

Leaflet: Software Risk Assessment – Guidelines for Manufacturers

Introduction

The aim of this leaflet is to provide recommendations for manufacturers of measuring instruments who submit their instruments to the conformity assessment body of PTB for Module B examination, according to the European Measuring Instruments Directive (MID) [1] or to the Measurement and Calibration, *Mess- und Eichgesetz* (MessEG) [2]. In both legal frameworks, the manufacturer is required to provide a suitable risk assessment of the instrument, regarding essential requirements, in addition to the documentation of the measuring instrument and the software (Annex I of the MID, or Annex 2 to the Measurement and Calibration Ordinance (MessEV) [3]). A more detailed description of the method can be found in [4].

A risk assessment is explicitly required in the MID modules A, A2, B, D1, E1, F1, G, H, and H1. This regulation has been transposed into the national legislation in § 10 MessEV, in conjunction with §§ 7 and 8 MessEV.

Although the risk assessment described here is primarily focused on software of measuring instruments, the procedure is not exclusively restricted to that specific area of application.

In the following, assets to be protected are first derived from the corresponding requirements in MID and MessEV. Afterwards, a procedure is proposed for the manufacturers to follow, when conducting risk assessments.

The norm ISO/IEC 27005 [5] defines the term risk as a combination of the consequences (impact), which follows from an unwanted event (threat), and the probability of occurrence of the threat. Thus, the risk associated with a threat can be modeled by the following equation:

$$\text{risk} = \text{impact} \times \text{probability of occurrence}$$

In the context of legal metrology, the term impact refers to a breach of the essential requirements. These essential requirements can be seen as the characteristics of the protection objectives of the MID (see [1], taking in consideration [6]).

Concerning the **severity of damage** (impact), only two categories are defined here:

- a. The impact resulting from a threat is considered to be low (factor $\frac{1}{3}$) when a threat only affects an essential requirement once and only for a short period of time.
- b. In all other cases an impact of 1 is assumed.

Derivation of assets to be protected

Every measuring instrument that is examined during a conformity assessment based on the MID or the MessEG must fulfill the essential software requirements listed in column 1 of the following table. These requirements are here to be interpreted in the form of **assets** (column 2) with their associated generic **security properties** (column 3). This derivation of assets to be protected is applicable to all manufacturers and all types of measuring instruments. It can be reused directly by the manufacturer.

Table 1: Correspondence between the software-related essential requirements, their derived assets to be protected, and their associated security properties

Software-related essential requirement in Annex I of the MID or Annex 2 of the MessEV	Assets (Object ID)	Security property
7.6 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.	identification of the legally relevant software (O9)	availability, integrity
	inadmissible influence on the legally relevant software (O5) through other software	non-availability ¹
8.1 The metrological characteristics of a measuring instrument shall not be influenced in any inadmissible way by the connection to it of another device, by any feature of the connected device itself or by any remote device that communicates with the measuring instrument.	inadmissible influence on the legally relevant software (O5) via communication interfaces	non-availability
8.3 Software that is critical for metrological characteristics shall be identified as such and shall be secured. Software identification shall be easily provided by the measuring instrument. Evidence of an intervention shall be available for a reasonable period of time.	presentation of the software identification (O10)	Availability
	evidence of an intervention (O2)	availability, integrity
8.2 A unit, decisive for the measuring technology features, must be designed, in such a way that it can be secured. The provided protective measures must allow proof of possible interventions. 8.4 Measurement data, software that is critical for measurement characteristics and metrologically important parameters stored or transmitted shall be adequately protected against accidental or intentional corruption.	measurement data (O3)	integrity, authenticity
	legally relevant software that is critical for metrological characteristics (O1)	integrity, authenticity
	metrologically important parameters (O4)	integrity, authenticity
10.1 Indication of the result shall be by means of a display or hard copy.	indication of the result (O6)	availability, integrity
10.2 The indication of any result shall be clear and unambiguous and accompanied by such marks and inscriptions necessary to inform the user of the significance of the result. Easy reading of the presented result shall be permitted under normal conditions of use. Additional indications may be shown, provided they cannot be confused with the metrologically controlled indications.	clear and unambiguous indication of the result, marks and inscriptions (O7) accompanying a measurement result	availability, integrity

¹ The term “non-availability” should be interpreted as follows: “There shall be no inadmissible influence on the legally relevant software.”

<p>11.1 A measuring instrument other than a utility measuring instrument shall record by a durable means the measurement result accompanied by information to identify the particular transaction, when: (a) the measurement is non-repeatable; and (b) the measuring instrument is normally intended for use in the absence of one of the trading parties.</p> <p>11.2 Additionally, a durable proof of the measurement result and the information to identify the transaction shall be available on request at the time the measurement is concluded.</p>	<p>record of a measurement result and necessary additional information (O8)</p>	<p>availability</p>
---	---	---------------------

Identification of threats and of possible attack scenarios

The invalidation of any one of the assets to be protected can be considered a relevant threat in the context of this leaflet. Based on the instrument and the submitted documents for conformity assessment, the manufacturer shall explain which threats (invalidation of the security properties of one or more assets) can be realized by specific technical steps. The manufacturer is kindly asked to describe, for each security property of an asset, which steps would be theoretically necessary to invalidate the respective security property. Where applicable, it shall be demonstrated that the invalidation of a security property is intrinsically impossible. Lists of current attack scenarios for measuring instruments that are, for example, connected to the Internet may, for instance, be found at <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment> or at <https://cve.mitre.org/>.

Calculation of the probability of occurrence

For each identified attack scenario, the manufacturer should evaluate which prerequisites a possible attacker should have to successfully implement an attack. It is recommended to base the evaluation on the following five criteria:

1. Elapsed Time (0-19 points)
2. Expertise (0-8 points)
3. Knowledge of the measuring system (0-11 points)
4. Window of opportunity (0-10 points)
5. Equipment (0-9 points)

For each criterion a point score shall be assigned, based on the tables given in the appendix. Depending on the sum of all points, each attack scenario is then given a probability score, as described in the following table. Details concerning the assessment scheme may also be found in the standard ISO/IEC 18045 "Information technology – Security techniques - Methodology for IT security evaluation" [7], part 2, B.4.2.2 ff.

Table 2: Mapping of point scores according to [7]

Sum of point scores	Resistance to attacks	Probability score
0-9	No rating	5
10-13	Basic	4
14-19	Enhanced basic	3
20-24	Moderate	2
>24	High	1

Calculation of the impact

If a threat affects an unlimited number of future or past measurements, then the impact shall be set to 1. If only individual measurements are affected by the thread, then an impact of $\frac{1}{3}$ is assumed.

Calculation of the risk

Finally, the determined probability of occurrence is transformed into a risk, while taking into account the estimated impact. To this end, impact and probability of occurrence are multiplied. Afterwards, if necessary, the result is rounded up to the next integer number. A detailed description of the entire procedure, with additional examples, may be found in [4].

Consequences

As a general rule, all threats with a risk of 4 or 5 must be mitigated by technical or organisational measures until, after a new assessment, a risk in the range between 1 and 3 is reached.

Example

In the following example, a measuring instrument based on a universal computer is examined, which contains a legally relevant storage unit for recorded measurement data. The storage shall be implemented as a text file that can only be read and written by the legally relevant application. The access control to the text file shall be implemented by operating system means, and the operating system itself shall be protected by a secret administrator password (here: 4 digits). Therefore, one possible attack on the availability of the stored measurement results (O8) consists of a user trying random password combinations until he or she has gained access to the system. With the acquired access rights, the user can then delete the text file. The assumed measuring instrument shall be available to the user without restrictions. In this described example, the asset to be protected is the storage of measurement results (O8), and the associated security property is availability.

Threat

The user with normal access privileges invalidates the availability of the record of the measurement results (O8).

Attack scenario

The user guesses correctly the administrator password by trying arbitrary four-digit combinations. Afterwards, the user deletes the text file.

Evaluation

- **Elapsed time:** There are $10^4 = 10,000$ different possible four-digit passwords. Assuming that entering and validating a password lasts a maximum of 10 seconds, all 10,000 combinations can be tested in 100,000 seconds = 27.78 hours = 1.15 days. Even if an attacker only tries combinations for 4 hours per day, he or she won't need longer than $1.15 \times 24 / 4 = 6.9$ days. On average, the correct combination will be found after trying half of the possible passwords, e.g. after 3.5 days. In any case, the search for the correct password will not take longer than a week. The point score to be selected is, therefore, 1.
- **Expertise:** No special knowledge is required to guess a digit combination and delete a text file. Accordingly, even a layman could be considered a likely attacker, and 0 points for expertise are given.
- **Knowledge of the measuring system:** In a first step, the attacker needs to identify where the records of the measurement results are stored on the system and that they can be deleted or modified only after entering the administrator password. In the case of most operating systems, however, simply finding the file will suffice, since the user will be asked for the administrator password when trying to open the file. Consequentially only restricted knowledge of the system is required. The point score to be assigned is therefore 3.
- **Window of opportunity:** because the user is a possible attacker with unlimited access to the instrument, without the risk of being detected, the respective point score should thus be 0.
- **Equipment:** No equipment is needed for the attack (0 points).

Table 3: Evaluation of the example

Threat	Attack scenario	Elapsed time	Expertise	Knowledge of the measuring system	Window of opportunity	Equipment	Sum	Probability score	Impact	Risk
The user with normal access privileges invalidates the availability of the record of the measurement results (O8).	The user guesses correctly the administrator password by trying arbitrary four-digit combinations. Afterwards, the user deletes the text file.	1	0	3	0	0	4	5	1	5

Since the described threat could affect all past measurements, the impact should be set to 1. Consequentially, the risk is identical to the calculated probability score, after multiplying impact and probability score.

Consequences

As a general rule, all threats with a risk of 4 or 5 must be mitigated by technical or organisational measures until, after a new assessment, a risk in the range between 1 and 3 is reached. In the presented example, an adjustment of the password length to 6 digits (100 times more combinations than for 4 digits) would result in point score of 19 for elapsed time (3.5 days * 100 = 350 days). This would virtually eliminate the threat of an attacker guessing the correct password.

References

- [1] „Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation 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] „Gesetz über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen (Mess- und Eichgesetz – MessEG)“, Bundesgesetzblatt, Volume 2013 Part 1 No. 43, July 2013.
- [3] „Verordnung über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt sowie über ihre Verwendung und Eichung (Mess- und Eichverordnung - MessEV)“, Bundesgesetzblatt, Volume 2014 Part 1, No. 58, December 2014.
- [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, Volume 4, Lodz Poland, September 2015, DOI: <http://dx.doi.org/10.15439/978-83-60810-66-8>, ISSN 2300-5963, (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] „The 'Blue Guide' on the implementation of EU product rules“, Council of the European Union, July 2015 Version 1.1.
- [7] “ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation”, International Organization for Standardization, Geneva, CH, Standard, August 2008.

Appendix

Elapsed Time	Points
less than 1 day	0
less than 1 week	1
less than 2 weeks	2
less than 1 month	4
less than 2 months	7
less than 3 months	10
less than 4 months	13
less than 5 months	15
less than 6 months	17
more than 6 months	19

Expertise	Points
Layman	0
Proficient	3
Expert	6
Multiple expert	8

Knowledge of the system	Points
Public	0
Restricted	3
Sensitive	7
Critical	11

Window of opportunity	Points
Unnecessary/unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**

**If access to the measuring system is impossible due to time constraints, the associated attack scenario does not need to be evaluated.

Equipment	Points
Standard	0
Specialized	4
Bespoke	7
Multiple bespoke	9