DOI 10.5162/sensoren2016/P7.4

Incorporating a Measure for Attacker Motivation into Software Risk Assessment for Measuring Instruments in Legal Metrology

Dr.-Ing. Marko Esche, Dr.-Ing. habil. Florian Thiel
Physikalisch-Technische Bundesanstalt, Abbestr. 2-12, 10587 Berlin

Abstract

Modern measuring instruments mainly rely on software to perform their intended operations. Measuring instruments are thus also susceptible to malicious software-related attacks. Especially in the highly regulated area of legal metrology, risk assessment is one possible tool for assessing the resistance of an instrument to unintended modifications and intentional manipulations. Where previous risk assessment approaches solely relied on the technical features of the instrument, the authors here propose a method that also covers the important influence factor of attacker motivation. Based on two different solutions to the problem, a well-suited method is selected with the help of a short experimental evaluation.

Keywords: measuring instruments, conformity assessment, software risk assessment, Common Criteria, attacker motivation

Introduction

In Europe, certain types of measuring instruments and measuring systems are subject to European and national regulations concerning the procedure of putting them on the market and the means for inspecting and testing them during use. Among these instruments are such diverse types as taximeters, fuel pumps, and speed measuring instruments for traffic control. All requirements, that such instruments have to meet, are detailed in Annex I of the Measuring Instruments Directive (MID) 2014/32/EU [1]. Conformity to those requirements is assessed by so-called Notified Bodies according to a set of predefined modules, which may be found in Annex II of the Directive [1].

In Germany, one such Notified Body is the Physikalisch-Technische Bundesanstalt, Germany's national metrology institute. In April 2016, a new requirement will come into force stating that the documentation submitted for conformity assessment shall be accompanied by an adequate assessment of the risks associated with the instrument. Since measuring systems are steadily becoming more complex and rely to a great extent on software for producing correct measuring results, simple technical requirements will not be able to cover all aspects of a measuring system in the future. Instead, the conformity assessment will depend to a great extent on the performed risk analysis. This analysis should have the severity of a breach of the essential requirements at its core, since loss of life or financial damages are beyond the aims of protection of the MID.

In light of the common European market, harmonization of such a risk assessment procedure is desirable with the aim of facilitating the recognition of assessment results among member states. Software risk assessment methods already in place either require the conduction of larger surveys [2] or are based on data, such as source code [3], which are usually not available to the Notified Body. Because of these deficiencies, the authors have developed a new risk assessment procedure [4] based on the ISO/IEC standards 27005 [5], 15408 [6], and 18045 [7]. The method will be briefly revisited in the next Section. Additional details and examples may be found in [4]. One of the major drawbacks of the method, nevertheless, is its dependency on the technical features of a device alone. As will be shown in this paper, attacker motivation and its representation during risk assessment also plays an important role. The remainder of the paper is structured as follows: In the next section, the risk assessment method from [4] is briefly revisited and two possible ways to include attacker motivation are outlined. Afterwards, both of these are in turn mathematically described and examined with the help of two real-world examples. Based on the outcome of the investigation, an optimal method is selected. A brief summary and an outline of future work conclude the paper.

The Software Risk Assessment Method

According ISO/IEC 27005, “risk is a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event.” [5] The procedure from [4] consists of a three-part process (see Figure 1).

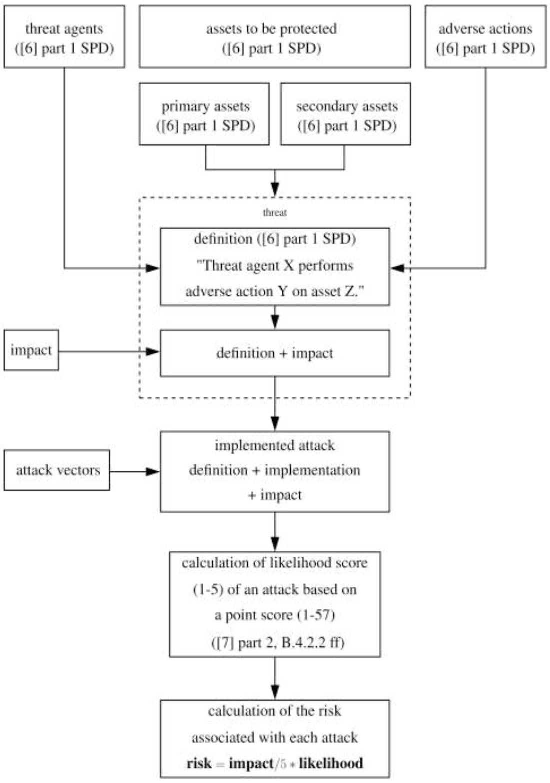

Fig. 1: Outline of the risk assessment workflow originally published in [4].

In a first step (top part of Figure 1), the legislative text is transformed into formal assets to be protected with associated security properties. Requirement 8.3 from Annex I of the MID, for instance, reads, “Evidence of an intervention shall be available for a reasonable period of time.” [1, L 96/173] The asset in this case is the evidence of an intervention. The security property of the asset is availability. Another requirement 7.6 states, “When a measuring instrument has associated software which provides other functions besides the measuring function, the software that is critical for the metrological characteristics shall be identifiable and shall not be inadmissibly influenced by the associated software.” [1, L 96/173] Here, two assets can be identified. One is the identification of the software, which shall be available and shall preserve its integrity. Another is the mentioned inadmissible influence. As it shall not be possible to manipulate the software, the respective security property is normally referred to as “unavailability”. Details on the complete derivation process may be found in [4]. For better comprehensibility the resulting list of assets and their security properties is given in Table 1.

Tab. 1: List of assets to be protected and their associated security properties as originally published in [4].

Asset to be protected	Security Property
A1: software critical for metrological characteristics	integrity, authenticity
A2: evidence of an intervention	availability, integrity
A3: measurement data	integrity, authenticity
A4: metrologically important parameters	integrity, authenticity
A5: inadmissible influence on the software	unavailability
A6: indication of the result	availability, integrity
A7: marks and inscriptions accompanying the indication of a result	availability, integrity
A8: record of a measurement result	availability, integrity, authenticity
A9: identification of the software	availability, integrity

Theoretically, this step can be adapted to any other requirement framework, too.

During the second phase of the risk assessment workflow, specific attack scenarios are examined for a given instrument with the aim of showing how one or more security properties of the formal assets can be invalidated. Such attack scenarios can either be constructed by making use of the submitted manufacturer’s documentation and the examiner’s expert knowledge or by referring to external public databases that cover known vulnerabilities of software products in general or measuring instruments specifically.

The last part of the procedure (see bottom part of Figure 1) consists of evaluating the attack scenarios with the help of the vulnerability analysis method from [7]. During this analysis, each attack vector is evaluated with respect to five different categories:

- elapsed time (0-19 points),
- required expertise (0-8 points),
- knowledge of the instrument (0-11 points),
- necessary window of opportunity (0-10 points),
- and equipment needed (0-9 points).

Based on the sum of point scores for each category, a probability score (between 1 and 5) can be computed, where a high sum score (indicating high resilience to attacks) is mapped to a low probability, see Table 2. Said probability score is then multiplied with the estimated impact of the realized threat (see lower part of Figure 1). Usually, an impact is assumed to be high (score of 5) if the threat affects a larger number of measurements. Otherwise, the impact is set to a low value (score of 2).

Tab. 2: Mapping of the sum score to the resistance of the target of evaluation (TOE) and to the probability score, originally published in [4], adapted from [7].

Sum of Points	**TOE Resistance**	**Probability Score**
0-9	No rating	5
10-13	Basic	4
14-19	Enhanced Basic	3
20-24	Moderate	2
>24	High	1

A similar method, that has an application area within the telecommunication sector, is described in ETSI standard TS 102 165-1 [8]. The main advantage of the described approach lies in the possibility to calculate reproducible meaningful risk scores that should be independent from the evaluator. As mentioned in the introduction, the method so far only relies on the technical properties of the examined instrument and does not take into account the motivation of a possible attacker. Two possible solutions for this problem will now be described in the following sections.

Problem Description

So far, the risk assessment procedure relies on the technical specifications of the examined instrument or system only. Subsequently, the likelihood of occurrence of a threat is directly linked to the difficulty of implementing the associated attack. In practice, another important aspect also comes into play: An attack is unlikely to be realized if the prospective attacker has no or little motivation to carry out the attack. In addition, resources or expertise may be bought if an attacker is sufficiently motivated. This fact is currently missing from both procedures described in [4] and [8]. In this context, [7] states that, firstly „motivation can imply the likelihood of an attack“. Secondly, „motivation can imply the expertise and resources with which an attacker is willing to effect an attack.“ Two alternative ways for including attacker motivation into the software risk assessment method from [4] thus present themselves. Both will now be discussed in turn.

Solution No. 1: Additional motivation score

The first alternative consists of establishing an additional motivation score similar to the expertise score defined in [6], section B.4.2.2, where high motivation will be mapped to a low score and vice versa. The mapping used here is given in the first and second columns of Table 2. The expertise score from [6] is shown in the third and fourth columns of Table 3 for comparison. The motivation score is then used in the following manner: Whenever the expertise or equipment scores required for an attack are smaller than the estimated motivation score, their values are replaced with the motivation score. This will essentially decrease the estimated probability of occurrence when the attacker’s motivation is low. The reasoning behind this approach is in line with the suggestions from [7]: Whenever a highly motivated attacker is considered, the original method from [7] remains unchanged as the motivation score is set to 0 and the scores for expertise and resources will not be modified under any circumstances. This relates to the fact that an attacker with high motivation will try to buy resources and expertise whenever required. On the other hand, an attacker with low motivation now imposes an upper bound on the expertise and resources available for an attack. Subsequently, the low motivation will eventually result in a lower TOE resistance and an increased probability score.

Tab. 3: Mapping of the assumed motivation level to a score value (left two columns). The right part shows the mapping between expertise level and score value as defined in [6] for comparison.

Expertise	**Score**	**Motiv-ation**	**Score**
Layman	0	No motivation	9
Proficient	3	Low	6
Expert	6	Moderate	3
Multiple Expert	8	High	0

Solution No. 2: Modifying the calculated probability score

The second alternative aims at modifying the calculated probability score according to the estimated motivation level before multiplying impact with probability. The modification could, for instance, be done by applying a correction factor between 0.7 and 1.3 to the sum score before calculating the probability score which corresponds to an increment or decrement of the attack probability as needed.

Here, the same levels of motivation as for the other method will be used, see Table 4. The assumption behind solution no. 2 is the view that the output of the vulnerability analysis from [7] forms a baseline, which itself should not be modified. The correction is only applied afterwards and can change the result in both directions: An attacker with low motivation will produce a lower probability score as was the case for solution no. 1. However, should the motivation be high, the attacker is now assumed to be able to procure even more resources than initially assumed and thus increase the likelihood of a realized threat.

Tab. 4: Mapping of the selected motivation level to the appropriate correction factor.

Motivation	**Correction Factor** (CF)
No motivation	1.3
Low	1.1
Moderate	0.9
High	0.7

Experimental Comparison

In the following two sections, two real-world examples are examined according to the method described in [4]. Both suggested solutions will then be applied to both examples in turn. In order to be able to evaluate the effect of attacker motivation, the examples have been chosen in such a manner that based on the monetary value of the measured quantities, different levels of motivation can be assumed.

Example No. 1: Grain moisture analyzer

The first measuring instrument examined here is a grain moisture analyzer responsible for measuring the moisture level of a sample of wheat or barley. The instrument consists of a computer module with a single-user operating system for embedded devices connected to a touch screen. The features of the operating system are used to protect the measuring software against modification and replacement and to inhibit attacks on the instrument over open hardware interfaces. The operating system is protected with a six-digit numeric password. A DC motor is used to transport the next measurement sample to a RF-cell where the moisture level is determined and the weight of the sample is measured. Further details concerning the instrument may be seen in Figure 2. The instrument has an open serial port which uses a proprietary protocol to start and stop individual measurements and to read out the measurement result remotely. In addition, the measurement results can optionally be exported to a USB-stick.

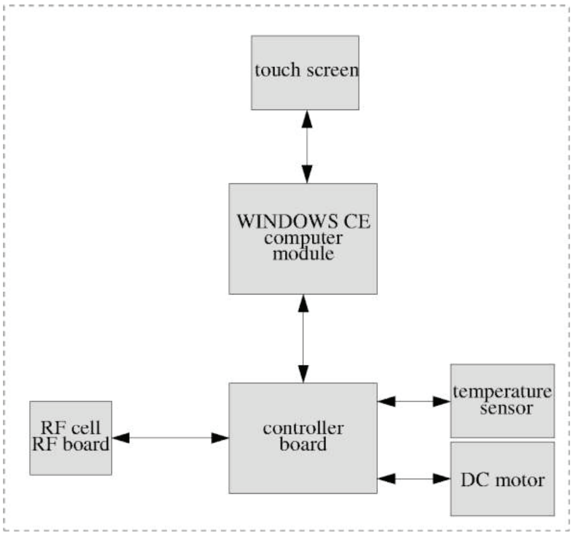

Fig. 2: The grain moisture analyzer uses a WINDOWS CE computer module with a touch screen. An RF cell and a temperature sensor perform measurements. The motor is used to move the next sample into the measuring cell and to later empty it.

Based on the technical features of the instrument, a list of attack vectors can be compiled. A few examples from the list will be given here. A more detailed description can be found in [4].

- **A_PASSWORD:** An attacker retrieves the admin password by trying all 6-digit combinations.
- **A_SW_REPLACE:** An attacker retrieves the admin password and replaces the legally relevant software.
- **A_INT_SERIAL:** An attacker exploits a vulnerability of the proprietary serial protocol and causes the instrument to malfunction.
- **A_INT_SERIAL_VALUE:** An attacker exploits a vulnerability of the proprietary serial protocol and manipulates a measurement value.
- **A_INT_USB:** An attacker manages to install malicious code by disabling the USB-port‘s protection.

The following Table 5 shows, for a short list of threats, possible technical realizations by means of the above-mentioned attack vectors. As an example, threat T2 with the following description is examined: “A user with the access rights of a local administrator invalidates availability or integrity of the evidence of an intervention.” Within the device a logbook is kept that records both errors and changes to legally relevant parameters. An attacker could, for instance, attack the serial port of the instrument to automatically generate an arbitrary number of error events. These will eventually flush the logbook until its memory capacity is exceeded and the evidence of other interventions, which is required by law, is no longer accessible.

Tab. 5: Evaluation of the identified threats (T) for example no. 1. Each attack vector (AV) is evaluated based on estimated time (ET), Expertise (Ex), Knowledge of the TOE (KT), the window of opportunity (WO), needed equipment (Eq). The resulting sum score is turned into a probability score (PS), which is then multiplied with the impact (I) to calculate the risk.

T	Description	I	AV	ET	Ex	KT	WO	Eq	Σ	PS	**Risk**
T1	Local admin invalidates integrity or authenticity of the metrological software.	5	A_SW_REPLACE	19	6	3	0	0	28	1	**1**
T2	Local admin invalidates availability or integrity of the evidence of an intervention.	5	A_INT_SERIAL	4	3	7	0	4	18	3	**3**
T3	Local admin invalidates the integrity of the metrological parameters.	5	A_INT_SERIAL_VALUE	7	6	7	0	4	24	2	**2**
T4	Local admin invalidates the availability of the evidence of an intervention by deleting the evidence.	5	A_PASSWORD	19	0	3	0	0	22	2	**2**
T5	Local admin invalidates integrity, authenticity or availability of a measurement result (A8).	2	A_INT_USB	7	6	3	0	4	20	2	**1**

It is assumed that finding such a vulnerability will take an attacker no longer than four weeks, resulting in a point score of 4. A detailed description of the individual point scores is given in [7, Section B.4]. The attacker will need to be proficient in the use of programming tools (score of 3) and have access sensitive information like the specification of the serial protocol (score of 7). As the attacker may also be the operator of the instrument, he will have unlimited access, which corresponds to a score of 0 for the window of opportunity. Finally, a laptop with a serial port and some standard software development tools are needed (score of 4 for equipment). The resulting some score Σ is 18. As the attack will affect all past and future measuring results, the impact is set to the highest possible value of 5. This value is turned into a probability score of 3 according to Table 2. Following the equation given at the bottom of Figure 1, impact and probability score are multiplied and divided by 5 to here produce a numeric risk value of 3. The respective results for the remaining threats are given in Table 5 as well. A medium risk of 3 is only calculated for threat T2. All other threats are either less probable or affect only one measurement at a time thus producing a smaller risk.

Example No. 2: Weigh bridge

The second exemplary measuring instrument is a weigh bridge for automatically measuring the net weight of transport vehicles filled with concrete. The measurement starts automatically when a vehicle stops on the measuring platform. The weight is determined by two independent load cells for both axles of the vehicle, see Figure 3. Sealed communication paths from both load cells to the respective evaluator units and finally to the terminal, which displays the results, ensure that the data cannot be corrupted along the way. Both evaluator units as well as the terminal are based on the same microprocessor. Data can be read from the terminal via RS 485 or can be written to a USB stick. At startup, the terminal checks the authenticity of all other units. Legally relevant parameters and software are stored in flash memory which is write-protected by a hardware switch. The legally relevant logbook is stored on a separate SD-card.

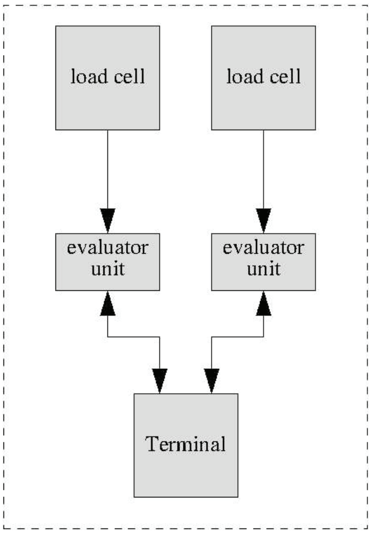

Fig. 3: The weigh bridge consists of two load cells which each communicate with an evaluator unit. These units and the terminal are based on the same microprocessor. The terminal's flash memory for parameters and software is protected by a hardware switch. The legally relevant logbook is stored on a separate SD-card.

For this instrument also, a reduced list of attack vectors will be given:

- **A_INT_SERIAL_SD:** An attacker exploits a vulnerability of the proprietary serial protocol and writes data to the SD card.
- **A_INT_SERIAL_VALUE:** An attacker exploits a vulnerability of the proprietary serial protocol and manipulates a measurement value.
- **A_INT_SERIAL_FLASH**: An attacker exploits a vulnerability of the proprietary serial protocol and overwrites parts of the flash memory.
- **A_INT_USB:** An attacker manages to install malicious code by disabling the USB-port‘s protection.
- **A_SW_REPLACE:** An attacker disables the USB port‘s protection as well as the hardware switch and replaces the legally relevant software.

Again, the technical realizations for certain threats together with their score are shown in Table 6.

Tab. 6: Evaluation of the identified threats (T) for example no. 2. Each attack vector (AV) is evaluated based on estimated time (ET), Expertise (Ex), Knowledge of the TOE (KT), the window of opportunity (WO), needed equipment (Eq). The resulting sum score is turned into a probability score (PS), which is then multiplied with the impact (I) to calculate the risk.

T	Description	I	AV	ET	Ex	KT	WO	Eq	Σ	PS	**Risk**
T1	An attacker manages to invalidate integrity or authenticity of the metrological software.	5	A_SW_REPLACE	19	6	7	0	0	32	1	**1**
T2	An attacker invalidates the integrity of the metrological parameters.	5	A_INT_SERIAL_FLASH	7	6	7	0	4	24	2	**2**
T3	An attacker manages to invalidate the availability or integrity of the evidence of an intervention.	5	A_INT_SERIAL_SD	7	6	11	0	4	28	1	**1**
T4	An attacker manages to invalidate the availability or integrity of the indication of the result.	2	A_INT_SERIAL_VALUE	7	6	7	0	4	24	2	**1**
T5	An attacker manages to invalidate the availability or integrity of all recorded measure-ment result.	5	A_INT_USB	7	6	3	0	4	20	2	**2**

Compared to the previous example, no risk of value 3 can be observed. Subsequently, it is assumed that the current protective measures are sufficient for the instrument.

Application of Solution No. 1: Additional motivation score

Based on the monetary gain an attacker could obtain from manipulating the two measuring instruments, the following categorization can be performed: The motivation to manipulate the grain moisture analyzer will be low, as the price of the grain is also determined by a number of other parameters such as the caloric value. Subsequently, low motivation is assumed, which corresponds to a motivation score of 6, see Table 3. Example no. 1 is now modified by replacing resource and expertise score with the value 6, whenever the originally estimated score was smaller, see left part of Table 7.

For the weigh bridge, on the other hand, the motivation will, however, be at least moderate as the quality of the delivered factory-produced concrete is always identical and the price thus solely depends on the measured weight. The results for both instruments with added motivation score are shown in Table 7.

Tab. 7: Modified evaluation results for examples 1 and 2 according to solution no. 1 “additional motivation score”.

	Grain Moisture Analyzer Ex. 1				**Weigh Bridge Ex. 2**			
T	original result		modified result		original result		modified result	
	Σ	Risk	Σ	Risk	Σ	Risk	Σ	Risk
1	28	1	34	1	32	1	35	1
2	18	3	23	2	24	2	24	2
3	24	2	26	1	28	1	28	1
4	22	2	34	1	24	1	24	1
5	20	1	22	1	20	2	20	2

As can be seen from the table, the effect of the additional motivation score is quite strong for the grain moisture analyzer (example no. 1), where the medium risk levels for threats T2 to T4 are all decreased, with a most obvious change for T4. For this threat, the protection originally relied mainly on time alone, with no needed expertise or special equipment. The modified score now shows, that the unmotivated attacker will almost certainly not attempt to tackle the time consuming task of password guessing. In the case of the weigh bridge (example no. 2), a small change of the sum score can only be observed for threat T1. Here, for most threats, it is not the motivation that limits the attack probability, but the pure technical difficulties associated with implementing an attack. Thus, the upper bound imposed by the original evaluation produced by the method from [4] is realized for almost all threats.

Application of Solution No. 2: Modifying the calculated probability score

As was the case for the previously described solution, the motivation for the attacker of the grain moisture analyzer is assumed to be low, the corresponding correction factor is 1.1, see Table 4. For the weigh bridge the correction factor will be 0.9, which again corresponds to moderate motivation. The modified scores may be found in Table 8.

Tab. 8: Modified evaluation results for examples 1 and 2 according to solution no. 2 “modifying the calculated probability score”.

Grain Moisture Analyzer Ex. 1					Weigh Bridge Ex. 2			
T	original result		modified result		original result		modified result	
	Σ	Risk	Σ	Risk	Σ	Risk	Σ	Risk
1	28	1	31	1	32	1	29	1
2	18	3	20	2	24	2	22	2
3	24	2	26	1	28	1	31	1
4	22	2	24	2	24	1	26	1
5	20	1	22	1	20	2	18	3

Compared to solution no. 1 (see Table 6), the modified risks now show a different behavior. For the grain moisture analyzer, threat T4 now also receives a risk level of 2. In the case of the weigh bridge, threat T5 (attack on all recorded measurement results via USB) now reaches a risk score of 3 and would thus require additional protective measures. Whether such a change is actually plausible will be discussed in the following section.

Comparison of the Two Solutions

As was shown during the individual application of the two prospective solutions, they both yield very similar results. In addition, solution no. 2 appears to be more intuitive, since the effect of the assumed motivation level is directly reflected in the sum score and subsequently in the risk score itself. However, there are a number of disadvantages to the simple multiplication with a correction factor: Just because an attacker has a higher degree of motivation, he will not be able to take technical hurdles more easily. On the contrary, certain aspects of an attack, such as time complexity and level of knowledge required, will be identical for all possible attackers regardless of their different motivation levels. This appears to be reflected quite well by solution no. 1. In addition, the method tested first, here yields more plausible results, and should, thus, be a well-suited way to represent attacker motivation during risk assessment. Nevertheless, the choice of this solution also requires additional changes to the assessment procedure to be followed. Usually, it is sufficient to evaluate the technically simplest way (attack vector) of realizing a threat. All other attack vectors with the same aim can be discarded. Now however, a greater number of attack vectors should be included in the assessment procedure. If these include different attacks, which require both high and low amounts of resources to realize the same threat, the limits set by the motivation score can then help to discover the most likely attack path and the associated highest risk.

Summary and Future Work

In this paper, the role of attacker motivation in software risk assessment for measuring instruments has been discussed. After having revisited the basic software risk assessment procedure, two different possible solutions were described and examined based on two real-world examples. With the aid of these, a best solution was selected with additional suggestions concerning its application in the field. Despite this choice, both solutions will be tested in practice within the ongoing research project “Harmonized Software Risk Assessment” of WELMEC’s working group 7 “Software”. In addition, methods will be investigated to yield an optimal, large set of attack vectors as input into the risk assessment method. Such an optimal set would then include attack vectors with a wide variation of needed resources, from which the motivation score will then with a certain likelihood select the most probable one.

References

[1] „Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonization of the laws of the Member States relating to the making available on the market of measuring instruments,” European Union, Council of the European Union ; European Parliament, Directive, March 2014.

[2] M. Sadiq, M. K. I. Rahmani, M. W. Ahmad, and S. Jung, “Software risk assessment and evaluation process (SRAEP) using model based approach,” in Proceedings of the IEEE International Conference on Networking and Information Technology, IEEE, June 2010, pp. 171–177

[3] A. van Deursen, T. Kuipers, “Source-based software risk assessment,” in Proceedings of the IEEE International Conference on Software Maintenance, IEEE, September 2003, pp. 385 - 388

[4] M. Esche, F. Thiel, „Software Risk Assessment for Measuring Instruments in Legal Metrology,“ in Proceedings of the Federated Conference on Computer Science and Information Systems, Vol. 4, Lodz, Poland, September 2015

[5] „ISO/IEC 27005:2011(e) Information technology - Security techniques - Information security risk management,” International Organization for Standardization, Geneva, CH, Standard, June 2011

[6] „ISO/IEC 15408:2008 Information technology – Security techniques – Evaluation criteria for IT security“ (Parts 1,2, and 3), International Organization for Standardization, Geneva, CH, Standard, August 2008

[7] „ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation,” International Organization for Standardization, Geneva, CH, Standard, August 2008

[8] “ETSI TS 102 165-1 Telecommunications and Internet converged Services and Protocols for Advanced Networking; Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis,” European Telecommunications Standards Institute, Sophia Antipolis Cedex, FR, Standard, March 2011, v4.2.3

[9] “WELMEC 7.2 Software Guide,” European cooperation in legal metrology, WELMEC Secretariat, Delft, Standard, March 2012