Проведено порівняльний аналіз загальних вимог в документах та настановах міжнародних та регіональних організацій законодавчої метрології OIML і WELMEC щодо випробування програмного забезпечення (ПЗ) для засобів вимірювальної техніки (ЗВТ). Визначено основні фактори та встановлені алгоритми щодо випробування ПЗ для ЗВТ згідно з вимогами OIML і WELMEC. Запропоновано універсальний алгоритм випробування ПЗ для ЗВТ

Ключові слова: програмне забезпечення, засіб вимірювальної техніки, випробування, законодавча метрологія, нормативне забезпечення

Проведен сравнительный анализ общих требований в документах и руководствах международных и региональных организаций законодательной метрологии OIML и WELMEC по испытанию программного обеспечения (ПО) для средств измерительной техники (СИТ). Определены основные факторы и установлены алгоритмы испытания ПО для СИТ по требованиям OIML и WELMEC. Предложен универсальный алгоритм испытания ПО для СИТ

Ключевые слова: программное обеспечение, средство измерительной техники, испытание, законодательная метрология, нормативное обеспечение

UDC 389:14:621.317:354
DOI: 10.15587/1729-4061.2018.125994

TESTING OF MEASUREMENT INSTRUMENT SOFTWARE ON THE NATIONAL LEVEL

O. Velychko
Doctor of Technical Sciences, Professor, Director
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
E-mail: velychko@hotmail.com
T. Gordiyenko
Doctor of Technical Sciences, Associate Professor, Head of Department
Department of standardization, conformity assessment and quality*
E-mail: t_gord@hotmail.com
O. Hrabovskyi
PhD, Associate Professor, Dean*
E-mail: gelond737@gmail.com
*Odessa State Academy of Technical Regulation and Quality
Kovalska str., 15, Odessa, Ukraine, 65020

1. Introduction

Specialized software (SW) for measuring instruments (MI) plays an ever greater role under conditions of the almost universal use of information technology (IT). Testing of MI SW in some form is conducted, especially in MI SW tests with the aim of confirming the type. Usually such a test is non-systematic in nature, and developers and users of automated MI largely do not have information about the state of the normative base in this field. Therefore, an analysis of the state of introduction of contemporary technologies into metrological practice and the development of approaches to harmonization of the corresponding documents at the national level are relevant. In doing so, it is necessary to take into account the recommendations of international and regional organizations that are concerned with issues of metrology, including legal metrology.

Appropriate decisions are needed in legal metrology on account of the general introduction of information technologies, particularly with regard to SW. These topics are discussed in the document [1] from the International Organization of Legal Metrology (OIML), and also documents and guidelines from regional metrological organizations, in particular: the recommendations [2] of the Euro-Asian Cooperation of National Metrological Institutions (COOMET), document [3] and guidelines [4, 5] from the European Cooperation in Legal Metrology (WELMEC).

The relevance of the work is confirmed by the urgent need to exercise legislative control over the MI before use and to conduct conformity assessment in accordance with the requirements of European directives or national legislation. As software is one of the key components of such MI, national metrology institutions are interested in developing effective methods for evaluating the MI SW status, risks and existing application-related threats. This can also be useful for conformity assessment bodies or industry and supports the comparability of risk assessment, SW validation and certification. Given this, the urgent issues are the research and development of harmonized approaches to the MI SW evaluation, taking into account the requirements of international and regional documents.

2. Literature review and problem statement

Foremost, national metrology legislation is to be harmonized on the basis of relevant documents, recommendations and standards of various international organizations concerned for the effective functioning of the Global Metrology System. The OIML was established to promote the global harmonization of legal metrology procedures. An important and difficult task is the transformation of national metrological legislation. It requires an effective adaptation of the National Metrology Service (NMS) and

alignment with modern requirements within the Global Metrology System.

The NMS legislative basis, its rules and its technical and organizational basis in Ukraine are defined by the Ukrainian law on metrology. The requirements of the European Directive 2014/32/EU on measuring instruments (MID) [6] are the basis of the Ukrainian legislation on legal metrological control of MI.

A thorough analysis of software for MI was the subject of previous studies by the authors [7–10]. The works [7, 8] explore the features of normative base and standardization support for MI SW certification. The main tests, stages and features of the monitoring of the MI SW in accordance with the requirements [1, 4, 5] are considered in [9]. The use of proven SW to analyze the uncertainty of equipment in accredited laboratories is presented in [10].

In [11], the issues of certification of the MI SW in accordance with the requirements of national documents and standards were considered. However, these studies do not take into account the requirements of international and regional documents [1, 4, 5].

The works [12–14] consider the issues of security, risk assessment and current threats associated with the application of MI SW, 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, these works do not take into account the requirements of the international document [1] and the possibility of application of SW for local MI.

In [15], SW risk classes, verification guidelines, and some possible methods for testing the SW for local MI in accordance with the requirements [1, 4, 5] are considered. However, this work does not consider the possibility of checking MI SW integrated into open networks.

In [16], an approach is proposed for automatic testing of parameters for SW built into the MI in accordance with the requirements of the international document [1]. The general criteria for assessing the safety and protection of IT components are considered. However, this 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 SW for the MI 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 regulatory documents and standards was not considered.

Therefore, the practical application of the above guidelines and recommendations requires a more detailed and critical consideration of the general requirements set out in the international document [1] and the regional recommendations [4, 5]. Such research should be carried out to harmonize these documents among themselves and to agree with the national normative documents on the verification and certification of the MI SW.

3. The aim and objectives of the study

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

To achieve this aim, the following tasks must be solved:

– to analyze the general requirements and to identify the main factors in testing the quality of MI SW in the documents of international and regional organizations;

– to establish and investigate the algorithms of testing the SW of the MI regarding the requirements of documents of international and regional organizations;

– to explore the possibility of developing universal test checklists for testing the SW for all categories of MI. In doing so, it is necessary to take into account approaches based on the requirements of documents and guidelines of international and regional metrology organizations.

4. Materials and methods of research on application of software of measuring instruments

The most advanced MI have modules of microsystems, that directly manage the processes of measuring, processing and distribution of measuring data, and present to their user (operator). All these processes are executed clearly and correctly only on condition that the SW worked out by a producer for MI will have the corresponding metrological algorithm and a certain level of protection from external interference.

SW is a complicated technological product, which, in addition to visible advantages, also has certain hidden problems. Breaking, unauthorized access, failures and incorrect operation of users are only part of the known problem issues that the developers of SW try to solve already on the stage of development. Ordinary sealing-of MI with SW or SW management do not solve the issue of providing the measurement accuracy and security of measurand.

In Fig. 1, the generalized structure of MI with SW is represented. AC/DC converter transforms the quantitative value of the physical measurand in its digital equivalent pursuant to a certain function of transformation. The resulting digital sequence is processed by SW that functions in a certain hardware program environment, on a certain algorithm. The current results of measurement can be represented on a display (indicator), written on the information carrier for storage, and sent via communication channels. Measurement results can be computed from the information carrier or brought to the communication channels. The user, if allowed by the SW developer, can manage the work of MI, change its settings, etc. SW in such MI, regardless of its complexity, executes a basic role in the process of measurement.

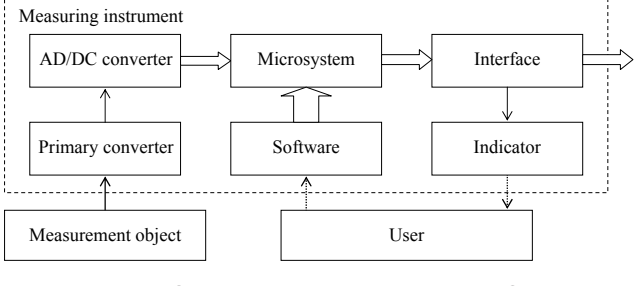

Fig. 1. Generalized structure of MI with SW

The main requirements relate to: SW identification, the correctness of algorithms and operation, the SW protection from premeditated and unpremeditated misrepresentation, SW maintenance (diagnostics). The main requirements for

specific SW: establishment and choice of the essential parts of SW and interfaces, general data presentation, data storage and transfer through communications systems, compatibility of an operating system as a whole and the parts, agreement of metrological requirements and SW, maintenance and reconfiguration (resetting).

The following methods are used for the MI SW testing:

– analysis of documentation and specifications (plan testing);

– functional testing of metrological and other SW functions;

– analysis of data flows;

– step-by-step checking of codes;

– module testing.

In order to implement these methods, specialists with various skills and appropriate hardware are necessary. The choice of testing method depends on the risk class for the MI SW used (Table 1, 2).

Table 1

Definition of SW risk classes

Risk class	SW protection level (1)	SW examination level (2)	Degree of SW conformity (3)
A	L	L	L
B	M	M	L
C	M	M	M
D	H	M	M
E	H	H	M
F	H	H	H

Notes: L – low level; M – medium level; H – high level

Table 2

Assignment of MI SW risk classes

Measurement purposes	Measuring instruments	Protection class	1	2	3
Calculations with users by means of MI with special SW	Water meters, gas meters, electric power meters, measuring transformers, heat meters	C(C)	M	M	M
		B(D)	H	M	M
Commercial agreements, service	Measurement systems for repeated and dynamic measurements of flow rates of liquids other than water; automatic weighing facilities; taximeters; length measurement means	C(B)	M	M	L
		B(D)	H	M	M
Direct control measurements	Direct output analyzers	–(F)	H	H	H
Environmental protection, health safety	External gas analyzers	C(B)	M	M	L

Notes: 1 – SW protection level; 2 – SW checking level; 3 – degree of SW conformity; L – low level; M – medium level; H – high level

Three levels of criticality have been determined for the MI SW:

– *low* (the SW does not distort measurement results, it has limited application, etc.);

– *medium* (the software may distort the final measurement result, but it is not used in the MI SW whose functioning has direct economic and social significance);

– *high* (the software may misrepresent the measurement result, used in the MI whose functioning has a high economic and social importance) [7].

Taking this into account, it is needed to check the following MI SW components: user interface, loading, structure, protection, trouble detection, long-term storage of measurement data.

Built-in and stand-alone special MI SW, which have both functional and verification features, are different. A built-in special MI SW is the SW of a stand-alone MI that is generally a special-purpose device having a set of measurement functions. Conversion of the measured value and processing of measurement data in this case are carried out by means of internal hardware and SW.

Stand-alone SW generally functions on the basis of a personal computer and is divided into two classes depending on connections with the MI SW. There are less stringent requirements for built-in MI SW for all research characteristics, which is connected in the majority of cases with limited access to SW and measurement data, whereas for a stand-alone MI SW there are higher requirements for the level of their protection and conformity.

On the whole, MI SW testing consists of two main parts: estimation of program documentation and experimental studies of SW.

5. General requirements of the OIML document for measuring instrument special software

When choosing the level of SW inflexibility for a certain category of MI and their field of application (calculations with users by means of MI with special SW, commercial agreements, service, direct control measurements, environmental protection, health safety) in accordance with OIML D 31 [1], the following indexes are used:

– risk of SW falsification (consequences of social and public influence of malfunction, cost of the product subject to measuring, the platform used; the influence of sources of potential falsification);

– required conformity of SW (practical manufacturabilities for satisfaction of the set level);

– required reliability of SW (environmental conditions, consequences of social and public influence of errors);

– possibility of SW falsification (simplicity of falsification can be a sufficient motivational factor);

– possibility of repetition or termination of measurements.

When estimating the quality of MI SW in accordance with the requirements of OIML D 31, the following basic parameters of SW are controlled:

– general characteristics of SW (SW identification, compatibility of the operating systems and hardware facilities, portability, correctness of algorithms and functions, general indication);

– protection of SW (prevention of misapplication, protection against falsification);

– support of hardware functions (support of fault-detection, support of reliable protection);

– determination and separation of the corresponding parts of SW and interface (separation of devices and components; separation of SW parts);

– data storage, transmission by communication networks (data protection by facilities, application of cryptographic methods, auto-save, transmission delay, interruption of transmission, times tamps);

– maintenance and reconfiguration (tested updating, traced updating).

For the identification and accounting of all substantial primary, secondary and other factors influencing on the result of quality estimation of MI SW in accordance with the requirements of the OIML D 31 document, it is expedient to build the corresponding Ishikawa cause-effect diagram (Fig. 2):

1. General characteristics of SW:
1.1 – SW identification;
1.2 – compatibility of operating systems and hardware, portability;
1.3 – correctness of algorithms and functions;
1.4 – general indications.
2. Protection of SW:
2.1 – prevention of misuse;
2.2 – fraud protection.
3. Support of hardware functions:
3.1 – support of fault detection;
3.2 – support of reliable protection.
4. Separation of SW parts:
4.1 – separation of electronic devices and sub-assemblies;
4.2 – separation of software parts.
5. Data storage and transmission:
5.1 – data protection by software;
5.2 –application of cryptographic methods;
5.3 – auto-save;
5.4 – transmission delay;
5.5 – interruption of transmission;
5.6 – timestamps.
6. Maintenance and reconfiguration:
6.1 – verified update;
6.2 – traced update.

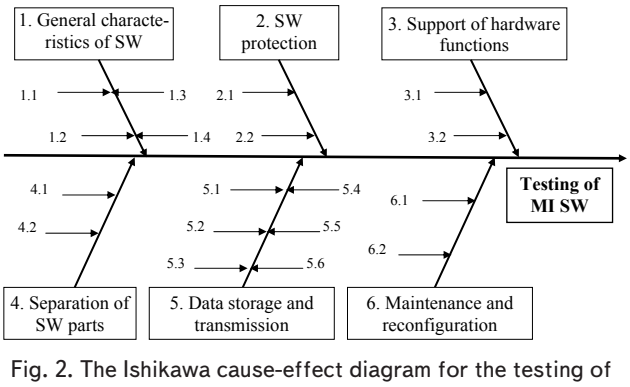

Fig. 2. The Ishikawa cause-effect diagram for the testing of MI SW in concordance with OIML D 31

The algorithm for testing the SW of the MI in concordance with the requirements of OIML is shown in Fig. 3.

Based on the results of the analysis of the International document OIML D 31, the Ishikawa cause-effect diagram was constructed and the main factors concerning the approaches to testing the quality of the MI SW were identified. On the basis of the conducted researches, the algorithm of testing the SW for MI in accordance with the requirements of the international document OIML is established.

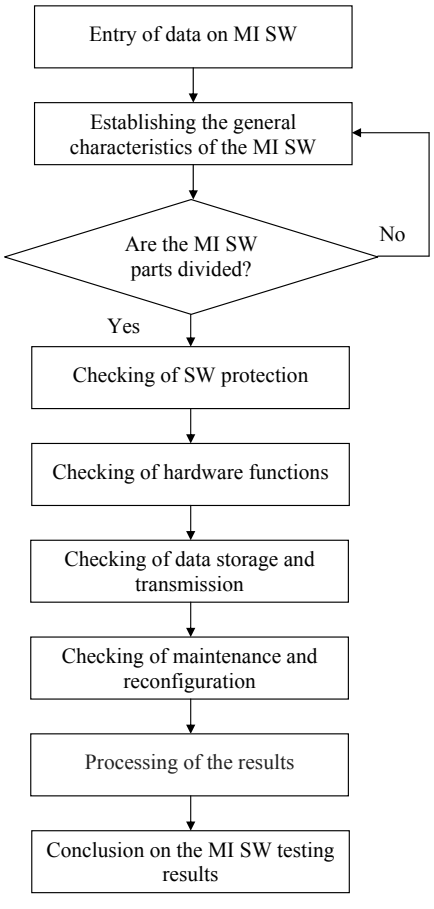

Fig. 3. The algorithm for testing the MI SW in accordance with OIML requirements

6. General requirements of WELMEC guide for measuring instrument special software

From 5 risk classes for the SW estimation set in WELMEC 7.2 [4], of practical interest are only 4 (B, C, D and E) and they embrace all MI that are subject to the European Directive on MI (MID) [6]. These risk classes provide sufficient possibility to change the level of risk estimation according to three basic parameters: the state of SW protection; inflexibility of SW verification; degree of SW conformity.

In MID requirements, the following values are set [6]:
– security and software identification (MID Annex I, 8.3);
– data transmission and data storage (MID Annex I, 8.4);
– interfaces (MID Annex I, 8.1);
– software separation (MID Annex I, 7.6).

The WELMEC 7.2 guide is built as the structured set of blocks of requirements. The general structure of this guide is related to the classification of MI in the basic configuration and classification in the so-called IT configurations. The set of requirements is complemented by the special requirements to MI. Three types of requirements are distinguished:

– requirements for two base configurations of MI (so-called parts P and U);

– requirements for four IT-configurations (so-called extensions L, T, S and D);

– requirements for the specific types of MI (so-called extensions I.1, I.2, ...).

WELMEC 7.2 consists of two basic parts: general requirements for SW embedded in the MI (part P); general requirements for SW installed on universal computers (part U).

Testing of MI SW in accordance with WELMEC 7.2 can be implemented on such basic elements (Table 3):

– checking of stored data (L);
– checking of data transmission (T);
– checking of download (D);
– checking of SW separation level (S).

Each set of these requirements is applied only if there is a corresponding function. Taking into account the requirements of MID and WELMEC 7.2 on the whole, the following basic requirements are set for MI SW given in Table 3.

Table 3

Testing requirements for MI SW (WELMEC 7.2)

Requirements for part P (built-for-purpose computer)	Requirements for part U (universal computer)
P1 – Documentation P2 – SW identification P3 – Influence via user interfaces P4 – Influence via communication interface P5 – Protection against accidental or unintentional changes P6 – Program protection against intentional changes P7 – Parameter protection	U1 – Documentation U2 – SW identification U3 – Influence via user interfaces U4 – Influence via communication interface U5 – Protection against accidental or unintentional changes U6 – Protection against intentional changes U7 – Parameter protection U8 – SW authenticity and presentation of results U9 – Influence of other SW
1. Check of stored data (L)	2. Check of data transmission (T)
L1 – Completeness of stored data L2 – Protection against accidental or unintentional changes L3 – Integrity of data L4 – Authenticity of stored data L5 – Confidentiality of keys L6 – Retrieval of stored data L7 – Automatic storing L8 – Storage capacity and continuity	T1 – Completeness of transmitted data T2 – Protection against accidental or unintentional changes T3 – Integrity of data T4 – Authenticity of transmitted data T5 – Confidentiality of keys T6 – Handling of corrupted data T7 – Transmission delay T8 – Availability of transmission services
3. Check of download (D)	4. Check of SW separation level (S)
D1 – Download mechanism D2 – Authentication of downloaded SW D3 – Integrity of downloaded SW D4 – Traceability of legally relevant SW download	S1 – Realization of SW separation S2 – Mixed indication S3 – Protective SW interface

Special requirements for MI SW (I) are as follows: failure detection (I1-1, I2-1, I3-1, I4-1, I6-1); facilities of data backup (I1-2, I2-2, I3-2, I4-2); possibilities of "waking-up" and restoration (I1-3, I2-3, I3-3, I4-3); internal permission (I1-4, I2-4, I3-4, I4-4); prohibition of resetting the cumulative measured values (I1-5, I2-5, I3-5, I4-5); indication for a customer (I1-6, I2-6, I3-6, I4-6); monitoring of battery life (I2-7); test of components (I2-9), etc.

For the identification and accounting of all substantial primary, secondary and other factors influencing on the result of MI SW estimation in accordance with the requirements of WELMEC, it is expedient to build the corresponding primary Ishikawa diagram (Fig. 4):

1. Basic configuration of MI: 1.1 – guidance and specifications for SW; 1.1.1 – P1; 1.1.2 – P2; 1.1.3 – P3; 1.1.4 – P4; 1.1.5 – P5; 1.1.6 – P6; 1.1.7 – P7; 1.2 – basic guidance for SW; 1.2.1 – U1; 1.2.2 – U2; 1.2.3 – U3; 1.2.4 – U4; 1.2.5 – U5; 1.2.6 – U6; 1.2.7 – U7; 1.2.8 – U8; 1.2.9 – U9.

2. IT-configuration: 2.1 – long-term storage of measuring data; 2.1.1 – L1; 2.1.2 – L2; 2.1.3 – L3; 2.1.4 – L4; 2.1.5 – L5; 2.1.6 – L6; 2.1.7 – L7; 2.1.8 – L8; 2.2 – transmission of measuring data; 2.2.1 – T1; 2.2.2 – T2; 2.2.3 – T3; 2.2.4 – T4; 2.2.5 – T5; 2.2.6 – T6; 2.2.7 – T7; 2.2.8 – T8; 2.3 – download of SW; 2.3.1 – D1; 2.3.2 – D2; 2.3.3 – D3; 2.3.4 – D4; 2.3.5 – D5; 2.4 – separation of SW; 2.3.1 – S1; 2.3.1 – S2; 2.3.1 – S3.

3. Requirements for specific types of MI: 3.1 – special requirements for MI SW; 3.1.1 – I1-1, I2-1, I3-1, I4-1; 3.1.2 – I1-2, I2-2, I3-2, I4-2; 3.1.3 – I1-3, I2-3, I3-3, I4-3; 3.1.4 – I1-4, I2-4, I3-4, I4-4; 3.1.5 – I1-5, I2-5, I3-5, I4-5; 3.1.6 – I1-6, I2-6, I3-6, I4-6; 3.1.7 – I2-7; 3.1.8 – I2-9; 3.1.9 – I6-1, etc.

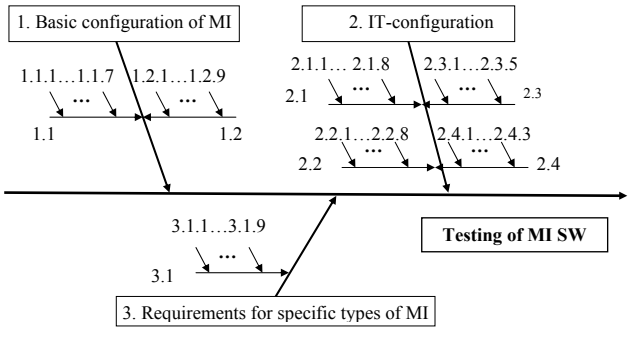

Fig. 4. The primary Ishikawa cause-effect diagram for the testing of MI SW in accordance with WELMEC 7.2

The algorithm of testing the MI SW taking into account the WELMEC requirements are shown in Fig. 5.

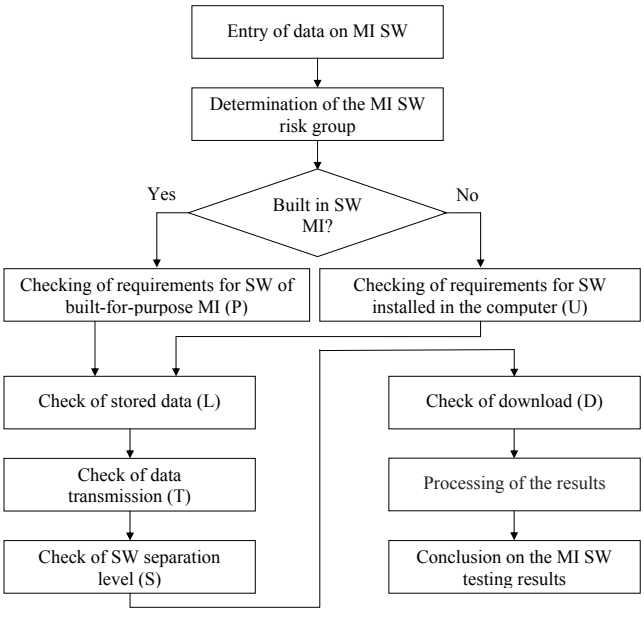

Fig. 5. The algorithm of testing the MI SW taking into account the WELMEC requirements

Based on the results of WELMEC's regional guide analysis, the Ishikawa cause-effect diagram was constructed and key factors were identified regarding the approaches to testing the quality of the MI SW. On the basis of the conducted researches, the algorithm of testing the SW for MI in accordance with WELMEC requirements is established.

7. Discussion of the results concerning the possibility of joint use of the requirements of international and regional documents on the national level

The consideration of the possibility of joint use of the requirements of the OIML document and WELMEC guide is expedient. To do this, it is needed to analyze the secondary components of the Ishikawa diagrams in Fig. 2, 4. In the presence of secondary components that simultaneously affect some of the original components, they are converted to the rank of primary. Taking into account the above, it is possible to regroup these components into a new Ishikawa cause-effect diagram (Fig. 6).

The resulting transformed Ishikawa cause-effect diagram (Fig. 6) takes into account primary factors similar to those shown in Fig. 2:

1. General characteristics of MI SW: 1.1 – documentation of SW manufacturer (P1, U1); 1.2 – SW identification (P2, U2); 1.3 – SW authenticity and presentation of results (U8); 1.4 – influence of other SW (U9); 1.5 – indication for a customer (I1-6, I2-6, I3-6, I4-6).

2. Protection of MI SW: 2.1 – parameter protection (P7, U7); 2.2 – confidentiality of keys (L5, T5); 2.3 – protection against accidental or unintentional changes (P5, P6, U5, U6, L2, T2); 2.4 – protective SW interface (S3); 2.5 – influence via user interfaces (P3, U3); 2.6 – influence via communication interface (P4, U4).

3. Support of hardware functions: 3.1 – failure detection (I1-1, I2-1, I3-1, I4-1, I6-1); 3.2 – traceability of legally relevant SW download (D4); 3.3 – testing of components (I2-9).

4. Separation of parts of MI SW: 4.1 – realization of SW separation (S1); 4.2 – mixed indication (S2).

5. Data storage and transmission: 5.1 – auto-save (L7); 5.2 – completeness of stored data and integrity of data (L1, L3, T3); 5.3 – retrieval of stored data and handling of corrupted data (L6, T6); 5.4 – storage capacity and continuity (L8); 5.5 – authenticity of stored/transmitted data (L4, T4); 5.6 – facilities of data backup (I1-2, I2-2, I3-2, I4-2); 5.7 – transmission delay (T7); 5.8 – completeness of transmitted data (T1); 5.9 – availability of transmission services (T8); 5.10 – prohibition of resetting the cumulative measured values (I1-5, I2-5, I3-5, I4-5).

6. SW maintenance and configuration: 6.1 – download mechanism (D1); 6.2 – authentication of downloaded SW (D2); 6.3 – integrity of downloaded SW (D3); 6.4 – monitoring of battery life (I2-7); 6.5 – internal permission (I1-4, I2-4, I3-4, I4-4); 6.6 – possibilities of "waking-up" and restoration (I1-3, I2-3, I3-3, I4-3).

The proposed algorithm for testing the MI SW on the basis of sharing the requirements of the OIML document and WELMEC guide are shown in Fig. 7.

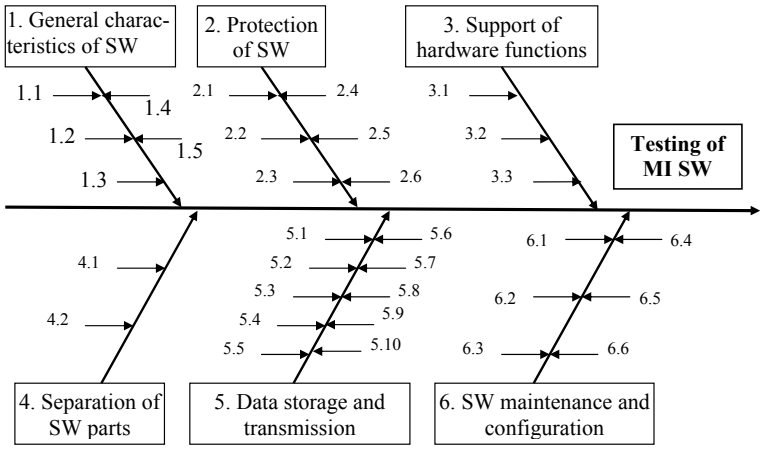

Fig. 6. Transformed Ishikawa cause-effect diagram for the testing of MI SW in accordance with OIML D 31 and WELMEC 7.2

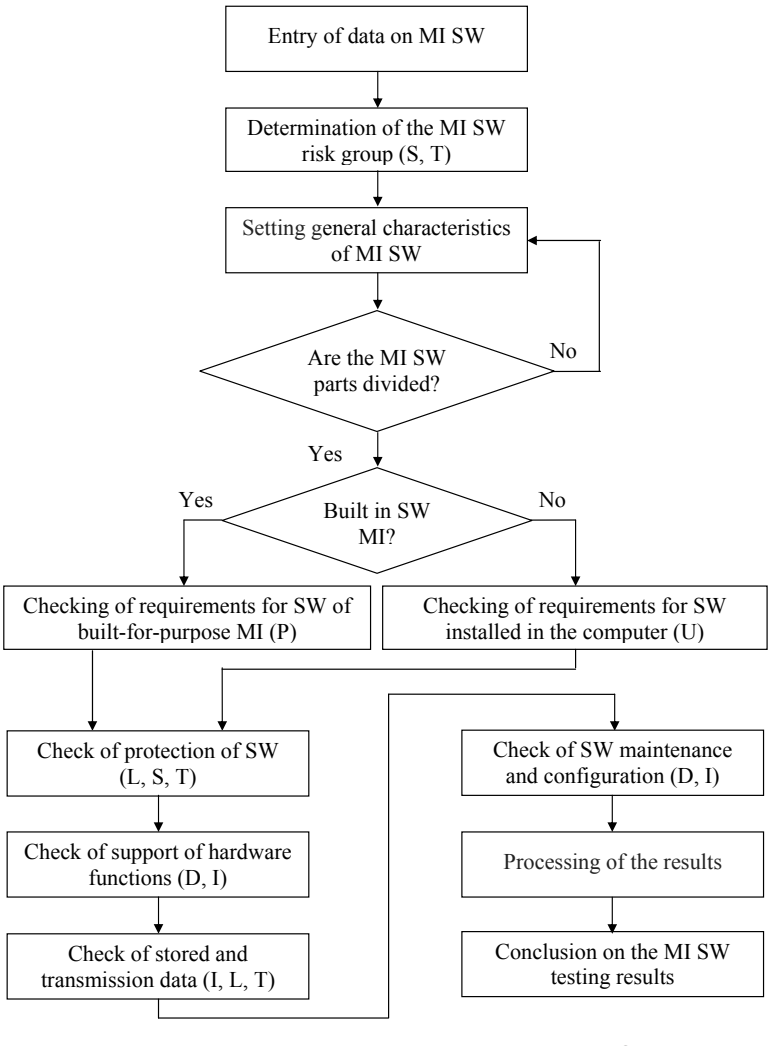

Fig. 7. The proposed algorithm for testing the MI SW

Based on the results of the analysis of the OIML international document and the WELMEC regional guide, the transformed Ishikawa cause-effect diagram was constructed (Fig. 6) and the main factors regarding the approaches to MI SW quality testing were identified. On the basis of the conducted research, an algorithm for testing the SW for the MI in accordance with the requirements of OIML and WELMEC (Fig. 7) was proposed.

The documents and recommendations of the international and regional metrology organizations OIML and WELMEC for the MI SW testing are widely used in the field of legal metrology of various developed countries. However, the requirements of the OIML document and the WELMEC guide must be agreed. It is therefore advisable to take into account the provisions of these documents at the national level by adopting specific national regulations or standards for testing the MI SW.

For the realization of these normative documents or standards, it is necessary to work out the special checklists for estimation of MI SW taking into account different risk classes (Table 1 and 2). For the preparation of special checklists, the developed Ishikawa cause-effect diagrams can be used (Fig. 2, 4, 6).

Using the original Ishikawa cause-effect diagram shown in Fig. 4, special checklists taking into account the requirements of the WELMEC guide for all categories of MI included in Annexes of MID can be prepared [6].

At the same time, using a the transformed Ishikawa cause-effect diagram (Fig. 6) and the proposed algorithm for testing the MI SW (Fig. 7), special universal checklists taking into account joint requirements of the OIML document and WELMEC guide can be prepared. This will allow estimating the SW of practically all categories of MI.

8. Conclusions

1. The analysis of the general requirements for the testing of the MI SW, as set out in the OIML document and the WELMEC guide, has been carried out. The necessity to take into account the requirements of these documents and guide at the national level as special national standards or standards for testing the MI SW was determined. Based on the results of the analysis, the Ishikawa cause-effect diagrams were constructed and key factors regarding the approaches in the OIML and WELMEC documents regarding the testing of the MI SW quality were identified.

2. The algorithms for testing the SW for MI in accordance with the requirements of documents of international and regional organizations of legislative metrology OIML and WELMEC were defined and investigated. A universal MI SW testing algorithm was proposed.

3. The possibility of joint use of the requirements of the OIML document and WELMEC guide has been explored, for which the general Ishikawa cause-effect diagram has been developed. Main factors determined using the Ishikawa diagram can be used for the development of special checklists for testing the MI SW taking into account different risk classes were established. These special universal checklists take into account the general requirements of the OIML document and the WELMEC guide and allow evaluating SW for virtually all categories of MI. This will confirm the authenticity and quality of the MI SW appraisals.

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 J. Europ. Union, L96/149 at 29.2.201. 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: 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: 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: 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: 10.4028/www.scientific.net/kem.381-382.599
11. Samoshina M. A., Baranov V. A. Metodika attestacii programmnogo obespecheniya sredstv izmereniy // VII Mezhdunarodnaya studencheskaya elektronnaya nauchnaya konferenciya «Studencheskiy nauchniy forum» – 2015. 2015. URL: https://www.science-forum.ru/2015/pdf/9003.pdf
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: 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: 10.15439/2015f127
14. Software risk assessment and evaluation process (SRAEP) using model based approach / Sadiq M., Md. Khalid Imam Rahmani Mohd. Wazih Ahmad, Jung S. // 2010 International Conference on Networking and Information Technology. 2010. doi: 10.1109/icnit.2010.5508535
15. Jacobson J. Validation of software in measuring instruments // Computer Standards & Interfaces. 2006. Vol. 28, Issue 3. P. 277–285. doi: 10.1016/j.csi.2005.07.006
16. 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.

Запропоновано формальні моделі основних етапів обробки даних в реконфігуровних комп'ютерних системах, що враховують вплив затримок передавання конфігураційних даних на ефективність обчислень та дозволяють оцінити і оптимізувати непродуктивні витрати часу на реконфігурацію обчислювального середовища на ПЛІС. Запропоновано формалізацію концепції адаптивного відображення алгоритмів на реконфігуровне обчислювальне середовище в режимі часу виконання, що базується на багаторівневому кешуванні конфігураційних даних

Ключові слова: реконфігуровні комп'ютерні системи, часткова динамічна реконфігурація, накладні витрати реконфігурації, відображення алгоритмів

Предложены формальные модели основных этапов обработки данных в реконфигурируемых компьютерных системах, учитывающие влияние задержек передачи конфигурационных данных на эффективность вычислений и позволяющие оценить и оптимизировать непроизводительные затраты времени на реконфигурацию вычислительной структуры на ПЛИС. Предложена формализация концепции адаптивного отображения алгоритмов на реконфигурируемую вычислительную среду в режиме времени выполнения, которая основана на многоуровневом кэшировании конфигурационных данных

Ключевые слова: реконфигурируемые компьютерные системы, частичная динамическая реконфигурация, накладные расходы реконфигурации, отображение алгоритмов

UDC 004.272.26, 004.274
DOI: 10.15587/1729-4061.2018.127361

FORMALIZATION OF THE CONCEPT OF ADAPTIVE TASKS MAPPING IN THE RECONFIGURABLE COMPUTERS ON FPGA

I. Klymenko
Doctor of Technical Sciences, Associate Professor*
E-mail: ikliryna@gmail.com
V. Tkachenko
PhD, Associate Professor*
E-mail: tkavalivas@gmail.com
A. Serhienko
Postgraduate student**
E-mail: ananserr@yahoo.com
Y. Kulakov
Doctor of Technical Sciences, Professor*
E-mail: ya.kulakov@gmail.com
*Department of Computer Engineering***
Department of System Programming and Specialized Computer Systems*
***National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
Peremohy ave., 37, Kyiv, Ukraine, 03056

1. Introduction

The result of the high level of modern progress is that extensive technologies of increasing the performance of high-speed processing reach their extreme opportunities. This is confirmed by violations of Moore's law in recent years [1]. The desire to increase performance further to the *exaflops* level makes the challenge to find the new intensive solutions. The dynamically reconfigurable computer systems [2–4] are one of such solutions. Their creation became possible on the base of modern technology of the partial dynamic reconfiguration (PDR) of the FPGA [3]. This direction is rapidly expanding today. The most advanced classes of tasks, which are solved in the dynamically reconfigurable computers, are the tasks of real-time control, particularly in undefined conditions, which have informational, multidimensional and dynamical nature [5–8].

In contrast to the static reconfiguration [9, 10], the dynamical reconfiguration is a precondition for the creation of the computing structures, adapted to the requirements of *Run Time* mode tasks solution [3, 11–13]. Firstly, this allows to overcome the limitations of the firm architecture of the high-speed multipurpose computer systems and to approach the real processing performance to the declared