

Proposal for simplified implementation of risk assessment method for measuring instruments

Martin Koval
 Czech Metrology Institute, Brno,
 Czech Republic
 Email: mkoval@cmi.cz

Federico Grasso Toro, Marko Esche
 Physikalisch-Technische Bundesanstalt, Berlin, Germany
 Email: {federico.grassotoro, marko.esche}@ptb.de

Abstract - Legal Metrology is the economic sector where measuring instruments subject to legal control (taximeters, electricity meters, etc.) are used. In this field, constant growth of Measuring Instruments using ICT technology is evident. For this reason, higher security requirements need to be imposed as stated by the relevant EU directives. Risk assessment is an additional security assurance requirement for software, based on current regulations Directive 2014/31/EU and Directive 2014/32/EU (MID) that state: “The documentation shall make it possible to assess the instrument’s conformity to the relevant requirements and shall include an adequate analysis and assessment of the risk(s).” [1]. Several methods for risk assessment of software exist, but based on this statement above, it is necessary to find appropriate solutions for the realization of risk assessment for metrological software, on the base of its technical documentation. The WELMEC Working Group 7 has developed a Risk Assessment method, based on international standards. In this article a simpler method is proposed, aiming for advantages such as universality, simplicity and transparency, in contrast with already existing methods. The combination of these advantages in the proposed method will allow its simple understanding and implementation for all active stakeholders (both the Notified Bodies and the manufacturers).

rating. The WELMEC Working Group 7 has developed a Risk Assessment method, based on international standards [4] to define these ratings. There exists a wide range of measuring instruments to be regulated. Each measuring instrument has its own specific parameters, which depend on the purposes of its usage. For the present risk assessment method, a model of an abstract measuring instruments (MAMI) is proposed. Real-world examples were used for the development of the risk method (Chapter VI). The diagram shown in Fig.1 describes the proposed method. The first step is checking the completeness of the technical documentation of the measuring instrument. The second step is the assessment of important parameters of the metrological software functionality. The assessment of parameters is based on 25 combinations of parameters (assets, threats and impacts: specification of technical parameters). The last step is an evaluation which summarizes the points and results in a potential risk. According to the MID [1] the assessment of the risk is a part of the documentation, which is necessary for the process of validation of metrological software. Notified Bodies (NB) must check the correctness of the documentation, meaning that they must also check if the evaluations and the result of potential risk are correctly realized.

I. INTRODUCTION

THE term *risk* can be defined in many ways for different purposes. One of these definitions is “Combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event.” [2]. It should be emphasized that, in this case, the risk is the likelihood of occurrence combined with the impact of the event, and it can be transformed into the event that has potentially happened. This potential risk can also be a factor for system hazard or weak security provisions against dangerous/unauthorized influences.

II. THE PROPOSAL OF RISK ASSESSMENT METHOD

The proposal of this method is on the base of the selection of technical parameters, present in measuring instruments in the real world. These parameters have an influence on the legally relevant software (LRS) and are assigned a point

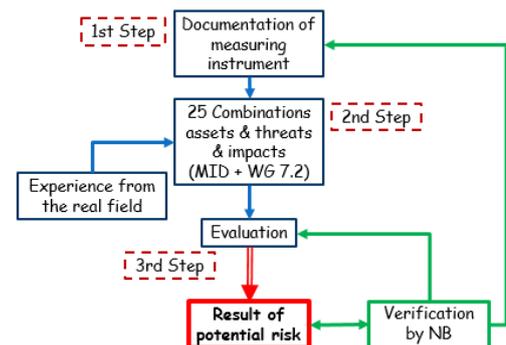


Figure 1. The basic structure of proposal of risk assessment method for metrological software.

III. TECHNICAL PARAMETERS OF MEASURING INSTRUMENT INFLUENCING METROLOGICAL SOFTWARE

The following technical parameters that have an influence on metrological software are inspired by WELMEC Guide 7.2 [3], the directive MID [1] and practical knowledge.

The resulting list of parameters is proposed based on developments and regulations, according to the current situation of ICT in the measurement area. The parameters are chosen on the base of combinations of three main factors:

- 1) Most used,
- 2) Most risky technologies, according to practical knowledge and
- 3) Parameters with different levels or the configuration possibilities.

Table I contains the proposed list of parameters, divided into 5 sections.

TABLE I: The basic division the parameters into 5 sections.

A	PC, Download LRS, Separation
B	User interface
C	Communication interface
D	Storage
E	Security

IV. ASSIGNING POINTS TO TECHNICAL PARAMETERS

Table I contains the list of parameters which has possibility for configuration. For risk assessment, it is necessary to assign points to all parameters. These points represent important characters for the analysis of the measuring instrument and its risk assessment:

- When the potential risk is zero: Absence of technical parameters which can increase the potential risk.
- When the potential risk is assigned with 1 point: The technical parameters are integrated part of the measuring instrument with metrological software.
- When the potential risk is assigned with 2 points: The technical parameters are a common part of the measuring instrument with metrological software.
- When the potential risk is assigned with 5 points: The technical parameters have weak security against the possibilities which are available. And, for this reason, the potential risk increases or the used technical parameters increase the overall potential risk.
- When the potential risk is assigned with 10 points: The technical parameters are sophisticated and their characteristics are considered as carriers of higher potential risk. These parameters can contain hidden functions or be considered as weakly secured elements.
- When the potential risk is assigned with 15 points: The technical parameters are sophisticated and their characteristics are considered as carriers of higher potential risk, including the parameters at the previous point. These parameters are considered riskier than with 10 points from the point of view of practical knowledge.

Once the potential risks are assigned, the risk assessment can be performed.

V. SPECIFICATION OF TECHNICAL PARAMETERS

Some of the technical parameters existing in the designed concept of the risk assessment method for metrological software have possibility for configuration. In Tables II-VI the configuration possibilities are represented and defined. These tables contain points rating for each specific technical parameter.

TABLE II. Specification of technical parameters: PC, Download LRS and Separation.

PC, Download LRS, Separation			Points
A	1	Using PC as like primary	10
	2	Download LRS	10
	3	Separation SW	15

Based on the possible configurations specific rating points can be assigned to specific technical parameters of the measuring instrument. For example, if the measuring instrument has a configuration based on a universal computer, then there is a higher likelihood for other functions that can have negative influences on the legally relevant software.

The download of the LRS without breaking the physical seal of measuring instrument means that there is a method for modification of the LRS, and it can also cause negative influences on the LRS even though conditions for security are fulfilled.

Separation of SW, dividing metrological software into legally relevant SW and legally non-relevant SW (LnRS) can have different realizations, e.g. both LRS and LnRS are in one source code or divided into two microprocessors. If the LnRS needs data from the LRS, then there must be a connection between the LRS and the LnRS. And since the LnRS is not under control, that means that potentially dangerous applications can exist, which can have negative influences on the LRS.

TABLE III. Specification of technical parameters: User interface.

User interface			Points
B	4	Button/s	2
	5	Keyboards (include numbers field)	10
	6	Without user interface	0

If measuring instruments have any button/s, there is potential risk that there can be a hidden combination for negative influences on the LRS. In the case that the measuring instrument has a keyboard, then the possibilities for hidden functions is even higher. If the measuring instrument has no user interface that has possibilities of entry to the metrological SW, then, in this case, the potential risk can be considered zero.

TABLE IV. Specification of technical parameters: Communication interface

Communication interface			Points
C	7	Physical	2
	8	Wireless	5
	9	Internet	15
	10	Without communication interface	0

Like in previous cases with the user interface, also, if the measuring instrument has no communication interfaces, then the potential risk can be considered zero. The communication interfaces can have different realizations. If the measuring instrument has a communication interface only by physical connections (USB, RS-232, etc.) there is a lower likelihood for the potential risk as there is for wireless connections. In case of wireless connection, there is higher likelihood for not allowed or hidden connections to the measuring instrument, where there is not enough security by means of physical seals. The cases where the measuring instrument has the possibility of connecting to the Internet, the potential risk is higher, since the measuring instrument may be exposed to cyber-attacks.

TABLE V Specification of technical parameters: Storage.

Storage			Points
D	11	Part of microprocessor	1
	12	Internal storage	2
	13	Removable storage	10
	14	Without storage (data on display only)	0

The memory for metrological software is often divided into storage for software and other storage for the measurement data – The Harvard architecture. There are cases when the storage is part of the microprocessor, which is physically sealed. But since the space for software must exist, it cannot be potential risk zero. Very often the micro-processor has a small memory, and for this reason the measuring instrument contains other internal storage. These storages offer the possibility for realizing separation of software (in LRS and LnRS). But the capacity of the internal storage can also be as big as to offer hidden space for non-allowed applications [5]. In cases where the storage is removable, the potential risk is higher, because there are many ways for negative exploitation.

The security aspect from the proposed solution is the most complicated to define, because each technical parameter has an additional configuration.

Event recording in metrological SW occurs in two forms:

1) Event Counter and 2) Event Logger. Event Counter records each change by binary value (1/0) or counting of changes. The Event Logger can record each change with date, time, and additional description of each change. In cases where there is no Event Record, the potential risk is the highest, because it is possible to realize any changes without

being recorded. The cases where passwords are used have potential risk, since every password can be broken. The passwords can be realized by number or combinations characters (alphanumeric). Most often a numerical combination is used, and the most used are 4 digits passwords. If a 4 digits password is used without a block protection, then there are only 10.000 possibilities, easy to break with IT technology. There are still measuring instruments without user or communication interfaces with LRS. In these cases, there is no need for passwords, since no access can happen to the LRS without breaking a physical seal. In the opposite example, if the measuring instrument has user and/or communication interfaces, there are many possibilities of changing or influencing the LRS, due to the lack of secure elements. Then, the conditions for security are not fulfilled. These cases are not acceptable.

TABLE VI. Specification of technical parameters: Security

Security: Event counter/logger			Points	
E	15	Event counter	2	
	16	Event logger	0	
	17	None	15	
	Security: Password			
	18	Numerical 4digits	10	
	19	Numerical more than 4 digits	5	
	20	Alphanumeric + block systems	2	
	21	None	0	
	Security: Seal cover			
	22	After break: device is not functional	0	
	23	After break: device is still functional	15	
	Security: Checksum			
	24	CRC 32 and weak	10	
	25	better then CRC-32	1	

The next part of the security aspect of the method are physical seals. The sealing of the measuring instrument is realized in different ways (it can be physical seal-lead/plastic, stamp). Physical seals that can be broken or removed are not applicable in legally metrology area. In the cases when the LRS of the measuring instrument and the physical seal are interconnected, where after the seal has been broken, the measuring instrument is not functional, the potential risk is considered zero. Given that there are cases where after seal breaking, the measuring instrument still works, there is a probability that the seal of measuring instrument is not enough for the security of LRS.

The final category for security are checksums. Currently, there are a lot of variations of checksums on the market.

The manufacturers mostly use the type CRC-16, for economic reasons. This type of CRC belongs to the weakest. Current WELMEC Guide 7.2 pushes for an acceptable solution CRC-32 [3]. This is the reason for this type of checksums in Table VI.

VI. EXAMPLES OF EVALUATION

On the base of the present technical parameters it is possible to propose different MAMI (Model Abstract Measuring Instrument).

The configurations MAMI A-D are considered as border cases, where it may occur:

- MAMI A: Proposed lowest potential risk.
- MAMI B: Proposed highest potential risk.
- MAMI C: Proposed basic technical parameters.
- MAMI D: Proposed advanced technical parameters.

TABLE VII. Evaluation of Risk assessment for metrological SW of MAMI (A-D).

Sect.	Num.	Technical parameters	Pts.	A	B	C	D	
PC, Download LRS, Separation								
A	1	Using universal computer	10	0	1	0	1	
	2	Download LRS	10	0	1	0	1	
	3	Separation SW	15	0	1	0	1	
User Interface								
B	4	Button/s	2	0	1	1	1	
	5	Keyboards (include NF)	10	0	1	0	1	
	6	Without user interface	0	1	0	0	0	
Communication interface								
C	7	Physical	2	0	1	1	1	
	8	Wireless	5	0	1	0	1	
	9	Internet	15	0	1	0	1	
	10	Without Comm. Inter.	0	1	0	0	0	
Storage								
D	11	Part of microprocessor	1	0	1	1	1	
	12	Internal storage	2	0	1	0	1	
	13	Removable storage	10	0	1	0	1	
	14	Without storage	0	1	0	0	0	
Security								
E	15	Event counter	2	0	0	0	0	
	16	Event logger	0	1	0	1	1	
	17	Without Event C/L	15	0	1	0	0	
	Passwords							
	18	Numerical 4 digits	10	0	1	1	0	
	19	Numerical more than 4 digits	5	0	0	0	0	
	20	Alphanumerical	2	0	0	0	1	
	21	Without password/s	0	1	0	0	0	
	Seal Cover							
	22	After breaking: is not functional	0	1	0	0	0	
	23	After breaking: is still functional	15	0	1	1	1	
	Checksum							
	24	CRC-32 and weak	10	0	1	1	0	
	25	Better than CRC-32	1	1	0	0	1	
	Summary of points				2	132	42	90

Table VII shows some examples of the evaluation of potential risks for metrological software for different MAMI (from A to D). Each technical parameter has been assigned rating points, where the columns for MAMI contains 1 or 0, depending on the technical parameters option. The last row of Table VII is the sum of points, where it is possible to realize further evaluations or adjustments to get the result of the potential risk by statistic or other methods. One of the possible solutions can be considered the MAMI B, for the maximum potential risk, assigning 132 points to the 100% of potential risk. Then, it is possible to create comparative graphs for the conclusions, see Figure 2.

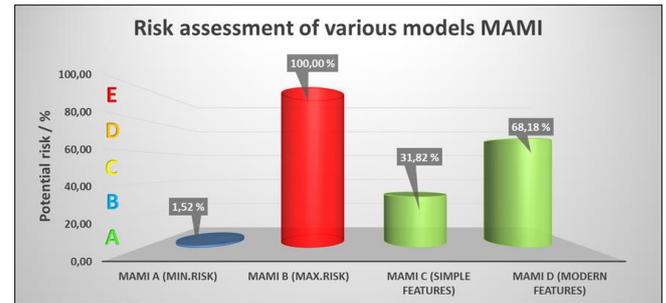


Fig. 2. Examples of Risk assessment for MAMIs (A-D).

The WELMEC Working Group uses a Risk Assessment method [4] that combines elements from the international ISO/IEC standards 27005 and 15408, to support the theoretical comparability of the risk assessment results. On the other hand, the present method focuses on existing measuring instruments, mostly type P according to WELMEC Software Guide 7.2[3].

The present method defines within the MAMIs four proposed model levels, allowing a quick approximation of the risk assessment for the modeled measuring instrument, supporting quick repeatability of analysis between very similar and well-known measuring instruments.

The method focused on existing measuring instruments with many previously detailed and collected reports regarding risk assessment, while the WELMEC Working Group 7 focuses on any kind of measuring instrument, even with previously unknown designs and the new developments.

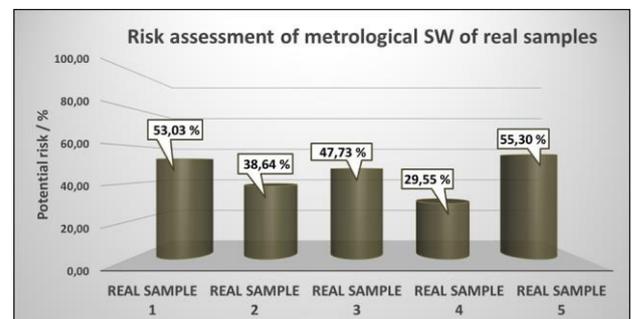


Fig. 3. Risk assessment for metrological SW of real samples.

VII. CONCLUSION

The present method for risk assessment for metrological software is not only focused on potential risk results in graphs, but it also analyses the resulting table with rating points. Table VII indicates which MAMI shows weak software protection (B and D). The proposal of the method is based on the potential risk that cannot be zero, but after the determination of technical parameters with assign rating point is possible the set within a maximum of potential risk of the metrological software. The cases MAMI A-D are specific cases, but after applying the method on real world examples (Fig.3), the potential risk results in the interval between 20% and 60%. This test on 5 real world samples is only for orientation purposes. For better results, it is necessary to apply this method on more real-world examples to check the quality of these results and the potential application of this simple method in the future.

ACKNOWLEDGEMENTS

This project is funded by Institutional Subsidy for Long-Term Conceptual Development of a Research Organization

granted to the Czech Metrology Institute by the Ministry of Industry and Trade.

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, February 2014.
- [2] ISO/IEC 27005:2011(e) Information technology - Security techniques - Information security risk management, International Organization for Standardization // Geneva, CH, Standard, June 2011.
- [3] WELMEC 7.2 Software Guide, / European cooperation in legal metrology, // WELMEC Secretariat, Delft, Standard, March 2012.
- [4] M. Esche and F. Thiel, "Software risk assessment for measuring instruments in legal metrology," 2015 Federated Conference on Computer Science and Information Systems (FedCSIS), Lodz, 2015, pp. 1113-1123. DOI: 10.15439/2015F127.
- [5] Ch.-B. do Prado, D.-R. Boccardo, R.-C.-S Machado, L.-F.-R. da Costa Carmo, T. -M. do Nascimento, L.-M.-S. Bento, R.-O. Costa, C.-G de Castro, S.-M. Camara, L. Pirmez and R. Oliveira / Software Analysis and Protection for Smart Metering in // NCSLI Measure: The Journal of Measurement Science. - 2014.-vol.9.-No.3 – p. 22-29. DOI: 10.1080/19315775.2014.11721691.