Journal of Electrical Engineering and Information Technologies, Vol. **10**, No. 1 pp. 5-11 (2025)
Article 226
Received: 16.12.2024
Accepted:22.04.2025
In print: ISSN 2545–4250
On line: ISSN 2545–4269
UDC: 004.413.4:621.317.7]:519.248

Original scientific paper

RISK ASSESSMENT FOR TESTING MEASURING INSTRUMENT SOFTWARE

Valentyn Gaman[1)] Oleh Velychko[2)] Serhii Kursin [3)]

[1,2,3,] All-Ukrainian State Research and Production Center for Standardization, Metrology, Certification and Consumers' Rights Protection", 4 Metrologichna str., 03143 Kyiv, Ukraine

[1)] velychko@hotmail.com

Abstract: This article is devoted to analysis and development of methodology to assess total risks from use of measuring instrument software based on subjective assessment of the probability of threats and the possible extent of damage. In the absence of statistical data on the probability for occurrence of threats and data on the possible size of losses from realization of these threats, it is suggested to use expert assessment on distribution of probabilities and size of the loss with assignment of conditional points. The proposed classification of possible threats and vulnerabilities in measurement software can be used to establish the overall risk for all threats. A generalized procedure for assessing specific risks has been developed to determine the level of verification during software testing of measuring instruments

Keywords: risk assessment, software, measuring instruments, testing, risk identification, risk analysis.

ПРОЦЕНКА НА РИЗИЦИ ОД УПОТРЕНА НА СОФТВЕР ЗА ТЕСТИРАЊЕ МЕРНИ ИНСТРУМЕНТИ

Апстракт: Статијата е посветена на анализа и развој на методологија за проценка на вкупниот ризик од употребата на софтвер на мерни инструменти врз основа на субјективна проценка на веројатноста од закани и можниот обем на штета. Во отсуство на статистички податоци за веројатноста на појава на закани и податоци за можната големина на загубите од спроведувањето на овие закани, се предлага да се користи стручна проценка за распределба на веројатностите и големината на загубата со доделување на условни точки. Предложената класификација на можните закани и пропусти во мерниот софтвер може да се користи за да се утврди севкупниот ризик од сите закани. Развиена е генерализирана процедура за проценка на конкретни ризици за да се одреди нивото на верификација при софтверско тестирање на мерните инструменти..

Клучни зборови: проценка на ризици, софтвер, мерни инструменти, тестирање, идентификација на ризици, анализа на ризици.

I. INTRODUCTION

MEASUREMENT data is an important stage in solving scientific problems and improving technical processes. Measuring instruments play an important role in science and technology, in various aspects of research and technology development. Important aspects of the role of measuring instruments include research for acquisition of reliable data and development of technologies, control of production processes and their quality, ensuring high accuracy and reliability of equipment, etc. The vast majority of modern measuring instruments contain special software. Such software must provide efficient processing and analysis of data received to ensure accurate measurements. It must interact with a specific measuring device, support various communication protocols and ensure its stable operation. The software should have capabilities to support automated processes of measurements and data processing for efficiency and reduction of measurement time, save and restore data to ensure archiving of measurement results, convenient management of databases, etc.

Most modern measuring instruments use microcontrollers or are controlled by computers. The software of such measuring instruments makes it possible not only to automate the processes of measurement and calculation of results, but also to ensure long-term storage and transmission of data, which significantly increases the risks of economic and other losses due to possible distortion of measurement results. Software testing is an important part of development, but they can also face various risks that can affect the product's quality and reliability. The main risks of software testing include: insufficient test plans, incorrectly defined requirements and inadequate data for testing, insufficient performance and security testing, insufficient testing process and lack of

its automation, unpredictable reactions to real conditions, etc. Managing these risks requires clear planning and a systematic approach to testing, which directly affects quality of the tests and detection of possible defects. The manufacturer of measuring instruments is responsible for researching and evaluating all possible risks.

II. Literature Review

The requirements stipulated in international standards on information security risk management [1], security assessment in the field of information technology [2], and information technology security assessment criteria [3] contain only general issues of software security and risk assessment without taking into account the scope of its application. The main principles of software risk assessment are given in [1], including the following procedures: risk identification, risk analysis, and risk assessment. An algorithmic approach to risk assessment of measuring instrument software is proposed in [4]. This document defines a specific set of functionality and corresponding security properties for measuring devices and offers a list of possible threats. However, this document covers only a few types of software-based measurement instruments.

The risk assessment analysis algorithm using the attack probability tree for taximeters is given in [5]. It is argued that it is impossible to assess the level of risks based on technical data alone without due consideration of other factors. The procedure for the threat relating to reading memory cores by unprivileged software user is shown in [6] as practical example. A simplified software risk assessment procedure is proposed in [7], but only for some threats to an ideal measurement instrument. A generalized risk assessment procedure for non-automatic weighing devices and measuring devices is given in [8], to which recommendations [9] are applied.

The results of a comparative analysis of general requirements in documents and guidelines of international and regional organizations of legal metrology regarding software testing for measuring instruments are given in [10], [11]. These works define the main indicators of the software for measuring instruments, both with built-in and external software.

III. Problem Statement

The reviewed literature, however, pays only general attention to risk assessment of software application to different categories of measuring instruments.

The purpose of the study examined in this article is to develop a methodology for assessing total risks from use of measuring instrument software, based on subjective assessment of the probability of threats and the possible extent of damage.

IV. Materials and Methods

Manufacturers must analyze and assess risks associated with use of measuring instrument software. However, not all threats related to functioning of measuring instruments may concern their software. Adequacy of the scope of measuring instrument tests themselves depends on correctness of software risk assessment.

Software threats can be classified into two main groups: intentional (I) and accidental (A) [1]. Among known types of threats, those that relate directly to measuring instrument software can be singled out here: functioning, data storage, and data transfer (Table 1). Threats that affect functioning include only those that could distort measurement results. Threats affecting data storage include those that could lead to data corruption or destruction. Threats affecting data transmission include those that could result in data corruption during transmission or data loss due to loss of telecommunications connection.

To determine possible threats to the software, it is necessary to study the measuring instrument's generalized structural diagram, the internal relationships between individual blocks of hardware and software modules. A generalized structural diagram of typical measuring instrument with software is presented in Figure 1. Interrelationships of structural elements and their functions are marked on the diagram.

Table I
Kinetic Parameters Obtained by Deconvolution

Type of harms	Source of threats	Type of threats	Manifestation*
1. Physical damage	1.1. Fire	I, A	LD, DC
	1.2. Water		
	1.3. Mechanical impact		
2. Natural events	2.1. Temperature	A	
	2.2. Humidity		
3. Malfunctions due to radiation	3.1. Electromagnetic radiation	I, A	
	3.2. Electromagnetic pulse		
4. Loss of necessary services	4.1. Loss of power supply		
	4.2. Failure of telecommunications equipment		DC
5. Technical failures	5.1. Equipment failure	A	LD, DC
	5.2. Equipment halting		
	5.3. Software crash		DM, LD, DC
6. Information compromising	6.1. Intercepting and sending compromised signal	I	DT
	6.2. Theft of data carriers		LD
	6.3. Theft of equipment		DC

Type of harms	Source of threats	Type of threats	Manifestation*
	6.4. Hardware tampering		DD, DT, DC
	6.5. Software tampering		DM
7. Unauthorized actions	7.1. Data distortion		DD, DT
8. Functions compromising	8.1. Error in use	I	LD, DC
	8.2. Abuse of rights	I, A	
	8.3. Falsification of rights	I	DD, LD, DT
	8.4. Denial of action		LD, DC

*Legend: LD is data loss; DC is disconnection of the communication line; DT is distortion during data transmission; DD is data distortion; DM is distortion of measurement results.

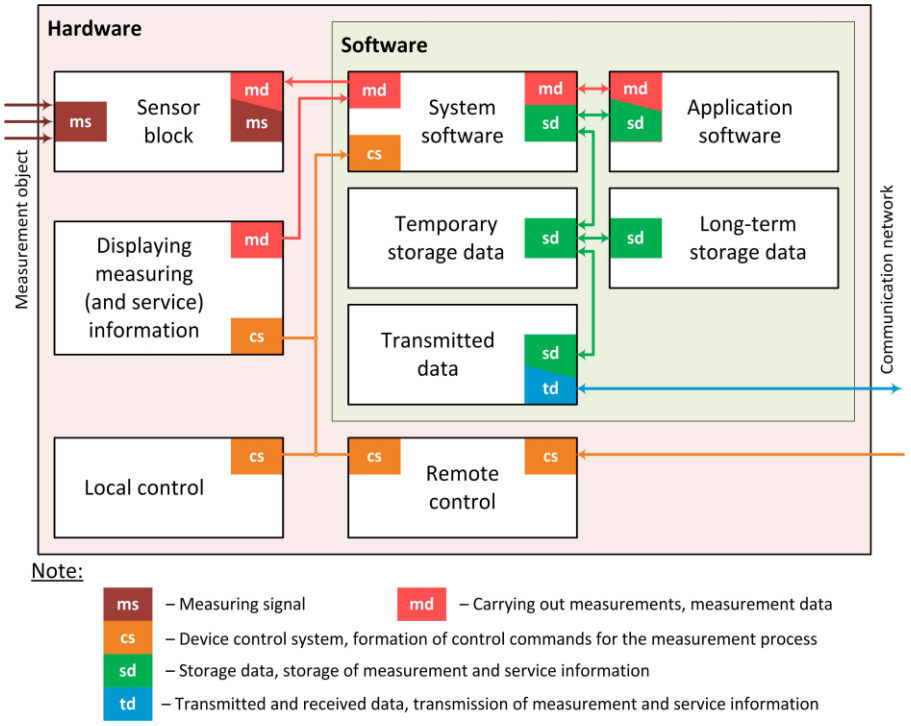

Fig. 1. A generalized structural diagram of typical measuring instrument with software

The hardware of a typical measuring instrument consists of the following blocks:

- **sensor,** which contains measuring transducers for obtaining measurement information from the measurement object (transformation of measurement signal into corresponding digital code);
- **local control,** which is an interface for manual control of the measuring instrument;
- **remote control,** which provides control of the measuring instrument by external devices using data reception-transmission interfaces and can be either cabled or wireless;
- **display,** which shows measuring (and service) information in modern measuring instruments and, in the case of touch screens, could be combined with a local control unit;
- **microprocessor with software.**

The software of typical measuring instrument consists of the following blocks:

- **system software**, which provides general control of the measuring instrument;
- **application software,** which provides execution of measurement algorithms, calibration, self-calibration, calculations, etc.;
- **temporary storage data**, which is necessary for storage of operational measurement information for the purpose of further processing, long-term storage or transmission;
- **long-term data storage**, which ensures long-term storage of measurement information;
- **transmitted data,** which is intended to form data for transmission or reception over a communication network.

It should be noted that the software's operation depends entirely on the hardware.

Figure 2 provides an overview of software vulnerabilities classification for measuring instruments. Software vulnerabilities can be conditionally divided into personnel, hardware and software, and network vulnerabilities. To ensure proper protection of measuring instruments and measurement results, and to secure data from possible threats, manufactures must take into account the maximum number of vulnerabilities. Any vulnerability that is not accounted for or insufficiently assessed increases the risk of exposing the measuring instrument to one or another threat.

An urgent task is to develop a risk assessment methodology based on typical structural diagram of typical measuring instrument with software, and proposed risk classification. At the same time, it is advisable to define a scoring scale and calculate limit values of specific risks. Risk is defined as the probability of harm due to certain vulnerability, taking into account the conditional amount of harm.

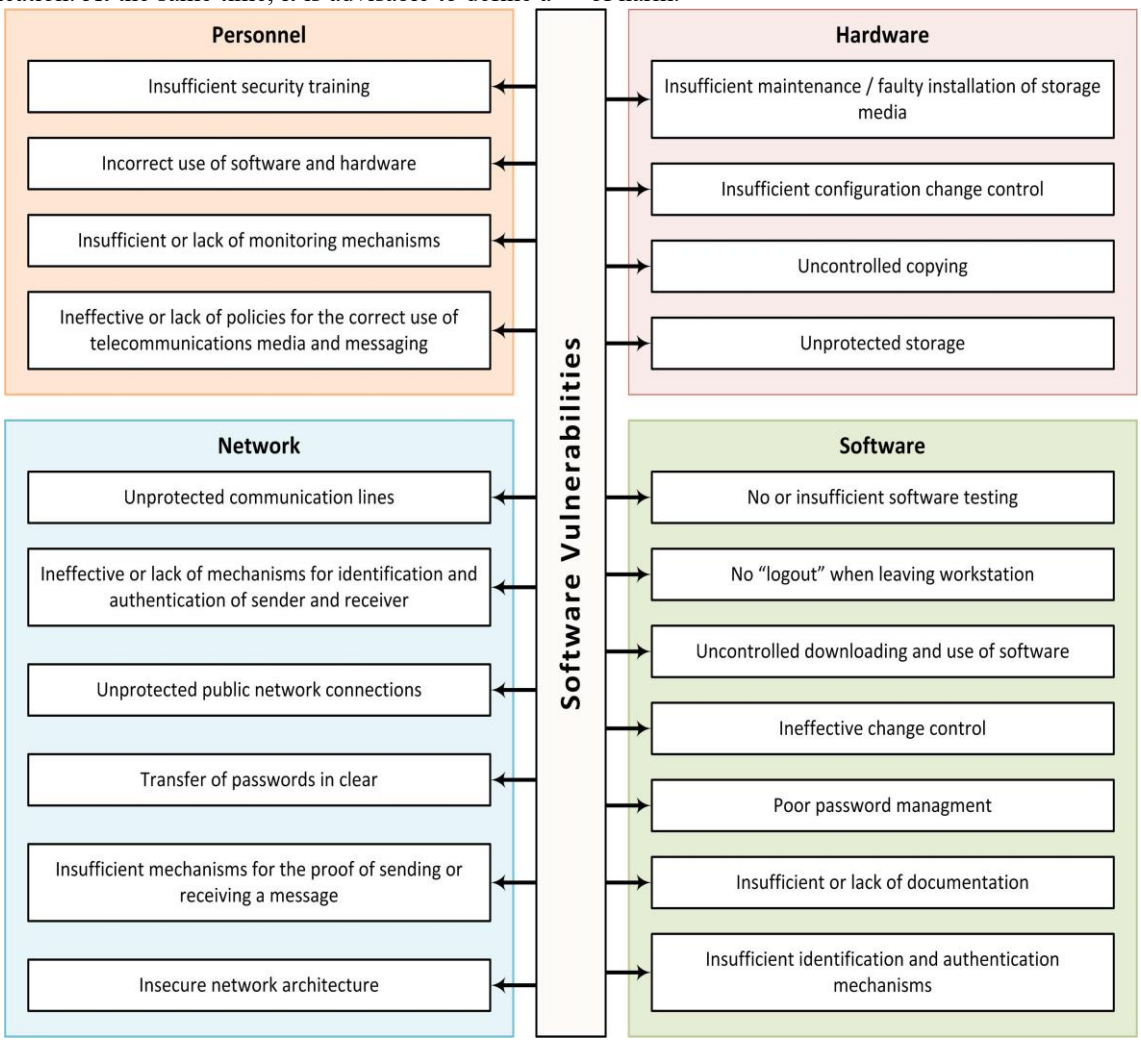

Fig. 2. Classification of measuring instrument software vulnerabilities

V. Results and Discussion

To assess the probability of threats and damage, in the absence of statistical data on use of certain type of measuring instruments, statistical data for similar types or general class of measuring instruments should be used. In the absence of posteriori information, it is necessary to assess threats and harms by taking into account available data on measuring instrument functionality and the expert's subjective assessment.

The probability for occurrence of threats can be estimated by three values: low (L), probable (P) and certain (C), with conditional values of 0.1, 0.5 and 0.9, respectively. Similarly, possible damages and their corresponding conditional points can be estimated: certain inconveniences (CI), material damages (MD), and threats to life and health (LH) with conditional values of 0.1, 0.5 and 0.9, respectively.

Data on assessment of occurrence of threats (Pi) for measuring instrument software according to the classification in Table 1 are presented in Table 2 (Pmax is maximum probability of a threat occurring due to certain vulnerability, Dmax is maximum expected amount of damage (loss) that could be caused by a realized threat).

The software cannot predict or reduce the impact of mechanical damage related to sources of danger such as fire, water, and mechanical impact. Given that, in the event of such measurement damage, data storage and transmission are impossible, the probability of receiving unreliable measurement data is zero. Also, it is impossible to prevent loss of temporary storage data and saved data by hardware or software means. Therefore, these factors are excluded from the software risk assessment. Similarly, the risk assessment excludes out-of-range measuring instrument operating conditions as they do not affect the software's functioning when the equipment is operating.

Sources of malfunction threats due to radiation are electromagnetic radiation (R1.1) and electromagnetic pulse (R1.2). If there are no measuring instruments for measuring electromagnetic field parameters, software tools cannot predict the occurrence of this impact factor. A measuring instrument must be designed with electromagnetic compatibility requirements in mind, but there is still a chance (5%) that particular example of measuring instrument does not meet the established electromagnetic compatibility requirements. Otherwise,

there is a possibility for failure when saving and transferring data (taking into account electromagnetic compatibility).

TABLE II
DATA ON ASSESSMENT OF OCCURRENCE OF THREATS FOR MEASURING INSTRUMENT SOFTWARE

Type of harms	Source of threats	Main manifestation	P_{max}	D_{max}
1. Malfunctions due to radiation	1.1. Electromagnetic radiation	Does not affect the software's operation	0.9	0.5
	1.2. Electromagnetic pulse		0.9	0.5
2. Loss of necessary services	2.1. Loss of power supply	Measurement is not possible	0.1	0.5
	2.2. Failure of telecommunications equipment	There may be a delay in data transmission until the connection is restored	0.5	0.1
3. Technical failures	3.1. Equipment failure	The probability for occurrence of this factor is entirely due to the hardware	0.1	0
	3.2. Equipment halting		0.5	0.5
	3.3. Software crash	Possible failure when saving and transferring data	0.1	0.5
4. Information compromising	4.1. Intercepting and sending compromised signal	It does not affect the operation of the software and the saving of data	0.1	0.5
	4.2. Theft of data carriers	If the internal carriers or equipment are lost, the measuring instrument may be inoperable. It is impossible to prevent possible loss of data stored on external carrier. This does not affect the software's operation and data transfer	0.1	0.5
	4.3. Theft of equipment		0.1	0.5
	4.4. Hardware tampering	It is impossible to predict or reduce losses from the possible impact of this factor by software means. Storage of invalid values, loss of data, transmission of invalid values is possible	0.1	0.9
	4.5. Software tampering	It is possible to affect accuracy of measurements, inoperability of the measuring instrument. It does not affect data storage and transmission	0.1	0.9
5. Unauthorized actions	5.1. Data distortion	Affects data retention, including temporary, but does not affect data transfer	0.1	0.9
6. Functions compromising	6.1. Error in use	Depends on the measuring instrument's complexity, does not affect data storage and transfer	0.1	0.5
	6.2. Abuse of rights	Distribution of rights is not provided, does not affect data storage and transfer	0.1	0.5
	6.3. Falsification of rights		0.1	0.5
	6.4. Denial of action	Built-in functions should not contain these actions; it does not affect data storage and transfer	0.1	0.5

In case of loss of service during operation of the measuring instrument software, it should be understood as loss of power supply (R2.1) and failure of telecommunication equipment (R2.2). The loss of power supply implies the following characteristics: impossibility of the software to predict or reduce losses from the possible impact of such failure, whereby the probability of receiving unreliable measurement data is zero, but data cannot be saved and transferred. To prevent or reduce the impact of this factor, it is necessary to use battery power or uninterruptible power supply units. Another setback concerns possible loss of unsaved or untransmuted data in the absence of data storage. This factor does not affect the state of saved data, as this probability is zero when batteries are used. When data being transferred have particular value, they must be stored beforehand, with the saving function frequency (number of saving functions per unit of time) set in proportion to their value. To mitigate the impact of telecommunication equipment failure, due consideration should be made of the fact that it is impossible for the software to predict occurrence of this impact factor. Hence, the construction of the data transmission channel should provide for temporary storage of data and transmission of data when the connection is restored.

Technical failures can include equipment failure (R3.1), equipment halt (R3.2), and software crash (R3.3). It is impossible for the software to predict occurrence of equipment failure and therefore the probability for occurrence of this factor falls entirely on the hardware. In case of software failure, it is necessary to account for the probability for failure of these structural elements as embedded software (system and application software), data storage and transfer modules, operating system (in case of using a universal computer). Thus, expressions for the probability of software crash dependent on its functioning are the following:

$$P_{33} = P_P + P_L + P_T, \quad (1)$$

$$P_{33} = P_U + P_O - P_U \cdot P_O + P_L + P_T, \quad (2)$$

where P_P is the probability for failure of embedded software, P_U is the probability for failure of universal software, P_O is the probability for failure of the operating system, P_L is the probability for failure of data storage modules, P_T is the probability for failure of data transfer modules, $P_U \cdot P_O$ is the probability that failure of the operating system will affect software work (equal to 0.1).

Information compromising can be caused by threats such as interception and dispatch of compromised signal (R4.1), and theft of carriers (R4.2, R4.3). The software cannot predict or mitigate the potential impact of interception and transmission of compromised data or data theft.

Interception is carried out on the communication line, necessitating use of protection that corresponds to the value of data that are being transmitted. When internal media is lost, the measuring device may become inoperable. Theft of equipment is characterized by loss of some or all measuring instrument parts, which the software cannot predict or reduce losses caused by this factor. It is equally impossible for the software to predict and prevent loss of stored data. Hardware tampering (R4.4) may affect accuracy of measurements. It is impossible to programmatically predict or reduce losses caused by this factor. This could also lead to possible storage of invalid values and loss of data, and transfer of invalid values. Software tampering (R4.5) is another possible factor that could lead to inaccuracy of measurements. In the case of measuring instrument malfunction, no measurements are taken, with a probability of 0.5 that such occurrence would lead to change of accuracy.

Interception is carried out on the communication line, necessitating use of protection that corresponds to the value of data that are being transmitted. When internal media is lost, the measuring device may become inoperable. Theft of equipment is characterized by loss of some or all measuring instrument parts, which the software cannot predict or reduce losses caused by this factor. It is equally impossible for the software to predict and prevent loss of stored data. Hardware tampering (R4.4) may affect accuracy of measurements. It is impossible to programmatically predict or reduce losses caused by this factor. This could also lead to possible storage of invalid values and loss of data, and transfer of invalid values. Software tampering (R4.5) is another possible factor that could lead to inaccuracy of measurements. In the case of measuring instrument malfunction, no measurements are taken, with a probability of 0.5 that such occurrence would lead to change of accuracy.

Distortion of data (R5.1) may occur during their storage, including temporary data and coefficients. At the same time, it is possible for such occurrence to affect accuracy of measurements. If coefficients are not used, this probability is zero.

Software functions compromising is possible in cases of defects in software development and accompanying documentation, and should be anticipated and eliminated at these stages. The error of using the program (R6.1) depends on the measuring instrument's complexity, which is associated with complex user interface, unclear documentation, absence of user manual, non-typical data formats (e.g., date recording). Abuse of rights (R6.2) can be associated with both, poor management of software development (insufficient testing, insufficient number of revisions, lack of automatic session closure in case of inactivity during a certain period) and incorrect distribution of access rights to software functionality. Forgery of rights (R6.3) can be caused by weaknesses in identification mechanisms for user authentication, forgery of access rights, insecurity of password and key tables. Denial of action (R6.4) is related to either inadequate segregation of information security duties or lack of confirmation for data sending or receiving on data interfaces.

Risk is defined as the probability of harm due to certain vulnerability, taking into account the conditional amount of harm. Numerically, the risk of separate vulnerability is determined by the following expression:

$$R_i(x) = P_i(x) \cdot D_i(x) \quad (3)$$

where $P_i(x)$ is the probability of a threat occurring due to certain vulnerability x; $D_i(x)$ is the expected amount of damage (loss) caused by the realized threat.

Risk is measured in units of damage (loss) caused by the hazard. The amount of damage is clearly determined by certain losses of the measuring instrument supplier or consumer. Determining this amount for software measuring tools is a difficult task. To develop a general methodology for assessment of such risks, it is appropriate to use conditional units (scores) that generally characterize the extent of possible damage due to certain threats.

The value of this probability can be estimated by taking into account statistical data on occurrence and realization of certain threats for specific types of measuring instruments. If such data are not available, it is advisable to use subjective probability assessments for occurrence of accidental event threats and presence of malicious intent for intentional events, and divide the probability of threats into three groups: low (L), medium (M), and high (H). Similarly, it is possible to distribute the amount of damage.

The total risk is calculated as the sum of risks for each vulnerability, as given in the following expression:

$$R_\Sigma = \sum_{x=1}^{N} R_i(x) = \sum_{x=1}^{N} \left[P_i(x) \cdot D_i(x) \right] \quad (4)$$

To assess the overall risk of measurement software, it is necessary to define conditional scores for both probabilities (P_i) and values of possible damage (D_i).

VI. Conclusion

In the absence of statistical data on the probability for occurrence of threats and data on the possible size of losses from realization of such threats, it is suggested to use expert assessment for distribution of probabilities and size of the loss with assignment of conditional points. Conditional scores are used to calculate and assess overall risk for all threats.

The proposed classification of possible threats and vulnerabilities in measurement software related to functions such as receiving, storing and transmitting

measurement data can be used to establish the overall risk for all threats. A generalized procedure for assessing specific risks has been developed in order to determine the level of verification during testing of measuring instrument software.

REFERENCES

[1] ISO, Information Technology – Security Techniques – Information Security Risk Management, ISO/IEC 27005. 2022.

[2] ISO, Common Methodology for Information Technology Security Evaluation, ISO/IEC 18045, 2008

[3] ISO, Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408, 2012.

[4] M. Esche and F. Thiel. “Software Risk Assessment for Measuring Instruments in Legal Metrology”, in Federated Conference on Computer Science and Information Systems (FedCSIS), Lodz, Poland, 2015, pp. 1113-1123.

[5] M. Esche, F. G. Toro, and F. Thiel. “Representation of Attacker Motivation in Software Risk Assessment Using Attack Probability Trees”, in Federated Conference on Computer Science and Information Systems (FedCSIS), Prague, Czech Republic, 2017, pp. 763-771.

[6] M. Esche and F. G. Toro. “Developing Defense Strategies from Attack Probability Trees in Software Risk Assessment”, in 15th Conference on Computer Science and Information Systems (FedCSIS), Sofia, Bulgaria, 2020, pp. 527-536.

[7] F. G. Toro, M. Koval, M. Esche. “Proposal for Simplified Implementation of Risk Assessment Method for Measuring Instruments”, in Federated Conference on Computer Science and Information Systems (FedCSIS), Poznan, Poland, 2018, pp. 43-47.

[8] WELMEC, Software Risk Assessment for Measuring Instruments, WELMEC Guide 07.06.2021. [Online]. Available at: https://www.welmec.org/welmec/documents/guides/7.6/2021/WELMEC_Guide_7.6_v2021.pdf.

[9] WELMEC, Software Guide (Measuring Instruments Directive 2014/32/EU1), WELMEC 07.02.2021. Issue 9. [Online]. Available at: https://www.welmec.org/welmec/documents/guides/7.2/2021/WELMEC_Guide_7.2_v2021.pdf.

[10] O. Velychko, T. Gordiyenko, and O. Hrabovskyi. “Testing of Measurement Instrument Software on the National Level”. Eastern-European Journal of Enterprise Technologies. Information and Controlling Systems, 2/9 (92), 2018, pp. 13–20.

[11] O. Velychko, V. Gaman, T. Gordiyenko, and O. Hrabovskyi. “Testing of Measurement Instrument Software with the Purpose of Conformity Assessment”. Eastern-European Journal of Enterprise Technologies. Information and Controlling Systems, 1/9 (97), 2019, pp. 19–26.