Wśród regulacji należy wyszczególnić: Dyrektywę MID [2], Dyrektywę NAWI [1], OIML D31 [3], przewodnik WELMEC 7.2 [6], normy branżowe dotyczące urządzeń pomiarowych (np. dla wag nieautomatycznych PN-EN 45501), przepisy dotyczące wymagań technicznych dla poszczególnych rodzajów przyrządów pomiarowych (np. przyrządów do pomiaru prędkości pojazdów w ruchu drogowym).

Organizacje odpowiedzialne za nadzorowanie i promowanie jakości w pracy laboratoriów badawczo-pomiarowych (np. Polskie Centrum Akredytacji, Klub Polskich Laboratoriów Badawczych POLLAB) zwracają uwagę na kwestie związane z wpływem oprogramowania, które stanowi integralną część przyrządu pomiarowego na jakość świadczonych usług. Znajduje to odzwierciedlenie zwłaszcza w „Ogólnych wymaganiach dotyczących kompetencji laboratoriów badawczych i wzorcujących" (PN-EN 17025 [5]).

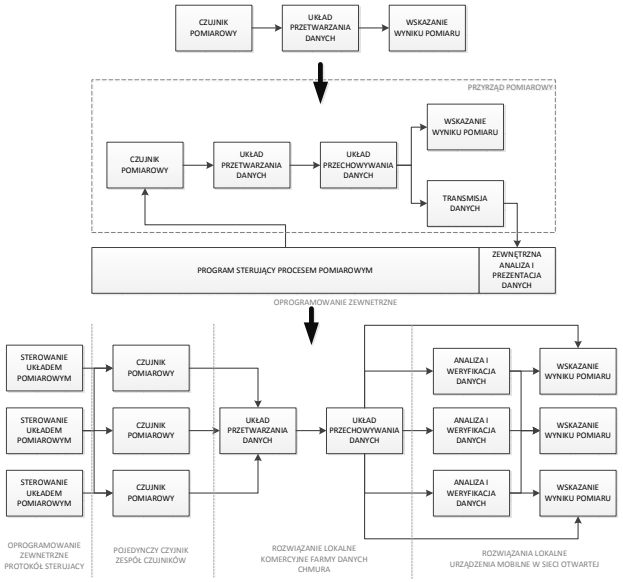
Elementami rozwiązań ICT determinującymi jakość realizowanych pomiarów są m.in.:
– stabilność wersji oprogramowania oraz środowiska software'owego (w tym konfiguracji przyrządu);
– bezpieczeństwo i odtwarzalność przetwarzania danych;
– bezpieczeństwo i powtarzalność przebiegu procesu pomiarowego.

Za spełnienie tych warunków jakości pomiaru odpowiedzialne są następujące elementy działania układu pomiarowego:
– oprogramowanie układu pomiarowego;
– układ przetwarzania i przechowywania danych;
– elementy programowe i sprzętowe odpowiedzialne za transmisję danych;
– moduły prezentacji danych i graficznego interfejsu użytkownika.

2. OCHRONA ŚRODOWISKA POMIAROWEGO

Podstawowymi elementami układów pomiarowych są: czujnik pomiarowy, układ przetwarzania oraz urządzenie wskazujące wynik. Wraz z postępem techniki, budowa przyrządu pomiarowego została rozszerzona o elementy odpowiedzialne za przechowywanie danych pomiarowych, komunikację zewnętrzną i oprogramowanie sterujące tymi funkcjami. Dzisiejsze przyrządy pomiarowe zawierają też funkcje niemetrologiczne, realizowane przez program sterujący lub przez oprogramowanie dodatkowe, osadzone na wspólnej platformie systemowej, które współużytkują zasoby sprzętowe i systemowe, procesy i sterowniki. Za wybrane funkcje przyrządu pomiarowego odpowiedzialne jest współpracujące z nim oprogramowanie zewnętrzne – najczęściej przeznaczone do prezentacji i weryfikacji danych albo zdalnego sterowania przyrządem,

czy przechowywania wyników. Rozwiązania z zakresu urządzeń rozproszonych oraz technologii chmurowych powodują, że zatarciu ulega granica przyrządu pomiarowego jakim dotąd była jego obudowa. Przyrząd pomiarowy może dziś zostać zdefiniowany jako system rozproszonych urządzeń cyfrowych i oprogramowania pracujących w architekturze otwartej. Rozwiązania zapewniające wiarygodność pomiaru uległy przekształceniu od rozwiązań fizycznych i sprzętowych, ku zabezpieczeniom cyfrowym. Przepływy danych i zależności pomiędzy poszczególnymi modułami oprogramowania mogą być czynnikami krytycznymi dla jakości i poprawności pomiaru.
Poglądowo zmiany konstrukcji i rozumienia przyrządów pomiarowych ilustruje rysunek 1.

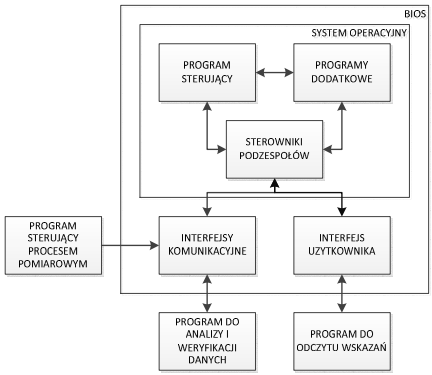


Rys. 1. Rozwój konstrukcji przyrządów pomiarowych

2.1. Ochrona oprogramowania

We wczesnych etapach cyfryzacji przyrządów pomiarowych, oprogramowanie sterujące umieszczone było w układzie pamięci stałej i stanowiło zamiennik mechanicznych bądź elektrycznych elementów sterujących. Jego wartością dodaną była szybkość działania, możliwość automatycznego sterowania procesami decyzyjnymi oraz uproszczenie konstrukcji przyrządu. Te same elementy sprzętowe mogły realizować różne funkcje, zależnie od zainstalowanego oprogramowania. Wówczas stworzono pierwsze regulacje związane z bezpieczeństwem IT przyrządów pomiarowych. Postęp techniki komputerowej dał możliwość wykorzystania komputerów do sterowania złożonymi procesami pomiarowymi. Dzisiaj mogą być to również aplikacje pracujące na urządzeniach mobilnych, komunikujące się z innymi elementami układu pomiarowego bezprzewodowo lub za pomocą sieci otwartych, przetwarzające dane w chmurze i składujące je na zewnętrznych, komercyjnych zasobach pamięci. Od pierwszego zastosowania komputerów do rejestracji sygnału pomiarowego zaszły kolosalne zmiany, jednak istota problemów została ta sama. Ze względu na współzależności funkcjonalne i konstrukcyjne pomiędzy elementami oprogramowania przyrządu pomiarowego ochrona nie może być ograniczona do oprogramowania sterującego lub czujnika pomiarowego. Środowisko programowe działania przyrządów pomiarowych ilustruje rysunek 2.

Współczesne przyrządy pomiarowe pracują pod kontrolą współpracujących ze sobą modułów i warstw oprogramowania. Jest to ściśle związane z warstwową strukturą oprogramowania systemów komputerowych. Technika komputerowa wymusza stosowanie różnych rodzajów struktur (warstwowej, modularnej, z jądrem) nie tylko w komputerach, ale również przyrządach mikrokontrolerowych, w których obecny jest system operacyjny (najczęściej Linux, mobilne wersje Windowsa i rozwiązania własne producentów). W urządzeniach tych podobnie jak w komputerach stosowany jest bootloader i niezależne sterowniki podzespołów (np. wyświetlaczy, interfejsów komunikacyjnych).



Rys. 2. Oprogramowanie przyrządów pomiarowych

Nadzór metrologiczny nie może sprowadzać się wyłącznie do ochrony głównego programu sterującego realizującego pomiar, ani oprogramowania czujnika pomiarowego. Takie ograniczenie dawałoby możliwość przekłamania wskazań przyrządu pomimo rejestracji poprawnego sygnału z czujnika pomiarowego czy transmisję niewiarygodnych danych do systemów zewnętrznych. Dlatego zarówno regulacje dotyczące przyrządów pomiarowych podlegających prawnej kontroli metrologicznej [2] [6] [3], jak i normy dotyczące jakości pracy laboratoriów pomiarowych [5], wskazują podejście holistyczne do oprogramowania infrastruktury pomiarowej obejmując ochronę wszystkich modułów i warstw oprogramowania mogących mieć wpływ na poprawność uzyskanych wyników.

2.2. Bezpieczeństwo oprogramowania

Głównymi założeniami ochrony oprogramowania metrologicznego są:
– zapewnienie wiarygodności uzyskanych wyników;
– zapewnienie powtarzalności procedury pomiarowej;
– zapewnienie bezpieczeństwa pomiaru.

Oprogramowanie przyrządu powinno zapewnić niezmienność i odtwarzalność przechowywanych wyników pomiarowych. Dostęp do jego zmiany może doprowadzić do wprowadzenia funkcjonalności dających możliwość nieuprawnionej ingerencji w dane lub ich utratę.

Pierwotne zasady ochrony oprogramowania metrologicznego definiowano dla tradycyjnych przyrządów pomiarowych (typu P [6]) o architekturze zamkniętej. W tego typu przyrządach stosowane oprogramowanie instalowane było w pamięci typu EPROM, a jego bezpieczeństwo gwarantowały rozwiązania sprzętowe. Aktualnie powszechnie stosuje się układy mikroprocesorowe z pamięcią Flash i z zabezpieczeniami umożliwiającymi uzyskanie podobnego stopnia niezmienności wgranego oprogramowania. Niezbędność serwisowej reinstalacji oprogramowania, bądź rynkowa potrzeba upgrade'ów

do nowszej wersji powoduje konieczność znalezienia innych zabezpieczeń. Są one realizowane w oparciu o kontrolę oprogramowania przez niezmienny moduł bootloadera czy BIOSu, kryptograficzne uwiarygodnienie uprawnionego użytkownika oraz nadzór nad narzędziami autoryzacyjnymi. Rozwiązania takie muszą być oparte o system jakości i kontroli produkcji urządzeń (dostępu do plików aktualizacji i poziomu administratora przyrządu). Inną kwestią są przyrządy o konstrukcji wykorzystującej oprogramowanie modułowe i o architekturze warstwowej. W przypadku stosowania podzespołów powszechnie dostępnych np. interfejsów we/wy, wyświetlaczy itp., nawet producent przyrządu nie ma wpływu na wprowadzenie nowych wersji sterowników sprzętowych i musi polegać na deklaracji kompatybilności ich wytwórcy. Powoduje to wyzwania w zakresie zarządzalności wersjami oprogramowania przyrządu, a także ryzyko zaburzenia cyklu pomiarowego. Błędy kompatybilności podzespołów, współpracy OS, oprócz luk w bezpieczeństwie przyrządu mogą prowadzić do niejednorodności interwałów czasowych punktów pomiarowych, braku powtarzalności procedury pomiarowej i zmiany środowiska pracy oprogramowania.

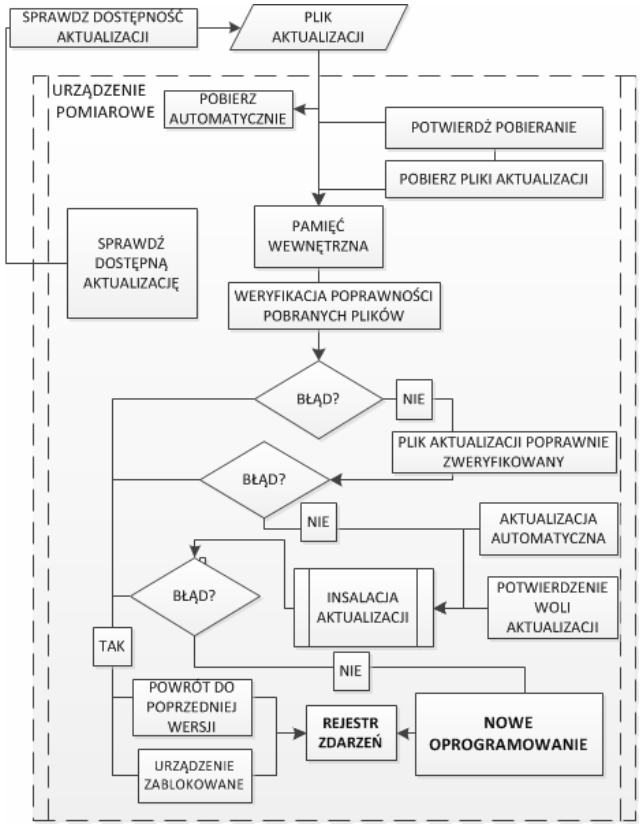
Ważnym aspektem jest stabilność oprogramowania. W złożonych instalacjach pomiarowych wykorzystujących zjawiska kriogeniczne, warunki próżniowe, generujące silne pola magnetyczne [4], zaburzenie priorytetyzacji przerwań, kompatybilności układów automatyki czy błędy komunikacji między elementami układu pomiarowego mogą doprowadzić do uszkodzenia unikatowej aparatury pomiarowej lub zagrożenia dla pracowników wskutek utraty kontroli nad przebiegającymi procesami. Oprócz stosowanych zabezpieczeń oraz regulacji dotyczących przyrządów podlegających prawnemu nadzorowi metrologicznemu, wskazane jest wdrożenie w laboratoriach pomiarowych zbioru „dobrych praktyk" w zakresie zarządzania oprogramowaniem, obejmujących:
– cykliczną identyfikację stosowanych wersji oprogramowania, przy czym oznaczenie wersji stosowane przez producenta często nie zapewnia identyczności oprogramowania (proponowane jest wprowadzenie mechanizmów weryfikacji ich sum kontrolnych);
– walidację zmian oprogramowania;
– konserwację środowiska programowego (w tym systemu operacyjnego, BIOSu itp.) poprzez weryfikację ustawień ich parametrów konfiguracyjnych, itp.;
– wprowadzenie ograniczeń w stosowaniu przez komputery sterujące innego oprogramowania, mogącego zaburzyć wartości rejestrów systemowych lub doprowadzić do utraty stabilności oprogramowania sterującego procesem pomiarowym. Dla programowalnych układów pomiarowych, wykorzystujących oprogramowanie własne użytkowników, wskazane jest zawarcie w nim procedur autoweryfikacji, wyznaczających sumę kontrolną z zawartości pamięci przechowującej kod wykonywalny programu (np. SHA, MD5) i porównywanie ich z wartością nominalną przechowywaną w odrębnej pamięci stałej.
Odrębnym zagadnieniem jest zapewnienie niezmienności i wiarygodności oprogramowania przeznaczonego do przetwarzania.

2.3. Aktualizacja oprogramowania i zarzadzanie wersjami

Współczesna technika wymusza potrzebę aktualizacji oprogramowania. W urządzeniach pomiarowych nie może ona przebiegać automatycznie, a w systemach wbudowanych system operacyjny i sterowniki znajdują się pod pełną kontrolą użytkownika. Ze względu na stosowanie zamkniętej architektury systemu przyrządu zmiana oprogramowania jest dokonywana wyłącznie poprzez metody sprzętowe (wymiana układów elektronicznych) lub z wykorzystaniem niejawnych ograniczeń dostępu (hasła do kont serwisowych, narzędzia autoryzacyjne i pliki dostępne tylko dla producenta itp.). Zmiana oprogramowania możliwa jest wyłącznie po zapewnieniu dostępu lokalnego do przyrządu pomiarowego i użytkownik systemu może ją kontrolować. Urządzenie musi trwale rejestrować aktualizację, a także dokonywać walidacji zainstalowanego oprogramowania. Zmiana oprogramowania przyrządów o architekturze zamkniętej wymaga uzyskania dostępu do tej funkcji. Standardowo stosowane rozwiązania obejmują:
– konieczność uzyskania dostępu do konta o uprawnieniach umożliwiający aktualizację oprogramowania;
– uzyskanie dostępu do plików aktualizacyjnych;
– rejestrację i odtwarzalność wprowadzonych zmian.
Aktualizacja oprogramowania nie może odbyć się bez zgody użytkownika i zazwyczaj wymaga dostępu lokalnego do przyrządu. W przypadku aktualizacji zdalnej, wg zasad opracowanych przez międzynarodowe organizacje metrologiczne [6] [3] wymagana jest zgoda użytkownika. Niezbędny jest też dostęp do informacji identyfikujących stosowaną w przyrządzie wersję oprogramowania (wymagania: P2, U2 [6]) oraz weryfikacja niezmienności (P5, P6, U5, U6 [6]). Zalecane jest stosowanie silnych haseł lub rozwiązań opartych o kryptografię w dostępie do konta o podwyższonych uprawnieniach. Należy pamiętać, że kluczowym dla bezpieczeństwa oprogramowania jest nadzór nad narzędziami umożliwiającymi aktualizację oprogramowania oraz zapewnienie kontroli nad dostępem do plików aktualizacyjnych, a także rejestracja i odtwarzalność historii zmian oprogramowania w niekasowalnym, zabezpieczonym rejestrze zdarzeń.

W zakresie aktualizacji oprogramowania dopuszczalne są dwie sytuacje:
– aktualizacji do innej wersji dopuszczonej do stosowania;
– reinstalacji oprogramowania tej samej wersji w celach serwisowych.
W pierwszym przypadku predefiniowanie możliwych do stosowania wersji programu pozwala na wbudowanie mechanizmu kontrolującego sumę kontrolną. Algorytm zawarty w bootloaderze zapewnia weryfikację zgodności sumy kontrolnej oprogramowania z zapisaną w pamięci niezmiennej przyrządu blokując możliwość aktualizacji w przypadku niezgodności. Przy potrzebie aktualizacji do wersji nieprzewidzianej podczas produkcji przyrządu, konieczne jest wgranie w przyrządzie, przez osoby uprawnione, cyfrowego certyfikatu dla nowego oprogramowania. Rozwiązania takie powinny być wsparte odpowiednimi procedurami zarzadzania dostępem do narzędzi autoryzacyjnych i certyfikatów producenta. Optymalny algorytm procesu aktualizacji oprogramowania ilustruje rysunek 3.

Konieczne jest, aby krytycznie odpowiedzialna za ochronę i kontrolę aktualizacji część oprogramowania była niezmienna (zawarta w układach lub obszarach pamięci niekasowalnej), tak aby uniemożliwić instalację niezatwierdzonego oprogramowania, które nie spełnia wymagań jakości i bezpieczeństwa procesu pomiarowego.



Rys. 3. Mechanizm kontroli aktualizacji oprogramowania[6]

2.4. Ochrona konfiguracji przyrządu

W zabezpieczeniu oprogramowania metrologicznego konieczne jest zapewnienie skuteczności jego ochrony. W przyrządach typu P [6] stosowana jest ochrona sprzętowa. Jednak nowoczesne rozwiązania przyrządów typu U [6] oparte są o uniwersalne układy mikroprocesorowe, których praca kontrolowana jest przez systemy operacyjne. Wówczas bezpieczeństwo przyrządu zależy od parametrów konfiguracji OS, uprawnień użytkowników oraz ustawień BIOSu. Podstawowym zabezpieczeniem jest ograniczenie dostępu do uruchamiania przyrządu z zewnętrznych nośników (bądź lokalizacji sieciowych). W przyrządach komputerowych wskazane jest zabezpieczenie BIOSu odpowiednio silnym hasłem i ograniczenie dostępu do zawierającego go układu scalonego oraz dostępu do przejścia w tryb komend i zapewnienie automatycznego startu programu metrologicznego.

Odpowiednio skonfigurowana ochrona przyrządów uniemożliwia dostęp do systemu operacyjnego poprzez wyjście poza interfejs programu metrologicznego (np. przez jego zamknięcie, zminimalizowanie itp.) lub w przypadku sytuacji awaryjnej (błędu procesu metrologicznego lub awarii OS). Zakres ograniczeń jest zależny od specyfiki zastosowanego systemu operacyjnego.

W systemach otwartych, osadzonych na przyrządach typu U [6], ochrona oprogramowania metrologicznego i konfiguracja systemu operacyjnego są zagadnieniami dość złożonymi, które wymagają zawansowanej znajomości wdrażanego rozwiązania urządzenia pomiarowego. W szczególności należy uwzględnić konfigurację praw dostępu do poszczególnych zasobów zawierających dane i oprogramowanie pomiarowe, pliki systemowe, sterowniki, biblioteki oraz wartości parametrów konfiguracyjnych systemu, rejestrów itd.. Krytyczne dla procesu pomiarowego zasoby (wartości parametrów konfiguracyjnych, wątków, procesów, kont użytkowników, systemu przerwań) muszą być chronione przed zmianami na równi z metrologicznym oprogramowaniem. Oprócz ograniczeń praw dostępu ważna jest też odtwarzalność modyfikacji (logi), weryfikacja sum kontrolnych zasobów pamięci stałej i operacyjnej oraz innych zasobów systemowych [6] [3].

3. WNIOSKI KOŃCOWE

Rozwój technologii sprawił, że dawne metody zapewnienia rzetelności pomiaru są niewystarczające. W przyrządach pomiarowych stosowanie są teleinformatycznych metody zabezpieczeń oprogramowania i przetwarzania oraz ochrony danych. Dodatkowo w metrologii istotne jest zapewnienie należytej ochrony środowiska pomiarowego zgodnie z aktualnie obowiązującymi standardami.

4. BIBLIOGRAFIA

1. Dyrektywa Parlamentu Europejskiego i Rady 2014/31/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku wag nieautomatycznych.
2. Dyrektywa Parlamentu Europejskiego i Rady 2014/32/UE z dnia 26 lutego 2014 r. w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do udostępniania na rynku przyrządów pomiarowych.
3. General requirements for software controlled measuring instruments, OIML D 31, 2008 (E).
4. Mosiądz M., Orzepowski M., Zastosowanie kriogenicznego komparatora prądowego do przekazywania jednostki miary rezystancji, „Pomiary Automatyka Kontrola" 2007, nr 9, s. 19–22.
5. Ogólne wymagania dotyczące kompetencji laboratoriów badawczych i wzorcujących, PN-EN ISO/IEC 17025:2018-02.
6. WELMEC 7.2, 2015: Software Guide (Measuring Instruments Directive 2014/32/EU), European Cooperation in Legal Metrology.

PROTECTION OF METROLOGICAL SOFTWARE

One of the basic objectives of metrology is to ensure the reliability and validity of measurement results. Modern ICT technologies are widely used in measuring instruments. It became necessary to determine rules for their application. In order not to lose the basic value of the measurement process – repeatability, reliability and reproducibility – defining the quality of the measurement process. This work reviews regulations concerning ICT in measuring instruments. Their applications in exemplary innovative technical solutions have been discussed. The importance for the security of the measurement process and measurement results is presented.

Keywords: digitization, ICT, security, measurement quality.