Проведено аналіз нормативної бази з випробування програмного забезпечення (ПЗ) для засобів вимірювальної техніки (ЗВТ) на національному рівні з метою встановлення її придатності для здійснення оцінювання відповідності. Здійснено порівняння загальних вимог національних нормативних документів та документів міжнародних і регіональних організацій законодавчої метрології OIML та WELMEC. Зокрема стосовно придатності ПЗ до застосування та захисту від несанкціонованого втручання. Встановлено, що чинний національний стандарт містить лише загальні вимоги щодо захисту ПЗ та не визначає методології проведення випробувань ПЗ. Це важливо, оскільки ЗВТ, призначені для застосування у сфері законодавчо регульованої метрології, повинні проходити процедуру оцінювання відповідності вимогам технічних регламентів.

Визначено основні відмінності та встановлені необхідні елементи для досягнення презумпції відповідності ПЗ суттєвим вимогам технічних регламентів під час оцінювання відповідності ЗВТ. Оцінено вимоги нормативних документів стосовно придатності до застосування та захисту від несанкціонованого втручання. Для конкретизації вимог до ПЗ і забезпечення виконання вимог методики випробувань ПЗ встановлено необхідність додаткового використання вимог документів OIML D 31 і WELMEC 7.2. Доведена потреба перегляду чинного національного стандарту щодо випробування ПЗ для ЗВТ. Встановлений та досліджений алгоритм проведення випробувань ПЗ ЗВТ з метою оцінки відповідності. Алгоритм враховує вимоги міжнародних стандартів щодо життєвого циклу ПЗ і щодо системи якості під час розробки ПЗ. Це дозволить врахувати всі елементи, необхідні для досягнення презумпції відповідності ПЗ суттєвим вимогам технічних регламентів

Ключові слова: програмне забезпечення, засіб вимірювальної техніки, випробування, оцінка відповідності, технічний регламент

UDC 389:14:621.317:354
DOI: 10.15587/1729-4061.2019.154352

TESTING OF MEASUREMENT INSTRUMENT SOFTWARE WITH THE PURPOSE OF CONFORMITY ASSESSMENT

O. Velychko
Doctor of Technical Sciences, Professor, Director*
V. Gaman
Head of Laboratory*
T. Gordiyenko
Doctor of Technical Sciences,
Associate Professor, Head of Department
Department of Standardization, Conformity Assessment and Educational Measurements**
E-mail: t_gord@hotmail.com
O. Hrabovskyi
PhD, Associate Professor, Director
Educational and Scientific Institute of Metrology, Automation, Intellectual Technologies and Electronics**
*Scientific and Production Institute of Electromagnetic Measurements
State Enterprise "All-Ukrainian State Scientific and Production Centre for Standardization, Metrology, Certification and Protection of Consumer", (SE "Ukrmetrteststandard")
Metrolohychna str., 4, Kyiv, Ukraine, 03143
**Odessa State Academy of Technical Regulation and Quality
Kovalska str., 15, Odessa, Ukraine, 65020

1. Introduction

Specialized software for measuring instruments (MI) plays an increasingly important role under the conditions of almost universal use of information technologies (IT). In accordance with the Law of Ukraine "On metrology and metrological activity", MI, intended for use in the field of legal metrology, must undergo conformity assessment procedure in accordance with requirements of technical regulations (TR).

The conformity assessment is a process of proving that the substantive requirements of the TR relating to the MI have been met. The following essential requirements that apply in one way or another to the software during MI conformity assessment are: suitability for use and protection from unauthorized interference.

According to national legislation, lists of national standards compliance with which, in particular, provides a presumption of compliance for the MI to the essential requirements of the TR are formed. Therefore, it is currently relevant to analyze the state of the normative framework for software testing of the MI and to develop approaches to harmonizing relevant documents at the national level. Simultaneously, it is advisable to take into account the documents and recommendations of international and regional organizations in the field of legal metrology.

Rules and procedures of software testing for the MI are set out in the document [1] of the International Organization of Legal Metrology (OIML), as well as the documents and recommendations of the regional metrological organizations. In particular: software testing procedures for MI are governed by the recommendation [2] of the Euro-Asian Cooperation of National Metrological Institutions (COOMET), document [3] and guidelines [4, 5] of the European Cooperation in Legal Metrology (WELMEC).

The relevance of the work is confirmed by the urgent need to carry out a conformity assessment of the regulated MI in

accordance with the requirements of national legislation, TR or European directives. Software is one of the key components of this MI in most cases. Therefore, national metrology institutes and conformity assessment bodies are interested in the existence of effective testing methods for MI software, risk assessment and application-related threats. In this regard, the urgent issue is the study of the state of the normative framework for software testing for the MI at the national level and the establishment of the necessary elements to achieve the presumption of compliance of the software with TR requirements in conformity assessment of the MI.

2. Literature review and problem statement

Currently, the important and difficult task is to transform the national metrological normative framework and its harmonization with the documents, recommendations and standards of the relevant international organizations. It is OIML that promotes the global harmonization of legal metrological procedures. The normative base of the national metrological service, rules, technical and organizational basis in Ukraine are determined by the legislation of Ukraine on metrology. In particular, the requirements of the European Directive 2014/32/EC for measuring instruments (MID) [6] are the basis of the Ukrainian legislation for conformity assessment of the MI.

A thorough analysis of software for MI was the subject of previous studies by the authors [7–11]. In [7, 8], the peculiarities of the normative provision of software testing of the MI were investigated. The main stages of testing the MI software and features in accordance with the requirements [1, 4, 5] were considered in [9]. The use of validated software for uncertainty assessment of measurements in accredited laboratories was presented in [10]. The main factors and algorithms for MI software testing in accordance with OIML and WELMEC requirements were considered, and a universal MI software testing algorithm was proposed in [11]. However, these studies do not include an analysis of the requirements and peculiarities of international and regional documents [1, 4, 5] for the purpose of joint implementation in the national standards for MI software testing.

The works [12–17] consider the issues of security, risk assessment and current threats associated with the application of MI software, including those that are integrated into open networks. These studies focus on methods that take into account the requirements of regional guidelines [4, 5] and international standards. However, [12–16] does not take into account the requirements of the international document [1], the possibility of using the software for local MI, and the provisions set out in [17] apply only to intelligent measurement systems.

In [18], software risk classes, verification guidelines and some possible test methods of software for local MI in accordance with the requirements [1, 4, 5] are considered. However, in the work the possibility of testing MI software integrated into open networks was not considered. In [19], an approach for automatic testing of parameters for software built into the MI in accordance with the requirements of the international document [1] is proposed. The general criteria for assessing the safety and protection of IT components are considered. However, the work does not take into account the requirements of regional guidelines [4, 5].

Thus, we can conclude that previous studies concerning the requirements of international and regional documents [1, 4, 5] on the testing of MI software did not analyze the possibilities of adaptation or joint application of the provisions of these documents. Also, the issue of the possible integration of these requirements into national normative standards was not considered.

Therefore, the state of the normative framework for MI software testing requires a more detailed analysis of the availability of the necessary elements, in particular those set out in the international document [1] and the regional recommendations [4, 5], in order to achieve the presumption of compliance of the software with TR requirements in conformity assessment of the MI. Such research should be carried out in order to determine the appropriateness of updating the national normative framework on the testing of the MI software or the additional use of the methodology set forth in the documents of international and regional organizations.

3. The aim and objectives of the study

The research was aimed at developing approaches to harmonize the requirements of documents of the international and regional metrological organizations for testing the special MI software at the national level.

To achieve this aim, the following objectives must be accomplished:

– to analyze the provisions of the national normative documents on the testing of the MI software for compliance with the essential requirements of the technical regulations and to compare with the requirements set forth in the documents of international and regional organizations;

– to establish and investigate the necessary elements sufficient to achieve the presumption of conformity of software with the essential requirements of the technical regulations in conformity assessment of the MI, especially with regard to the suitability of the software for application and protection against unauthorized interference;

– to establish and investigate the algorithm of testing the MI software for the purpose of conformity assessment.

4. Materials and methods of research for the application of software of measuring instruments

Software protection in the broadest sense is a set of measures aimed at preventing the unauthorized use, study, distribution and modification of software, as well as protection against accidental interference. Protection of software and its components, measurement data against unauthorized modification, unintentional and accidental interventions for the MI software is important, namely:

– software source code;

– measurement data from the sensors of the measuring system;

– user input command;

– measurement data displayed on the display;

– measurement data and calibration coefficients stored in the device's long-term memory;

– measurement data transmitted through communication channels.

Different approaches and measures are used to protect the software, its components and data depending on the type of construction of the MI, with the built-in software (Fig. 1) or on the basis of a universal computer (Fig. 2).

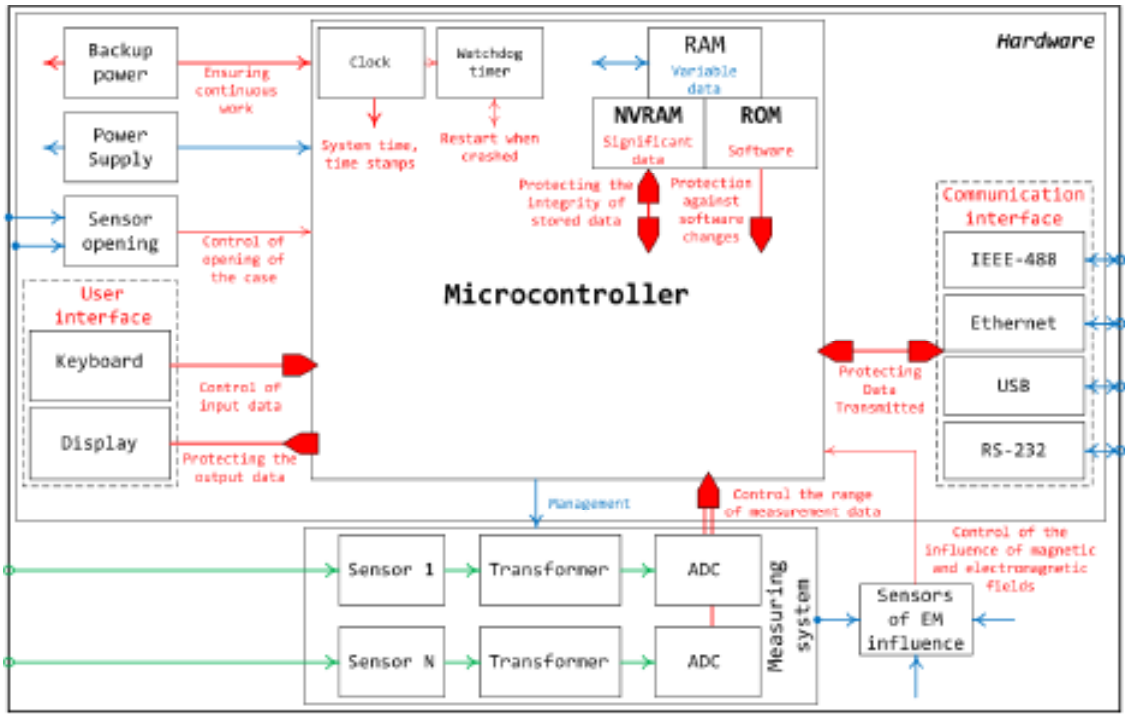

Fig. 1. Block diagram of MI with built-in software

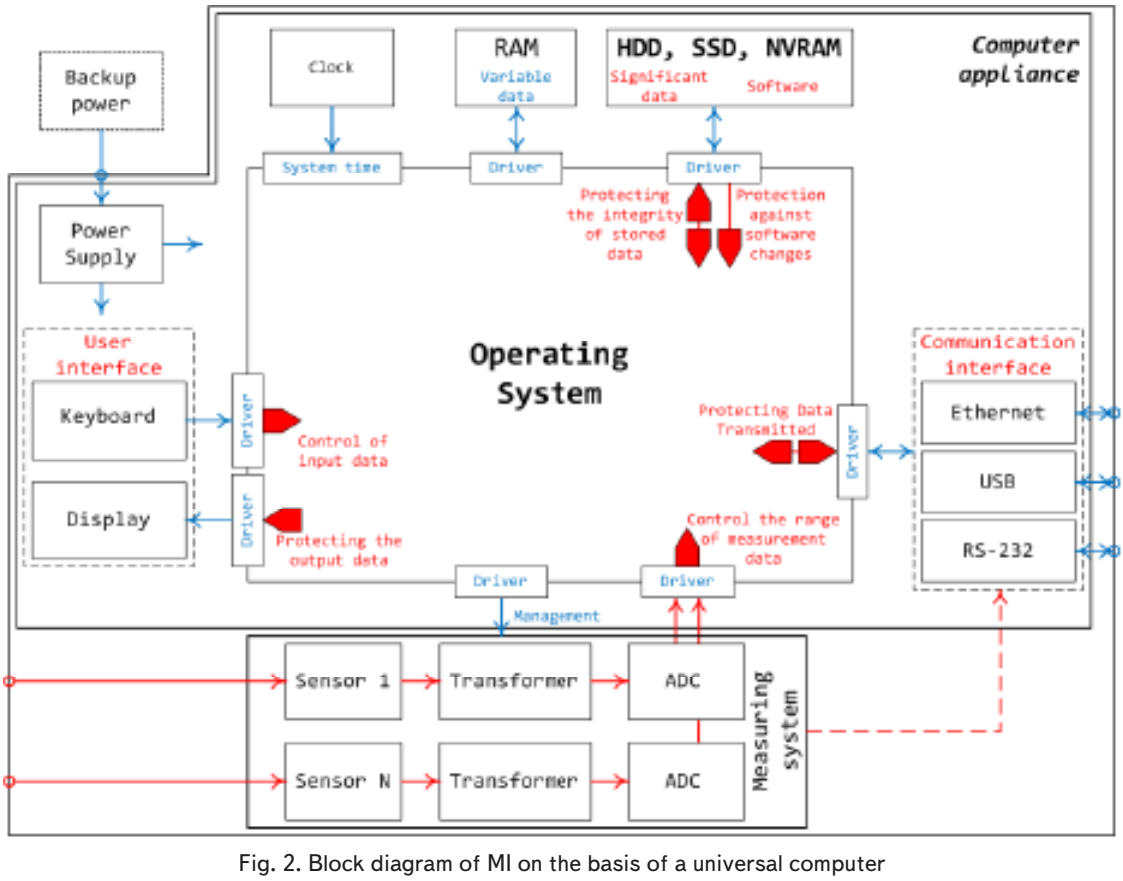

Fig. 2. Block diagram of MI on the basis of a universal computer

MI with built-in software has the following main features:

– realized only for implementation of specific measurements, established by the manufacturer;

– contain a microcontroller with a fixed set of commands and components necessary for operation;

– only the commands set by the manufacturer can be entered from its panel;

– only the manufacturer's information is displayed on its display;

– only the manufacturer's communication interfaces can be used;

– the measuring and hardware parts are located in a protective case that can be physically secured.

These features provide such opportunities for protection of both software and MI as a whole:

– possible hardware block up for rewriting the built-in software;

– the use of specialized microcontrollers with built-in analog-to-digital conversion (ADC) channels allows you to enter measurement data from sensors or transducers immediately to the microcontroller, which excludes the possibility of intervention in them;

– it is possible to use microcontrollers with built-in specialized modules to provide protection;

– the inability to spoil the data and commands transmitted between the microcontroller and the user interface without intervention in the hardware part of the device;

– the microcontroller has the necessary amount of internal constant, operational and energy-independent memory;

– the absence of mechanisms for interfering with stored data than those established by the manufacturer;

– possibility to restart it by a watchdog timer command in the event of a failure of the MI related to the software;

– commands and data related to the measurement process are transmitted only the communication interfaces the manufacturer-defined;

– in the case of opening the MI case or when triggering the magnetic and electromagnetic field sensors near the sensitive elements of the measuring system, corresponding entries in its event log are created.

MI on the basis of a universal computer have the following main features:

– intended for the implementation of specific measurements, but can also be programmed for other measurements;

– processing of measurement data, storage and transmission of measured values occur using a universal computer that runs under the control of a particular operating system;

– possibility to execute other tasks on the universal computer with the input of any data simultaneously with the measurement process;

– the display of a universal computer may display information selected by the user and not related to the measurement process;

– communication interfaces provided by the manufacturer of a universal computer may be used, which may not be used in the process of measuring or transmitting measurement data;

– the measuring and software hardware can be placed in both the same and in different cases, and this does not guarantee protection against intervention in the software.

These features require the following measures to ensure software protection:

– to ensure the integrity of the software by means of checking the checksums of its meaningful files;

– to control the data from the measuring system, especially when these data are received through the communication interface;

– to restrict user access rights to software resources, operating system, if necessary;

– indication of measurement data should be a priority during the measurement;

– to use checksums to verify the integrity of data and duplicate data for the protection of measurable and other significant data stored for recovery in case of their destruction;

– to control the data and commands transmitted through the communication interfaces, in order to prevent unauthorized influence on the work of the MI software;

– to ensure the protection of data transmitted between significant and non-significant parts of the MI software;

– mechanisms for verifying authentication, authenticity and integrity of data may be involved in updating the software with the possibility of refusing to upgrade the software and returning to the previous version;

– the use of an external source of continuous power is necessary to ensure the continuous operation of the MI.

The MI software having the required level of protection is protected. The software will be designed in such a way as to ensure maximum suitability for the correct application of the MI, including:

– documentary functions or commands that may affect the metrological characteristics or functionality of the MI are absent;

– intentional or unintentional user actions through interfaces that may distort measurement results are excluded.

The above requirements apply to software, if it can affect measurement results, storage or transmission of measurement results. This can be either the main MI (built-in or universal) software, or additional or auxiliary software used to process measurement results.

Additional (auxiliary) software must also be identified and protected, that is, it needs to perform the same test procedure as for the basic software. Manufacturers of MI with software must provide all necessary information regarding the identification of the software, the measures taken to ensure the security and suitability of the software.

The DSTU 7363 standard [20] may be applied to verify compliance with the requirements of the MI software, and is included in the list of national standards, the compliance of which gives a presumption of compliance of the MI with the essential requirements of the TR for the MI.

The OIML D 31 document [1] is recommended for use in OIML member countries during the approval of software-controlled MI. To verify compliance of the MI software with the requirements of the MID [6], a special recommendation WELMEC 7.2 [4] has been developed.

5. General requirements of international and regional documents on software for measuring instruments

The OIML D 31 document [1] sets the general requirements for software-controlled MI. The requirements of the document do not cover all the technical requirements that are individual for each category of MI. These requirements should be set out in the relevant regulatory documents. The main object of the document is the MI with software.

Requirements for MI are divided into the following:

– the basic requirements concerning identification of software and correctness of applied algorithms, functions;

– requirements for software protection (prevention of accidental misuse of MI and fraud protection);

– requirements for hardware support in case of error detection to ensure the reliability of the MI with software;

– special requirements for individual configurations depending on the scope of the MI;

– definition and division of the hardware and software into legally significant and insignificant, allocation of controlled parts and their interfaces;

– ensuring the compatible display and printing of information of legally significant and insignificant parts; data storage and transmission over communication networks;

– compatibility of operating systems and hardware, portability;

– conformity to the approved type;

– technical services and configuration change.

OIML D 31 regulates the type approval procedure and the methods of testing the software; and describes the software test program depending on the established level of risk. The documents provided by the manufacturer of the MI (software developer) during the type approval must contain information sufficient to verify compliance with the requirements of OIML D 31 [1].

The WELMEC 7.2 recommendation [4] sets the general requirements for the MI with software. In the first place, the recommendation focuses on the objects of regulation of the MID [6], which is harmonized in Ukraine as an appropriate TR. Since the recommendation is general, it can also be applied to other MIs with software. The requirements of the recommendation apply only to software and do not cover the technical requirements that are individual for each type of MI. Requirements should be set out in the relevant normative-legal documents.

The main object of the WELMEC 7.2 recommendation is the software, but attention is also paid to the hardware part of the MI. The recommendation has a structured set of requirements blocks, consisting of:

– requirements to the basic configurations of the MI (with built-in software – P, based on a universal computer – U), namely:

– for the compulsory data of the program documents, which are provided in addition to the special documents necessary to describe the implementation of the requirements for the configuration and special requirements;

– on identification of software and methods of its protection for high levels of risk;

– regarding the impact through the user interface;

– regarding the impact through the communication interface;

– protection against accidental and unintentional changes;

– protection against intentional changes;

– regarding parameter protection;

– regarding the authenticity of the software (only for type U);

– regarding the impossibility of the impact of other software on MI (only for type U);

– requirements for the configurations of measuring technologies (long-term storage – L, communication interface – T, software separation – S, download of updates – D), including requirements for protection of data stored and transmitted, data restoration and error detection;

– special requirements to the MIs regulated by the MID (water meters – I1, gas volume meters and converters – I2, active energy meters – I3, heat meters – I4, systems for continuous and dynamic measurement of the volume of liquids, except water – I5, automatic weights – I6, taximeters – I7).

Each of these blocks has its own name and contains well-defined requirements related to it, explaining the comments, necessary information in the program documents, test guidelines and examples of acceptable decisions. The volume of requirements depends on the chosen risk class. The recommendation contains certain risk categories for some MIs, depending on the scope and recommendations for determining the risk profile for other MIs. The unchanged software has a risk class A and, according to the recommendation, is not subject to testing.

Documents provided by the manufacturer of the MI (software developer) during the type approval must contain information sufficient to verify compliance with the requirements of the WELMEC 7.2 recommendation.

6. General requirements of the national standard for special software for measuring instruments

The national standard DSTU 7363 sets the general requirements for MI software (integrated and universal), which can be changed during operation. The main object of the standard is the MI software. Requirements to the MI software are divided into the following:

– requirements for the structure to ensure testing of the functions of the software for compliance with the requirements of the standards and other regulatory documents, the absence of influence of other software on them;

– requirements for software protection, namely:

– protection against unauthorized access through program and hardware interfaces;

– protection against crashes and distortions that may affect the integrity of the data and measurement results;

– protection against unintentional and deliberate changes in software;

– entering categories of users with different access rights;

– ensuring the integrity control of software;

– application of software in accordance with established requirements;

– requirements for software documenting.

Requirements for the identification, security and suitability of the MI software are set regardless of the test levels, but the extent of the tests and the degree of compliance of the software with the set requirements depend on the specified level of rigidity. The standard contains a recommendation for determining the level of rigidity. In addition, the level of rigidity can be determined using the ISO/IEC 27005 standard [21]. At the same time, the level of rigidity will meet the established level of risk.

7. Discussion of the results on the possibility of sharing the requirements of international and regional documents at the national level

A comparative analysis of software requirements and tests in accordance with the requirements of DSTU 7363, OIML D 31 and WELMEC 7.2 recommendations is shown in Table 1.

The national standard DSTU 7363 does not consider the possibility of dividing software into legally significant and insignificant parts, all software is considered legally significant. Also, the possibility of updating the approved software is not considered. For each version (or when changing the identification), separate tests are required. The requirements of the standard apply only to the software, therefore, for MI verification it is necessary to apply additionally the corresponding standards and recommendations concerning the specific type of MI.

Table 1

Comparative analysis of requirements and software testing

Software requirements	Item and section of the normative document		
	DSTU 7363	OIML D 31	WELMEC 7.2
1. Documentation	4.4	6.1	P1, U1
2. Identification	4.3.7	5.1.1	P2, U2
3. Security			
3. 1. Software integrity			
– protection against accidental and unintentional changes of software	4.2.5	5.1.3.2	P5, U5
– protection against intentional changes of software	4.2.1, 4.2.5	5.1.3.2	P6, U6
– protection of software integrity and presentation of measurement results	4.2.2, 4.2.5	5.1.4.2	U8
3. 2. User interface			
– input data (keyboard)	4.2.2*	5.1.3.2	P3, U3
– output data (display)		5.1.3.1	
3. 3. Data stored			
– protection against accidental and unintentional changes in stored data	4.2.6*	5.1.3.2, 5.2.3.1,	L2
– protection against intentional changes in stored data		5.2.3.2,	L3
– protection of software parameters		5.2.3.4	P7, U7
– validity of stored measurement data		*	L4
– confidentiality of keys		5.1.3.3	L5
– recovering stored data		-	L6
3. 4. Data transmitted through the communication interface			P4, U4
– protection against accidental and unintentional changes in data transmitted over communication networks	4.2.1, 4.2.2*	5.2.3.1, 5.2.3.2,	T2
– protection against intentional changes in data transmitted over communication networks		5.2.3.5, 5.2.3.6	T3
– reliability of measured data transmitted over communication networks		*	T4
– confidentiality of keys		5.1.3.3	T5
– actions with corrupted data during transfer		*	T6
4. Suitability			
– functional compliance (principle of functioning)	4.3.4	5.1.2	*
– intended use	4.3.2	5.1.3.1	L1, L7, L8, T1, T7, T8, Ix-3
– protection from the impact of other software	4.1.2	5.2.4	U9
– processing of non-standard situations	4.2.3, 4.4.8, 4.4.9	5.1.4.1	Ix-1, Ix-4

*Note: * – the requirement is general, indirect or applies to the entire section*

DSTU 7363 sets criteria for conformity assessment of software, but does not include testing methods. That is, it does not allow determining the level of presumption of conformity of software with TR requirements during conformity assessment of MI. In order to specify the requirements for the software and to ensure the test procedure, it is necessary to use additional OIML D 31 document and WELMEC 7.2 recommendation.

A schematic representation of the application of standards, documents and recommendations for conformity assessment of software to TR requirements is shown in Fig. 3.

As can be seen from Fig. 3, the use of these normative documents during conformity assessment of MI to TR requirements for B, F1 and G modules is sufficient because they cover the same software requirements as TR. Using module F, the compliance of the program identification indicated during the approval of the type of MI (module B) is checked, no other test software is used.

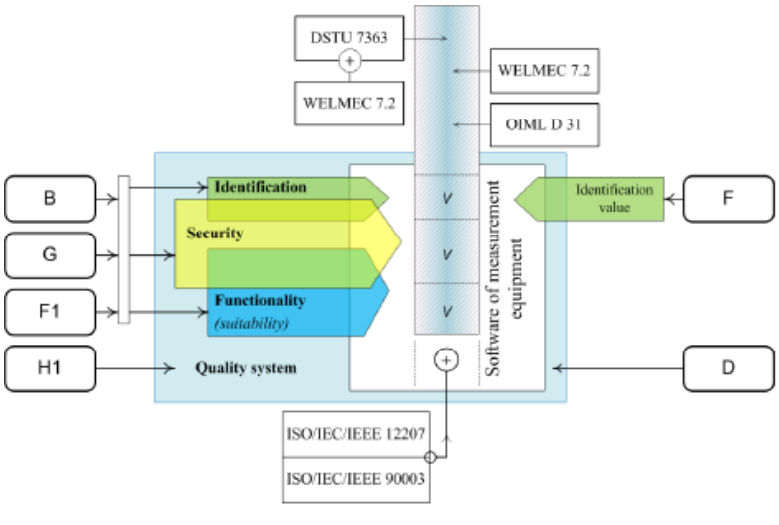

Fig. 3. Application of standards, documents and recommendations for conformity assessment of MI software to TR requirements

Using the D and H1 modules, the MI manufacturer must additionally demonstrate compliance with the software life cycle requirements [22] and use standards related to the quality system when developing the software [23].

The presumption of compliance of the MI software with the TR requirements gives:

– for B, F1 and G modules – compliance with the DSTU 7363 standard, OIML D 31 document or WELMEC 7.2 recommendation, which is confirmed by the relevant test protocols;

– for D and H1 modules – additional confirmation of the requirements of ISO/IEC/IEEE 12207 and ISO/IEC 90003 standards.

The use of the DSTU 7363 standard for MI software testing requires the additional use of the documents of international and regional organizations OIML and WELMEC in order to meet the requirements of the test methodology.

On the basis of the conducted researches and data obtained in Table 1, an algorithm for testing the MI software for the purpose of conformity assessment was proposed, which is shown in Fig. 4.

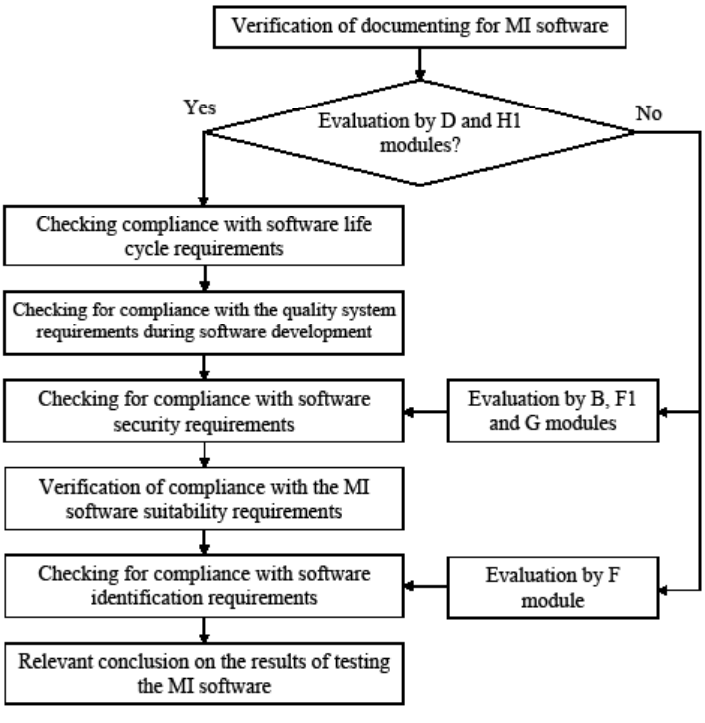

Fig. 4. Proposed algorithm for testing the MI software for the purpose of conformity assessment

The algorithm is constructed taking into account requirements of the documents of international and regional organizations of legal metrology OIML and WELMEC, as well as the national standard DSTU 7363. In addition, the algorithm takes into account the requirements of international standards ISO/IEC/IEEE 12207 concerning the life cycle of software and ISO/IEC 90003 concerning the quality system during software development. As can be seen from Fig. 4, the largest volume of tests is performed during the MI evaluation by D and H1 modules, somewhat smaller – by B, F1 and G modules, and the smallest (only software identification verification) – by F module. Thus, the application of the proposed algorithm for testing the MI software allows taking into account all necessary elements sufficient to achieve the presumption of conformity of software with essential TR requirements.

Using the proposed algorithm (Fig. 4), special checklists for software testing for each of these modules were developed. Such checklists are analogous to those listed in the WELMEC 7.2 recommendation [4, 11] and are applicable to specific MIs intended for use in the field of legally regulated metrology. The State enterprise "Ukrmetrteststandard" (Ukraine) only in 2018 completed testing of the MI software by module B (one of the most common modules) for about 100 types of MIs, and by module F – about hundreds of thousands of MIs, using the developed special checklists.

At present, the general technical requirements for the MI software and the procedure for conformity assessment with the essential requirements of TR at the national level are regulated only by the national standard DSTU 7363, which does not define the software testing methodology. The research can be used for reviewing the DSTU 7363 standard and developing a new national standard for its replacement, taking into account the provisions of the documents of the international and regional organizations of legal metrology OIML and WELMEC.

8. Conclusions

1. A comparative analysis of the provisions of national normative documents and documents and recommendations of international and regional organizations OIML and WELMEC concerning the testing of the MI software for compliance with the essential requirements of the TR for MI was conducted. In particular, regarding the suitability of software for application and protection against unauthorized interference. It was found that the existing national standard DSTU 7363 contains general requirements for the protection of software and does not determine the methodology of software testing.

2. The necessary elements sufficient to achieve the presumption of conformity of software with the essential requirements of the TR during conformity assessment of the MI were established and investigated. The necessity of additional application of international and regional documents OIML D 31 or WELMEC 7.2 for the specification of requirements of the software of the MI and WELMEC 7.2 for ensuring the methodology for testing the software of the MI was determined. The need for additional use of the documents of international and regional organizations OIML and WELMEC during the testing of software for the MI confirmed the necessity of revision of the national standard DSTU 7363.

3. The software testing algorithm for the MI for conformity assessment with the requirements of the documents of the international and regional organizations of legal metrology OIML and WELMEC, as well as the national standard DSTU 7363 was established and investigated. The algorithm takes into account the requirements of international standards ISO/IEC/IEEE 12207 concerning the life cycle of software and ISO/IEC 90003 concerning the quality system when developing software. This will take into account all the necessary elements sufficient to achieve the presumption of conformity of software with the TR essential requirements.

References

1. OIML D 31:2008. General Requirements for Software Controlled Measuring Instruments. OIML. Paris, 2008. 53 p.
2. COOMET R/LM/10:2004. COOMET Recommendation: Software for Measuring Instruments: General Technical Specifications. COOMET, 2004. 10 p.

3. WELMEC 7.1. Informative Document: Development of Software Requirements. URL: http://www.welmec.org/fileadmin/user_files/publications/WG_07/7-1_FRPO.pdf
4. WELMEC 7.2. Software Guide (Measuring Instruments Directive 2004/22/EC). URL: http://www.welmec.org/fileadmin/user_files/publications/WG_07/Guide_7.2_2015__Software.pdf
5. WELMEC 2.3. Guide for Examining Software (Non-automatic Weighing Instruments). URL: http://www.welmec.org/fileadmin/user_files/publications/2-3.pdf
6. Directive 2014/32/EU on the harmonisation of the laws of the Member States relating to the making available on the market of measurement instrument (recast) // Official Journal of the European Union. 2004. L96/149. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0032
7. Velichko O. N. Normative base for certification of measurement provision software // Measurement Techniques. 2007. Vol. 50, Issue 4. P. 364–371. doi: https://doi.org/10.1007/s11018-007-0076-5
8. Velychko O., Gordiyenko T. The implementation of general international guides and standards on regional level in the field of metrology // Journal of Physics: Conference Series. 2010. Vol. 238. P. 012044. doi: https://doi.org/10.1088/1742-6596/238/1/012044
9. Velichko O. N. Basic tests, stages, and features in monitoring measuring instrument software // Measurement Techniques. 2009. Vol. 52, Issue 6. P. 566–571. doi: https://doi.org/10.1007/s11018-009-9308-1
10. Velychko O. Using of Validated Software for Uncertainty Analyses Tools in Accredited Laboratories // Key Engineering Materials. 2008. Vol. 381-382. P. 599–602. doi: https://doi.org/10.4028/www.scientific.net/kem.381-382.599
11. Velychko O., Gordiyenko T., Hrabovskyi O. Testing of measurement instrument software on the national level // Eastern-European Journal of Enterprise Technologies. 2018. Vol. 2, Issue 9 (92). P. 13–20. doi: https://doi.org/10.15587/1729-4061.2018.125994
12. Achieving Software Security for Measuring Instruments under Legal Control / Peters D., Grottker U., Thiel F., Peter M., Seifert J.-P. // Position Papers of the 2014 Federated Conference on Computer Science and Information Systems. 2014. Vol. 3. P. 123–130. doi: https://doi.org/10.15439/2014f460
13. Esche M., Thiel F. Software Risk Assessment for Measuring Instruments in Legal Metrology // Proceedings of the 2015 Federated Conference on Computer Science and Information Systems. 2015. Vol. 5. P. 1113–1123. doi: https://doi.org/10.15439/2015f127
14. Software risk assessment and evaluation process (SRAEP) using model based approach / Sadiq M., Rahmani M. K. I., Ahmad M. W., Jung S. // 2010 International Conference on Networking and Information Technology. 2010. doi: https://doi.org/10.1109/icnit.2010.5508535
15. Software evaluation of smart meters within a Legal Metrology perspective: A Brazilian case / Boccardo D. R., dos Santos L. C. G., da Costa Carmo L. F. R., Dezan M. H., Machado R. C. S., de Aguiar Portugal S. // 2010 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe). 2010. doi: https://doi.org/10.1109/isgteurope.2010.5638881
16. A Secure System Architecture for Measuring Instruments in Legal Metrology / Peters D., Peter M., Seifert J.-P., Thiel F. // Computers. 2015. Vol. 4, Issue 2. P. 61–86. doi: https://doi.org/10.3390/computers4020061
17. IT Security standards and legal metrology – Transfer and Validation / Thiel F., Hartmann V., Grottker U., Richter D. // EPJ Web of Conferences. 2014. Vol. 77. P. 00001. doi: https://doi.org/10.1051/epjconf/20147700001
18. Jacobson J. Validation of software in measuring instruments // Computer Standards & Interfaces. 2006. Vol. 28, Issue 3. P. 277–285. doi: https://doi.org/10.1016/j.csi.2005.07.006
19. Thiel F., Grottker U., Richter D. The challenge for legal metrology of operating systems embedded in measuring instruments // OIML Bull. 2011. Vol. 52, Issue 1. P. 5–14.
20. DSTU 7363:2013. Prohramne zabezpechennia zasobiv vymiriuvalnoi tekhniky. Zahalni tekhnichni vymohy. Kyiv: Minekonomrozvytku Ukrainy, 2013. 11 p.
21. ISO/IEC 27005:2018. Information technology. Security techniques. Information security risk management. International Organization for Standardization, 2018. 56 p.
22. ISO/IEC/IEEE 12207:2017. Systems and software engineering. Software life cycle processes. International Organization for Standardization, 2017. 145 p.
23. ISO/IEC/IEEE 90003:2018. Software engineering. Guidelines for the application of ISO 9001:2008 to computer software. International Organization for Standardization, 2018. 69 p.