European Cooperation in
Legal Metrology (WELMEC) e. V.
Bundesallee 100
38116 Braunschweig
Germany

WELMEC Guide 7.6

Software Risk Assessment

for Measuring Instruments

Version 2021

For information:
This Guide is available for the Working Group Measurement Instruments
For future reference on the Europa Website.

WELMEC is a co-operation between the legal metrology authorities of the Member States of the European Union and EFTA. This document is one of a number of guides published by WELMEC to provide guidance to manufacturers of measuring instruments and to Notified Bodies responsible for conformity assessment of their products. The guides are purely advisory and do not themselves impose any restrictions or additional technical requirements beyond those contained in relevant EC Directives. Alternative approaches may be acceptable, but the guidance provided in this document represents the considered view of WELMEC as to the best practice to be followed.

Published by:
WELMEC Secretariat

e-mail: secretary@welmec.org

Website: www.welmec.org

Software Risk Assessment for Measuring Instruments

Contents

Foreword 4
Introduction 5
1 Terminology 6
2 Workflow of Software Risk Assessment 7
3 Risk Identification 8
3.1 Main assets 8
3.2 Threat definition 10
3.3 Generic threats with high-level attack vectors derived from the MID 10
3.3.1 High-level attack vectors independent of the main assets 10
3.3.2 Child attack vectors derived from 3.3.1 11
3.3.3 Summary of generic threats with high-level attack vectors for instruments 12
3.3.4 Instrument-specific attack vectors for instruments 12
3.4 Attack probability tree-based threats 13
3.4.1 Attack probability trees based on generic threats with high-level attack vectors 13
3.4.2 Attack probability trees based on instrument-specific attack vectors 18
4 Risk Analysis: Analysis of Attack Vectors 19
4.1 Risk analysis on top level attack vectors 19
4.2 Risk analysis on instrument-specific attack vectors 19
4.2.1 Identification of additional attack vectors 19
4.2.2 Probability estimation 20
5 Risk Evaluation 21
5.1 Risk evaluation in the context of a measuring devices purpose and the respective motivation of an attacker 21
5.1.1 Attacker's Benefit (AB) 21
5.1.2 Attacker's Risk of being suspected (ARS) 21
5.1.3 Attacker's Risk, when getting caught (ARC) 22
5.1.4 Taking into account the attacker's motivation 22
6 Risk Assessment Report 22
7 References 22
Annex A Checklist 24
Annex B Tables and Examples 25
Annex C Report Format 29
Annex D Assessment of Attack Probability Trees 30

Foreword

This guide is intended for the software and IT risk assessment of measuring instruments under the Measuring Instruments Directive (MID) [1] and the Non-Automatic Weighing Instruments Directive (NAWID) [2].

This guide is purely advisory and does not itself impose any restrictions or additional technical requirements beyond those contained in the MID [1] or the NAWID [2].

Alternative approaches may be acceptable, but the guidance provided in this document represents the considered view of WELMEC as to a good practice to be followed.

Other WELMEC Working Groups may impose additional formal or technical requirements for the risk assessment.

Although this guide is oriented on instruments included in the regulations of the MID [1] and the NAWID [2], the method is of a general nature and may be applied beyond.

Introduction

Within the frame of conformity assessment for measuring instruments according to the MID [1] or NAWID [2], a risk assessment shall be performed and documented by the manufacturer to demonstrate conformity of the instrument with the essential requirements, see MID [1] Annex II, Module B 3c and NAWID [2] Annex II, Module B 1.3c.

It is the responsibility of the notified body to analyse the submitted risk assessment to determine if all essential requirements have been adequately covered.

This document describes a method for assessing the software-related risks of a measuring instrument subject to the MID [1] and NAWID [2]. This guide does not deal with other risks such as EMC, health issues, risk of electrical shock etc. Wherever MID [1] or WELMEC 7.2 [3] is referred, this applies also to NAWID [2] and WELMEC 7.5 [4] which have equal or similar requirements. In both cases, this guide provides a method to assess instrument-specific risks, especially for new technologies not addressed by established acceptable solutions.

The method is targeted at manufacturers of such instruments to help them provide an adequate risk assessment report and notified bodies, specifically the notified bodies under module B, G and H1 of the MID [1] and the NAWID [2], to aid them in the task of analysing the submitted report, i.e. does the report cover all threats against the assets to be protected and are the proposed measures to mitigate the threat acceptable.

It is strongly recommended that the risk assessment is performed by a group of people with different responsibilities (for example marketing, support, design, testing etc.)

According to ISO/IEC 27005 [5], “A 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.”

Therefore, three items are needed to estimate software-related risks for measuring instruments:

1. a list of unwanted events – also referred to as threats, in case of legal metrology a threat to assets derived from the corresponding requirements in the MID [1],
2. a measure for the consequences – also referred to as impact – resulting from a realized threat and
3. an estimate for the likelihood of occurrence.

Section 1 introduces the terminology used in this guide.
Section 2 describes the general workflow of the software risk assessment method.
Section 3 derives applicable assets from the MID [1] and introduces threat definitions.
Section 4 describes the risk analysis from section 3, by means of elementary attack vectors.
Section 0 places the estimated risk scores in the context of the measuring instrument type and its field of application.
Section 0 provides a suggested risk assessment report format.

1 Terminology

Some terminology is taken from ISO/IEC 27005:2011 [5], ISO Guide 73:2009 [6] and ISO/IEC Guide 73:2002 [7].

Attack vector: technical steps taken by an attacker to realize a threat

Attack Probability Tree (AtPT): a graphical representation of a threat and its associated attack vectors highlighting how an attack may be subdivided into intermediate sub-goals/attacks

NOTE 1: The level of detail of an AtPT is chosen by the assessor.

NOTE 2: Leaf nodes of the tree, which are not divided further, are referred to as elementary attacks.

Assessor: In this guide, assessor refers to the person/-s chosen from the manufacturer of a measuring instrument, performing the risk assessment.

Asset: Anything that has value to the organization, and which therefore requires protection [ISO/IEC 27005:2011].

NOTE: Assets are assigned one or more of the following security properties: availability, integrity, authenticity.

NOTE: Assets can be properties of measuring instruments which must be protected.

NAWID: Non-Automatic Weighing Instrument Directive, 2014/31/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 26 February 2014 (recast).

MID: Measuring Instrument Directive, 2014/32/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 (recast).

Risk Analysis: Process to comprehend the nature of risk and to determine the level of risk.

NOTE 1: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

NOTE 2: Risk analysis includes risk estimation [ISO/IEC 27005].

Risk Assessment: Overall process of risk identification, risk analysis and risk evaluation [ISO Guide 73:2009].

Risk Estimation: Process to assign values to the probability and consequences of a risk [ISO/IEC Guide 73:2002].

Risk Evaluation: Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable [ISO Guide 73:2009].

Risk Identification: Process of finding, recognizing and describing risks [ISO Guide 73:2009].

Threat: An unwanted event that may lead to the invalidation of one or more security properties of an asset.

2 Workflow of Software Risk Assessment

The method described here follows the framework and definitions provided by ISO/IEC 27005 [5], which divides the process of risk assessment into three distinct stages:

1. Risk Identification (see Section 3): This process results in a list of unwanted events (threats to assets) derived from the legal requirements of the MID [1].
2. Risk Analysis (see Section 4): During this stage, the identified threats are assigned a quantitative or qualitative risk measure by evaluation of so-called attack vectors. Depending on the assigned risk class for the instrument type (see WELMEC Guide 7.2 [3]), only simple generic attacks (most instruments of risk class C and lower) or more complex attacks (mainly risk class D and higher) should be investigated. For complex attacks, Attack Probability Trees (AtPT) can be used to help with the evaluation.
3. Risk Evaluation (see Section 5): Here, the risk is calculated in the context of the examined measuring instrument and its anticipated field of application, to determine if the residual risk (after risk mitigation) is acceptable.

Figure 2-1 illustrates the anticipated workflow of the procedure.

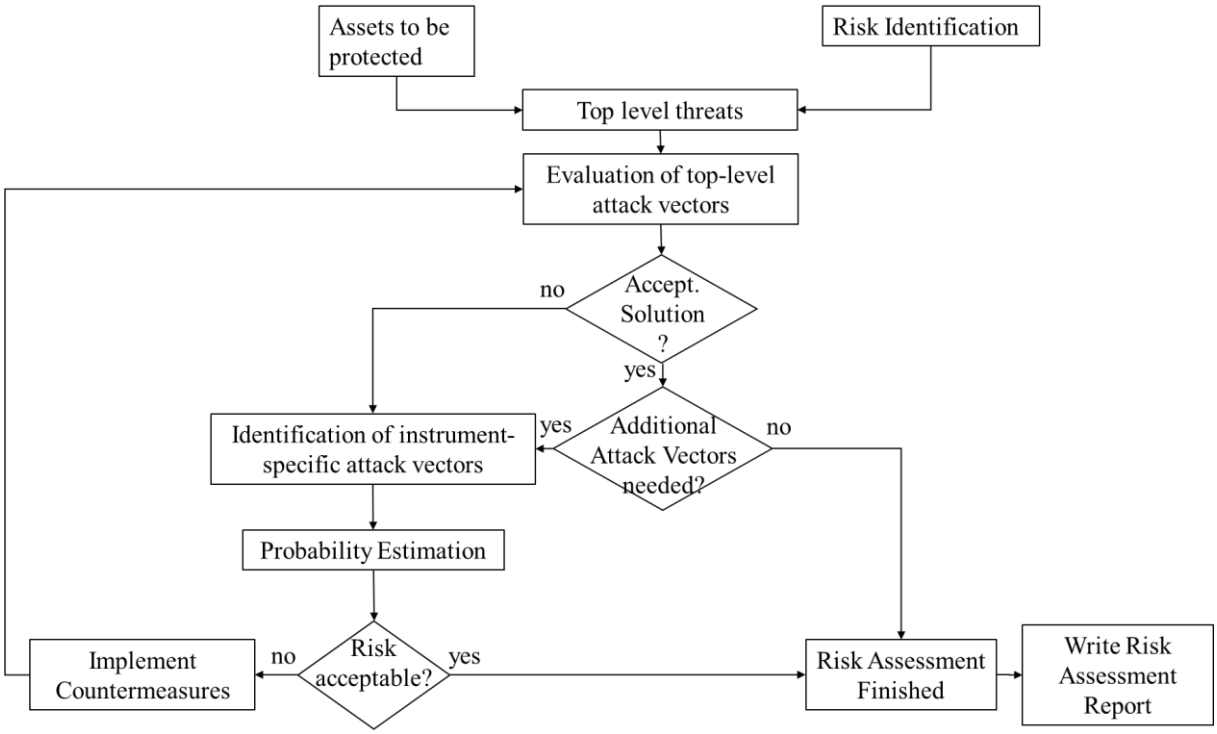

Figure 2-1: Workflow of the risk assessment procedure.

The risk assessment could be performed in two phases.

1. In the first phase, risk assessment takes place with the defined top-level threats given in 3.3.1.
2. Depending on the complexity of the measuring instrument or its risk class, instrument-specific attack vectors have to be defined, see 3.3.4, and further assessments based on these instrument-specific attack-vectors need to be performed. Note that examination of additional attack vectors might be required regardless of the risk class of the instrument.

3 Risk Identification

Within the scope of this document, all risks are related to a possible non-conformity with the essential requirements of the MID [1].

Note: The MID [1] requirements have to be fulfilled even if the risk that an occurrence takes place is very low (e.g. MID [1] requires an adequate protection against software changes. Hence, no protection does not fulfil the essential requirements.)

Note: Only evidence of an intervention is not an adequate protection against software changes. The software should be protected against unintentional and intentional changes (MID Annex I clause 8.4) and there should be an evidence of an intervention (MID Annex I clause 8.3) See guidance in WELMEC Guide 7.2 [3] P5, P6 and U5 and U6 (also P5, P6 and U5 and U6 in WELMEC 7.5 [4]).

3.1 Main assets

*The requirements of Annex I in MID [1] are similar to the ones in Annex I of NAWID [2], see especially requirements 8-10, 14

Nr.	Asset	Security properties	Requirement (Annex I, MID [1])*
1	legally relevant software	• availability • integrity • authenticity	• 7.1 • 7.2 • 7.6 • 8.3 • 8.4
	identification of the legally relevant software	• availability • integrity • authenticity	• 7.6 • 8.3
	evidence of an intervention of the legally relevant software	• availability • integrity • authenticity	• 8.2 • 8.3
	Adequate protection of the legally relevant software	• availability	• 8.1
2	legally relevant parameters	• availability • integrity • authenticity	• 7.1 • 8.4
	Adequate protection of the legally relevant parameters	• availability • integrity • authenticity	• 8.2 • 8.3
	Evidence of an intervention[1] of the legally relevant parameters	• availability • integrity • authenticity	• 8.1

[1] Although evidence of an intervention is not required in the case of parameter protection or protection of stored measurement results, it is a typical form of protection so this needs to be considered when evaluating the integrity of the parameters and stored measurement results.

Nr.	Asset	Security properties	Requirement (Annex I, MID [1])*
3	measurement result, including the measurement result relevant data	• availability • integrity	• 7.1 • 8.4
	Adequate protection	• availability • integrity • authenticity	• 8.1
4	record of a measurement result	• availability • integrity	• 11.1 • 11.2
	Adequate protection	• availability • integrity • authenticity	• 8.2 • 8.3
	Evidence of an intervention[1]	• availability • Integrity • authenticity	• 8.1
5	indicating the measurement result: • markings • Indication of the measurement result: clear and unambiguous	• availability • integrity • authenticity	• 7.1 • 9 • 10.2 • 7.1 • 10.1 • 10.2 • 10.4
	Adequate protection	• availability • integrity • authenticity	• 8.1

3.2 Threat definition

Threats consist of at least one asset to be protected and one correspondent statement of which security property (availability, integrity and/or authenticity) can be invalidated by the threat. Theoretically, at least one threat for each of the assets would need to be formulated.

3.3 Generic threats with high-level attack vectors derived from the MID

The main assets derived from the MID [1], see 3.1, such as software, parameters, measurement result, indication and stored result can be mapped to a generic set of threats with high-level attack vectors independent of the main assets, such as influence through other software or through the user interface or communication interface, or influence by replacing hardware or software by focusing only on the manner of the attack and not distinguishing between attacks on software, parameters etc.

Each of these high-level attack vectors can be subdivided into alternative child attack vectors:

- For influence through the communication interface, direct influence or influence during transmission should be taken into consideration.
- For inadmissible influence with regard to replacing hardware, inadmissible influence through replacing (complete) parts, components or by connecting a device to the measuring instrument should be taken into consideration.

The purpose of this division is to help define the root node of an attack tree, which represents an attacker's target and/or goal, while child nodes are refinements of such an attack. The leaves of the tree then represent elementary attacks that can no longer be refined. A simple example is given in **Figure 3-1**.

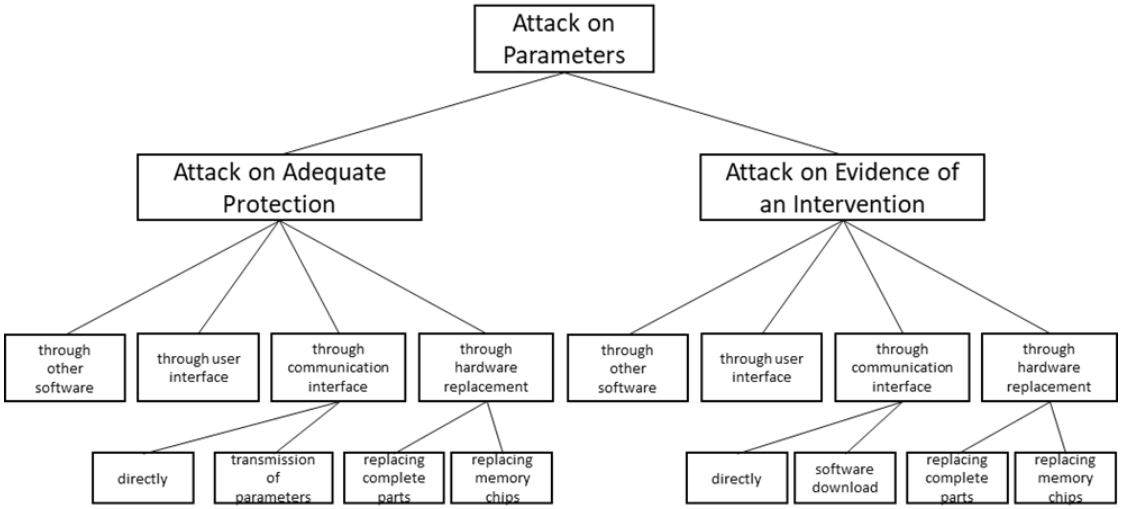

Figure 3-1: Simple illustration of attacks on "parameters", as an asset to be protected.

A detailed explanation can be found in [8].

In section 3.4, an implementation through AtPTs is described.

3.3.1 High-level attack vectors independent of the main assets

Nr.	High-level attack vector	Requirement (Annex I, MID [1])
1	inadmissible influence on the main assets* **through other software**	• 7.1 • 7.2 • 7.6 • 8.3 • 8.4
2	inadmissible influence on the main assets **through the user interface**	• 7.1 • 7.2 • 8.3 • 8.4
3	inadmissible influence on the main assets **through the communication interface**	• 7.1 • 7.2 • 8.1 • 8.3 • 8.4
4	inadmissible influence on the main assets **through replacing hardware of the measurement instrument**	• 7.1 • 8.2
5	inadmissible influence on the main assets **through replacing software**	• 8.3 • 8.4

3.3.2 Child attack vectors derived from 3.3.1

With regard to no influence through the communication interface:

Nr.	Child attack vector	Requirement (Annex I, MID [1])
1	inadmissible influence directly through the communication interface by connecting a device to the measurement instrument	• 8.1 • 8.3 • 8.4
2	inadmissible influence during transmission, including software download	• 8.1 • 8.3 • 8.4

With regard to no influence through replacement of hardware:

Nr.	Child attack vector	Requirement (Annex I, MID [1])
1	inadmissible influence through replacement of complete parts	• 7.1 • 8.2
2	inadmissible influence through replacing components	• 7.1 • 8.2

3.3.3 Summary of generic threats with high-level attack vectors for instruments

Based on the MID [1] or NAWID [2] and WELMEC Guide 7.2 [3], the following top-level threats can be defined. These include Nr. 6 from 3.3.1 as influence through other software and Nr. 4 as influence through communication interfaces.

An attacker attacks the software, parameters, measurement result, stored result or indication through

- *Other software*
- *User Interface*
- *Communication interface*
  - *Direct influence by connecting a device to the measurement instrument*
  - *Through transmission (including software downloads)*
- *Connecting a device to the instrument*
- *Replacing hardware.*
  - *Replacing complete parts*
  - *Replacing components*
- *Replacing software (for Type U instruments*)*

**Note for the assessors: "Type U" instruments or “Measuring instruments using a Universal computer”, according to WELMEC 7.2 [3]. See further details in WELMEC 7.2 [3]: "Type U" is further explained in Chapter 5.1; and correspondingly Chapter 4.1 describes "Type P" instruments or “Embedded Software in a Built-for-purpose Measuring Instrument”.*

3.3.4 Instrument-specific attack vectors for instruments

Based on the top-level threats instrument-specific attack vectors can be defined.

However, if a threat on the top level cannot be realized, it might not be necessary to define instrument-specific attack vectors.

On the other hand, if an instrument is based on a Universal Computer or if some hardware modules are "placed in the Cloud", instrument-specific attack vectors might need to be defined (even for instruments of risk class B or C).

Furthermore, the extraction of secret start vectors/keys in the case of a Class D or E instrument during transmission is an instrument-specific attack vectors, derived from no inadmissible influence during transmission. There shall be an assessed motivation to explain why instrument-specific risks/ attack vectors exist or not.

Notes for the assessors:

- *On a built-for-purpose (see 3.3.1) measuring instrument of risk class B, not connected to other instruments and containing all modules in one housing, the attacks on the software through the user interface is mitigated if there is a software module that receives and interprets commands from the user interface.*
- *This software module forwards only allowed commands to the other legally relevant software modules. All unknown or not allowed sequences of switch or key actuations are rejected, having no impact on the legally relevant software, device-specific parameters, measurement result, stored result or indication.*
- *Under the condition that this software module is correctly implemented, there is no need to specify instrument-specific attack vectors for this measuring instrument, concerning attacks through the user interface (see also 3.2).*
- *In that case, justification for the shorter selection of threats should be provided in the Risk Assessment Report (see section 6).*

3.4 Attack probability tree-based threats

AtPTs are a graphical representation of threats and their associated attack vectors, which can be used to efficiently examine complex threats and attack vectors alike (mainly risk classes D and E). The root node of an attack tree represents an attacker's target and/or goal, while the child nodes are refinements of such an attack. These leaf nodes of the tree then represent elementary attacks that can no longer be refined.

Examples for AtPTs may be found in [8]. Within the context of this document, AtPTs are used for three distinct purposes:

- to represent graphically the top-level threats for measuring instruments (see Section 3.3.1),
- to model additional threats for identifying applicable attack vectors for complex instruments (see Section 3.3.4),
- to estimate the probability of occurrence for complex attack vectors by means of attribute propagation (see Section 4.2.2).

3.4.1 Attack probability trees based on generic threats with high-level attack vectors

All following examples relate to the identified main assets (software, parameters, measurement result, stored result and indication), from 3.1 and to the generic threats from Section 3.3.1.

3.4.1.1 Attacks on legally relevant software

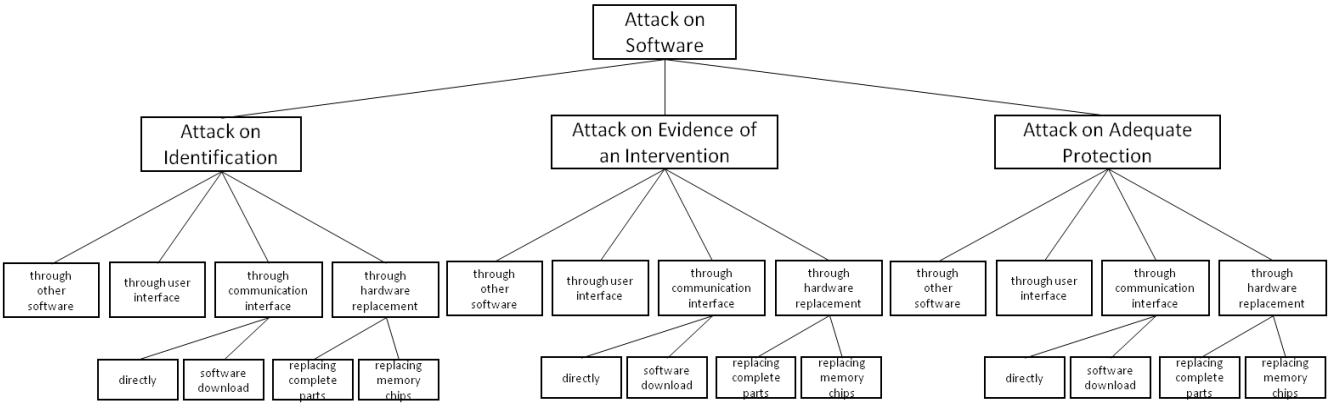

Figure 3-2: Generic AtPT for threats pertaining to the manipulation of software and its derived assets.

An attack can have an impact on the identification, evidence of an intervention or general protection of the software during processing (inadmissible influence).

The three sub-trees indicate (based on the measuring instrument architecture from WELMEC Guide 7.2 [3]) how an attack might be implemented without going into any technical detail.

3.4.1.2 Attacks on legally relevant parameters

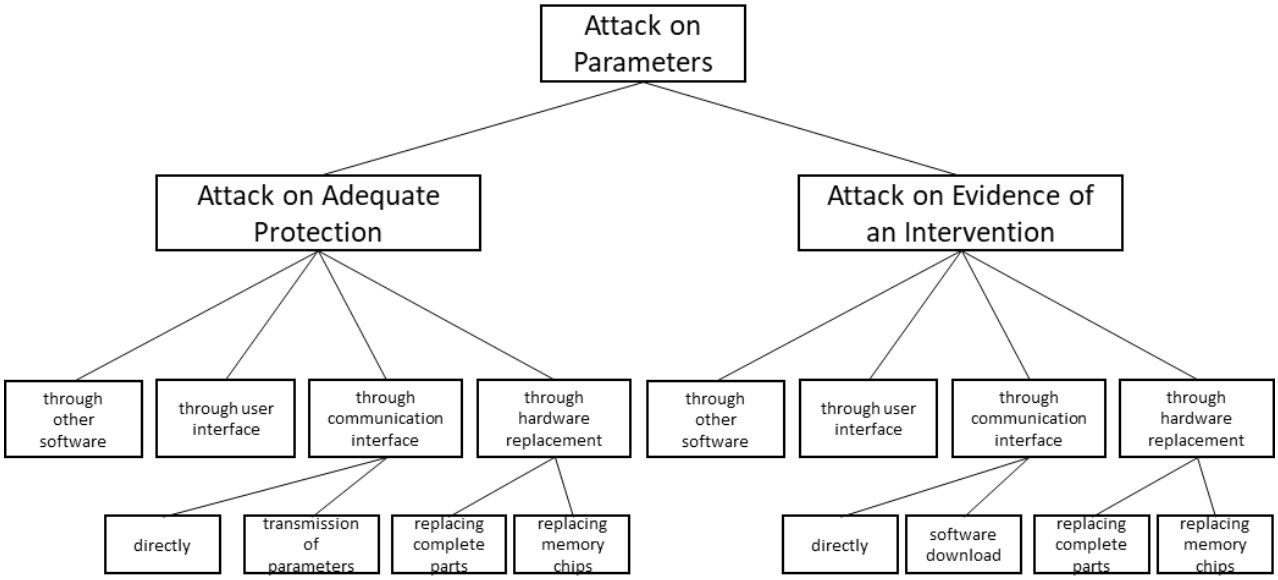

Figure 3-3: Generic AtPT for threats pertaining to the manipulation of parameters.

3.4.1.3 Attacks on legally relevant measurement results during processing

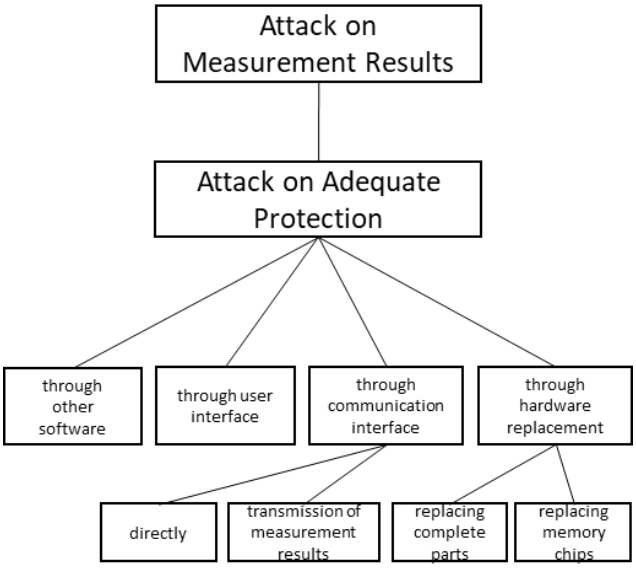

Figure 3-4: Generic AtPT for threats pertaining to the manipulation of measurement results.

3.4.1.4 Attacks on stored measurement results

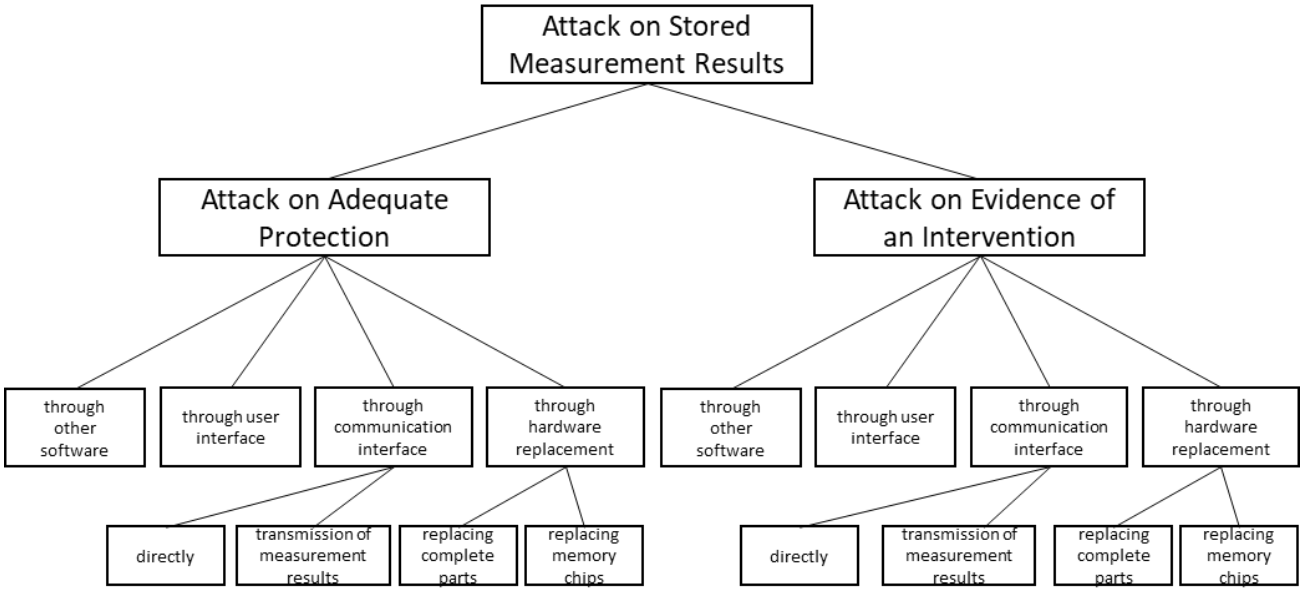

Figure 3-5: Generic AtPT for threats pertaining to the manipulation of stored measurement results.

3.4.1.5 Attacks on the legally relevant indication of a measurement result

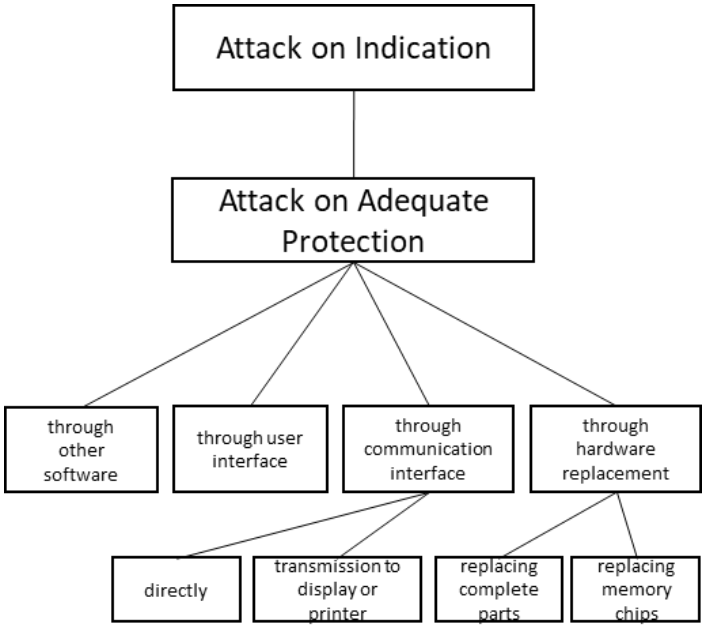

Figure 3-6: Generic AtPT for threats pertaining to the manipulation of the legally relevant indication.

3.4.2 Attack probability tree based on instrument-specific attack vectors

Instrument-specific threats can be represented by attack probability trees (see **Figure 3-7**). These allow an examiner to split certain threats into separate sub goals depending on the instrument properties. To allow for the comparability of assessment results for such threats, it is important to document the respective attack probability trees fully, see Annex C.

The following is an example of a taximeter taken from [8]. The example is described in detail in annex D.

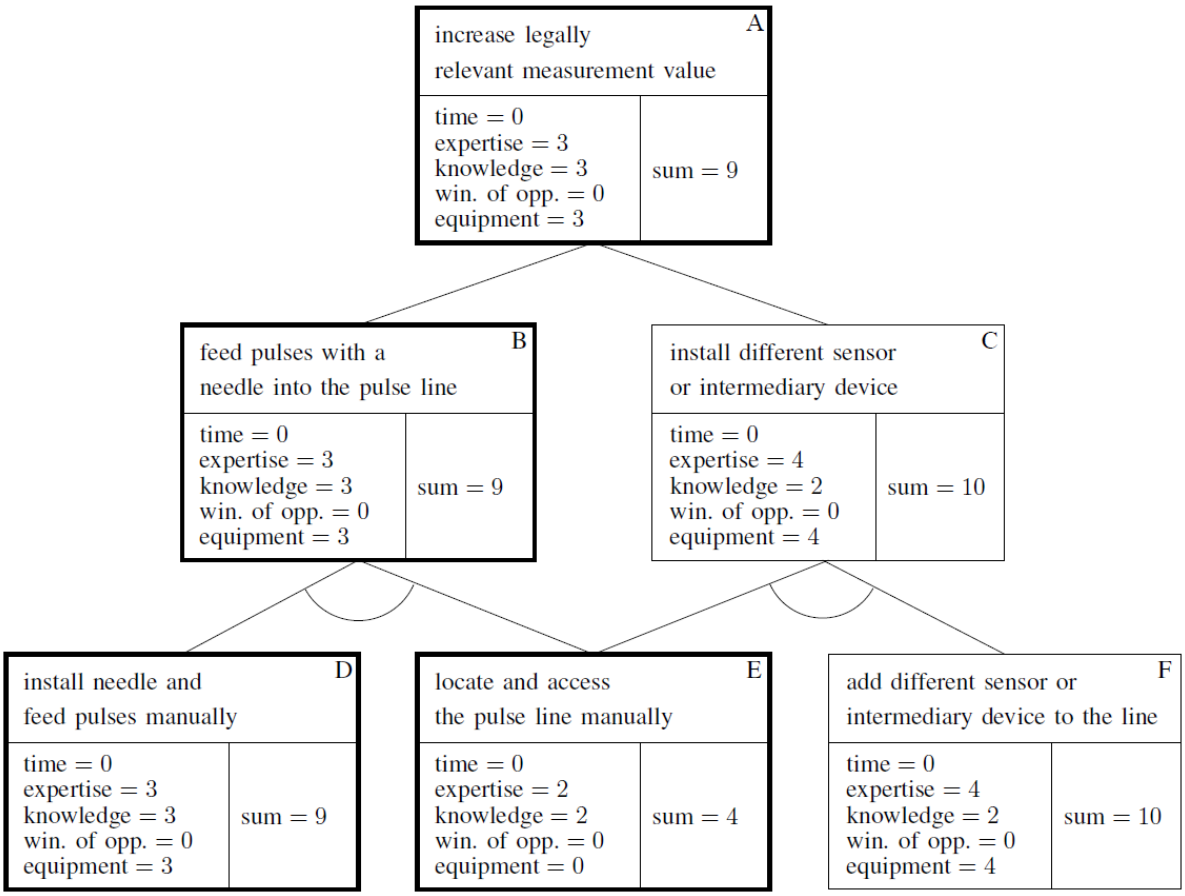

Figure 3-7: Exemplary Attack Probability Tree with assigned scores for all nodes for manipulation of a taximeters measurement value by tampering of the analog signal path. In this scenario, two known attack vectors exist: the manual feeding of additional pulses into the pulse line by means of a needle (node (B)) and the installation of a different pulse generator or other intermediary device into the signal path (node (C)). As these two attack vectors are alternatives of one another, they are linked to the parent node (A) by an OR-connection expressed by two simple edges. An arc between two or more edges would represent an AND-connection.

[8]

4 Risk Analysis: Analysis of Attack Vectors

The risk analysis shall take the design of the instrument into consideration.

If for example the instrument consists of separate modules and/or has peripheral devices included in the measuring chain, the risk shall be evaluated on two levels:

1. For each separate module[2] or peripheral;
2. For the complete instrument.

The fact that the software of one module is adequately protected does not necessary mean that the complete instrument is adequately protected, i.e. software on the other modules might be inadequately protected.

And the integrity of the complete instrument might be compromised by attacking one module or the interface between modules of the instrument.

4.1 Risk analysis on top level attack vectors

The risk assessment on the top-level threats consists of two steps:

1. The assessor shall discard all elementary attack vectors from the generic AtPTs (see Section 3.4.1) which are not applicable, i.e. because the addressed property (such as other software or a communication interface) is not present. Those attack vectors do not need to be examined further.
2. The assessor shall also check that the remaining top-level attack vectors are countered by a countermeasure according to one of the acceptable solutions from WELMEC Guide 7.2 [3]. These attack vectors are considered to be adequately mitigated by the implementation of these acceptable solutions.

If the measuring instrument is assigned risk class C or lower where acceptable solutions listed in WELMEC 7.2 are used and no additional instrument specific threats need to be considered (see 3.3.4), the risk analysis is finished when the top-level attack vectors are analyzed.

Otherwise, the probability of occurrence for the remaining attack vectors shall be estimated according to the method described in Section 4.2.

4.2 Risk analysis on instrument-specific attack vectors

4.2.1 Identification of additional attack vectors

This method can be a tool to find additional threats, attack vectors and assets, in addition to the generic ones identified from the MID [1]/NAWID [2] and WELMEC 7.2 [3]. Regardless of the risk class of the instrument, the assessor shall consider if additional attack vectors exist, for example related to non-simple technology such as cloud connection or distributed instrument:

[2] It might be helpful that producers of modules and/or peripheral have their equipment risk assessed under the voluntary modular approach, see WELMEC guide 8.8 and the different technical implementation guides for the voluntary modular approach for specific measuring instruments on the WELMEC website.

1. For instrument that do not use an acceptable solution listed in WELMEC Guide 7.2 [3] instrument-specific attack vectors shall be considered.
2. For complex instruments, it might be necessary to consider instrument-specific attack vectors, see 3.3.4.
3. For measuring instruments from risk classes D and higher, more complex attacks shall be taken into account in addition to those attacks described in Section 3.3.1. For example, such attacks could use more than one interface (e.g. a combination of user interface and communication interface) or could depend on cryptographic attacks on data during transmission (e.g. extraction of secret start vectors/keys).

If the attack vectors become too complex to handle in full, AtPTs can be used to illustrate which (simple) elementary attack vectors can be combined for a threat to be realized. The usage of AtPTs in legal metrology is explained in detail in [8].

4.2.2 Probability estimation

In order to estimate the probability of occurrence of an attack vector, a method called vulnerability analysis from ISO/IEC 18045 [10] is used. The analysis consists of assigning a point score to the attack vector in five different categories, namely required time, expertise and knowledge of the attacked target of evaluation (TOE) as well as the window of opportunity and special equipment needed.

Attack ID	Attack vector description	Time	Expertise	Knowledge	Window of opportunity	Equipment	Total	Impact	Justification
AVx1									
AVx2									
AVx3									

Table 4-1: Evaluation of elementary attack vectors

Each attack vector (AVxy) must be properly described for an easy evaluation of the assessment results. Based on this description, a justification for the selected point scores must be given to ensure the objectiveness of the results. Examples for evaluated attack vectors with associated justification of the point scores are given in Annex D. Each individual complete attack vector (e.g. the root node of the Attack Probability Tree) must have an assigned impact score, which can be either 1 for attacks executed once affecting all future (or past) measurements, or $\frac{1}{3}$, for attacks needing to be repeated for each individual measurement event.

For mapping the calculated sum score to a probability score respectively, refer to **Table 7-6** in Annex B. Afterwards, the risk associated with each attack vector is calculated by multiplying impact and probability score.

If an AtPT has been used to examine a complex attack vector, rules to calculate the probability of occurrence of the root node from the scores of the leaf nodes are given in [8]. The risk associated with the root node is then again calculated by multiplying its impact and probability score.

5 Risk Evaluation

In the final step of risk assessment, the estimated risk scores are put into the context of the measuring instrument type. For instruments in risk class C and lower, a risk score lower than four is generally acceptable. If the calculated risk score is higher, the assessor should request the manufacturer to implement additional protective measures and to repeat the assessment. For risk classes D and higher, the assessor should decide if the upper limit for the risk assessment score needs to be set to a lower value depending on the intended field of application.

For simple instruments (generally risk class C and lower), no score is needed in case that all attack vectors have countermeasures according to an acceptable solution or are not applicable and if no instrument-specific attack vector exist, see 4.2.1 and **Figure 2-1** workflow.

5.1 Risk evaluation in the context of a measuring devices purpose and the respective motivation of an attacker

WELMEC Guide 7.2 [3] gives examples for some kinds of measuring devices in Extension I. However, for instruments that are not covered there and/or instruments with a dedicated purpose, the following procedure may be applied in order to account for the purpose of the measuring instrument type:
The calculated “Risk Point Score” according to Chapter 4 may be taken as an upper limit and may be reduced under the following considerations:

Assess the purpose of the device under the following three aspects in an “Attacker’s Risk Assessment Considerations”:

5.1.1 Attacker’s Benefit (AB) – what will be the benefit of the manipulation?

Though attacks “just for the sake of it” can of course not fully be excluded, there is still a higher likelihood for a particular attack, when the attacker has some benefit from this attack. This may be taken into account with the following classification:

	Benefit	Point Score
I	None	3
II	Small financial benefit or harming a competitor	2
III	Medium financial benefit	1
IV	High financial benefit	0

Note: The distinction between small and large financial gain is, certainly, somewhat subjective. As a rule of thumb: If the attacker can gain enough money to live from it, it should be considered a “high financial benefit”.

5.1.2 Attacker’s Risk of being suspected (ARS) – how obvious is it, who benefits from the manipulation?

If it is likely that an attacker will be suspected, because he is the only person who would benefit from a particular attack, this attack will be less likely than one, where the attacker can hide in anonymity.

	Profiteers	Point Score
I	Only a single person would benefit from the manipulation	3
II	Small group of persons (e.g. staff of a particular company)	2
III	Large, but limited group of persons	1
IV	Literally anyone	0

Note: This aspect is similar to "Risk of Sanction" in WELMEC Guide 5.3, Annex I, 10.

5.1.3 Attacker's Risk, when getting caught (ARC) – what would be the consequences, if the attacker gets caught?

The higher the potential punishment for a particular manipulation is, the less likely it will be that someone is willing to take this risk.

	Potential punishment	Point Score
I	Long arrest	3
II	Short arrest	2
III	Large financial fee	1
IV	Small financial fee	0

Note: This aspect is similar to "Severity of Sanction" in WELMEC Guide 5.3, Annex I, 11.

5.1.4 Taking into account the attacker's motivation

The point scores from 5.1.1 to 5.1.3 can be summed up to give a measure of the attacker's motivation, yielding values between 0 (high motivation) and 9 (low motivation). Following the argumentation given in [9], this value can be taken as a lower limit for the point scores for "expertise" and "equipment" for each attack vector – i.e. if the sum of 5.1.1 to 5.1.3 yields 6, the point scores for "expertise" and "equipment" should not be chosen lower than 6.

6 Risk Assessment Report

For simple instruments using acceptable solutions, the checklist from Annex A can be used to report the results of the risk assessment.

For all other instruments, a report template is provided in Annex C.

7 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", Official Journal of the European Union L 96/149, 29.3.2014

[2] „Directive 2014/31/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 non-automatic weighing instruments", Official Journal of the European Union L 96/107, 29.3.2014

[3] WELMEC Guide 7.2 "Software", https://www.welmec.org/guides-and-publications/guides/

[4] WELMEC Guide 7.5 “Software in NAWIs (Non-automatic Weighing Instruments Directive 2014/31/EU))” https://www.welmec.org/guides-and-publications/guides/

[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 Guide 73:2009 Risk management — Vocabulary, Geneva, CH, Standard, November 2009”

[7] “ISO/IEC Guide 73:2002 Risk management — Vocabulary — Guidelines for use in standards, Geneva, CH, Standard, January 2002”

[8] Esche et al. “Representation of Attacker Motivation in Software Risk Assessment Using Attack Probability Trees.” Federated Conference on Computer Science and Information Systems (FedCSIS) 2017 https://annals-csis.org/Volume_11/drp/pdf/112.pdf

[9] Esche, Thiel: “Incorporating a Measure for Attacker Motivation into Software Risk Assessment for Measuring Instruments in Legal Metrology.” 18. GMA/ITG-Fachtagung Sensoren und Messsysteme 2016 https://doi.org/10.5162/sensoren2016/P7.4

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

Annex A **Checklist**

See separate Excel-file “Annex A_Riskanalysis (version 4).xlsx”

Annex B **Tables and Examples**

Table 7-1 to **Table 7-5** provide the point scores to be assigned for the different attributes of an attack. Explanations of which score to choose for a specific case may be found in the remarks column.

Elapsed Time	Points	Remarks
less than 1 day	0	An assumed attacker with the needed expertise, knowledge and equipment, who has access to the instrument can implement the considered attack vector in less than one day.
less than 1 week	1	An assumed attacker with the needed expertise, knowledge and equipment, who has access to the instrument can implement the considered attack vector in less than one week, as the attacker needs to prepare a simple script to perform the attack or perform a simple strength password search.
less than 2 weeks	2	An assumed attacker with the needed expertise, knowledge and equipment, who has access to the instrument can implement the considered attack vector in less than two weeks, as the attacker needs to prepare a simple program to perform the attack or perform a simple strength password search.
less than 1 month	4	An assumed attacker lacks in the needed expertise, knowledge or equipment, or does not have the access to the instrument and can implement the considered attack vector in less than one month, as the attacker needs to prepare a moderate complex script to perform the attack or perform a moderate strength password search.
less than 2 months	7	An assumed attacker lacks in the needed expertise, knowledge or equipment, or does not have the access to the instrument and can implement the considered attack vector in less than two months, as the attacker needs to prepare a moderate complex program to perform the attack or perform a moderate strength password search.
less than 3 months	10	An assumed attacker lacks in the needed expertise, knowledge or equipment, or does not have the access to the instrument and can implement the considered attack vector in less than three months, as the attacker needs to prepare a moderate complex program to perform the attack or perform a moderate strength password search.
less than 4 months	13	An assumed attacker lacks in the needed expertise, knowledge or equipment, or does not have the access to the instrument and can implement the considered attack vector in less than four months, as the attacker needs to prepare a complex program to

		perform the attack or perform a strong strength password search.
less than 5 months	15	An assumed attacker lacks in the needed expertise, knowledge or equipment, or does not have the access to the instrument and can implement the considered attack vector in less than four months, as the attacker needs to prepare a complex program and infrastructure to perform the attack or perform a strong strength password search or simple cryptographic key.
less than 6 months	17	An assumed attacker lacks in the needed expertise, knowledge or equipment, or does not have the access to the instrument and can implement the considered attack vector in less than four months, as the attacker needs to prepare a complex program and infrastructure to perform the attack or perform a strong strength password search or moderate cryptographic key.
more than 6 months	19	An assumed attacker will need longer than half a year to implement the attack. This includes both steps performed on the actual instrument and preparatory work performed elsewhere, as the attacker needs to prepare a complex program and infrastructure to perform the attack or perform a strong strength password search or strong crypto-graphic key.

Table 7-1: Point scores for elapsed time

Expertise	Points	Remarks
Layman	0	With respect to IT skills, a layman is any person able to browse websites with a PC.
Proficient	3	A proficient user would be anyone able to find, install and use specialized software (such as a network sniffer) for a specific task.
Expert	6	Anyone able to write, build and use specific software to perform a certain task would count as an expert.
Multiple expert	8	The expertise level “multiple expert” should only be chosen when expertise in more than one field (software development, cryptography, hardware development) is required to implement an attack.

Table 7-2: Point scores for expertise

Knowledge of the system	Points	Remarks
Public	0	The knowledge needed to implement the attack is publicly available. Any information that can be found by searching the Internet falls into this category.
Restricted	3	Examples for restricted knowledge are user manuals only shipped together with an instrument. Such information is available only to a restricted group of people and not to the public.

Sensitive	7	Information only known to the manufacturer and authorized persons. An example for sensitive information would be connection settings only shared between the manufacturer and the user.
Critical	11	Information only known to a limited number of employees of the manufacturer and possibly the conformity assessment body are classified as “critical”. A password set by a verification officer would also fall into this category.

Table 7-3: Point scores for knowledge of the system

Window of opportunity	Points	Remarks
Unnecessary/ unlimited access	0	Unnecessary/unlimited access signifies that an attacker does not need to have access to the instrument to implement an attack or that there is no risk of being detected during access.
Easy	1	Access qualifies as easy if access to the instrument is obtainable without difficulty and if it does have to last longer than a day.
Moderate	4	If an attacker does not need to have access to the instrument for longer than a month and if the access is probably detected this qualifies as moderate access.
Difficult	10	Difficult access signifies that an attacker will need to directly access the instrument for more than a month and detection is highly probable.
None	**	If access to the measuring system is impossible due to time constraints, the associated attack scenario does not need to be evaluated.

Table 7-4: Points scores for window of opportunity

Equipment	Points	Remarks
Standard	0	Standard equipment is any equipment readily available such as any common tool on a PC or software that can be freely downloaded from the Internet.
Specialized	4	If a tool needs to be bought or can be written without major effort, this falls into the category of specialized equipment.
Bespoke	7	Bespoke equipment would be highly sophisticated software that needs to be developed specially for the purpose of attacking the instrument.
Multiple bespoke	9	The level multiple bespoke should only be used if several bespoke tools for different purposes (cryptanalysis, software development etc.) are needed.

Table 7-5: Point scores for equipment

Sum of point scores	Probability score	Remarks

0 – 9	5	The instrument offers no resistance to attacks and the attack is very likely to occur.
10 – 13	4	The instrument has only basic security features; an attack is likely to occur.
14 – 19	3	The security features of the instrument offer enhanced basic protection. The attack is not very likely to occur.
20 – 24	2	The instrument offers moderate resistance to attacks and an attack is unlikely to occur.
>24	1	The security features of the instrument ensure high protection against attacks; the attack is very unlikely.

Table 7-6: Mapping of point scores to probability score

A selection of exemplary fully evaluated attack vectors is given in **Table 7-7**.

Attack ID	Attack vector	Time	Expertise	Knowledge	Window of opportunity	Equipment	Justification
Exp. 1	The attacker guesses correctly a four-digit administrator password by trying arbitrary combinations.	1	0	0	0	0	Assumed attacker: user of the instrument. Entering a password lasts a maximum of 10 seconds, all 10,000 combinations can be tested in 100,000 seconds = 1.15 days. Any layman able to operate a PC can execute the attack. As the user is the attacker, the window of opportunity is unlimited. No special equipment is needed.
Exp. 2	The attacker constructs a fake measurement result from measurement datasets that are protected by a CRC32 calculated with a secret start vector.	0	3	3	0	0	Assumed attacker: customer Since CRC is a linear logical operation on binary vectors, an XOR-connection of two datasets automatically produces a third dataset with correct CRC. The XOR-connection can be calculated with standard software by any proficient user. For obtaining two or more datasets, no window of opportunity is needed for the customer. The kind of checksum (CRC32) is described in the user manual.
Exp. 3	The attacker calculates the secret CRC32 start vector from captured measurement datasets that were each created using the secret start vector.	1	6	3	4	4	Assumed attacker: customer A CRC32 start vector has a length of 32 bits. Therefore, 2^32 = 4.3*10^9 possible start vectors exist. Any attacker with programming skills (expert) could write a program (specialized tool) to find the correct start vector by brute-force search within a few hours. To check whether the correct vector has been found several thousand datasets with checksums are needed. Obtaining those requires a moderate window of opportunity. The kind of checksum (CRC32) is described in the user manual.

Table 7-7: Exemplary evaluated attack vectors

Annex C **Report Format**

1) Brief summary of the assessed [measuring instrument type] [name].

ID	Type of component	Description
C1	Communication interface	
U1	User interface	
S1	Storage of measuring data	
X1	Transmission of measuring data	
P1	Storage of legally relevant software	

Table 1: List of data transmissions, storages, user and communication interfaces.

2) Checklist for top-level threats

Here, the filled-in checklist from Annex A shall be included.

3) Additional instrument-specific attack vectors

Here, an assessed motivation shall be provided to explain why instrument-specific risks/attack vectors need to be considered or not. In case additional instrument-specific threats need to be considered (see 3.3.4) the following Tables shall be completed.

a) List of additional threats enabled by instrument-specific attack vectors

ID	Threat target	Description
T1		
T2		
T3		

Table 2: List of considered threats.

Note: Targets (Tx.x) from Annex A can be used as threats for risk class C and lower.

b) List of evaluated attack vectors (AVxy) that enable threat Tx.

Attack ID	Attack vector Descrip-tion	Time	Expertise	Knowledge	Window of oppor-tunity	Equipment	Total	Impact	Justifica-tion
AVx1									
AVx2									
AVx3									

Table 3: Evaluation of elementary attack vectors

If elementary attack vectors need to be combined by means of an attack probability tree to fulfil an additional threat, such attack probability trees shall be provided here.

c) List of probability score, assigned impact and final risk score for each attack vector (AVxy)

Attack ID	Total	Proba-bility Score	Impact	Risk
AVx1				
AVx2				
AVx3				

Table 4: Risk score assigned to each attack vector.

Note: The rules for calculation of total, impact, probability score and risk are given in Chapter 4.

4) Conclusion

A statement indicating if the identified risks are acceptable for the instrument or if countermeasures need to be implemented shall be made here.

Annex D **Assessment of Attack Probability Trees**

The most basic properties of any attack tree can be summarized as follows: While the root node of such a tree constitutes an attacker's main goal, its child nodes can be seen as refinements thereof, which need to be achieved in order to reach said goal. Following this interpretation, the leaf nodes of an attack tree constitute atomic attacks, for which no further refinement is possible. An exemplary tree that only consists of six nodes is given in **Figure 7-1**.

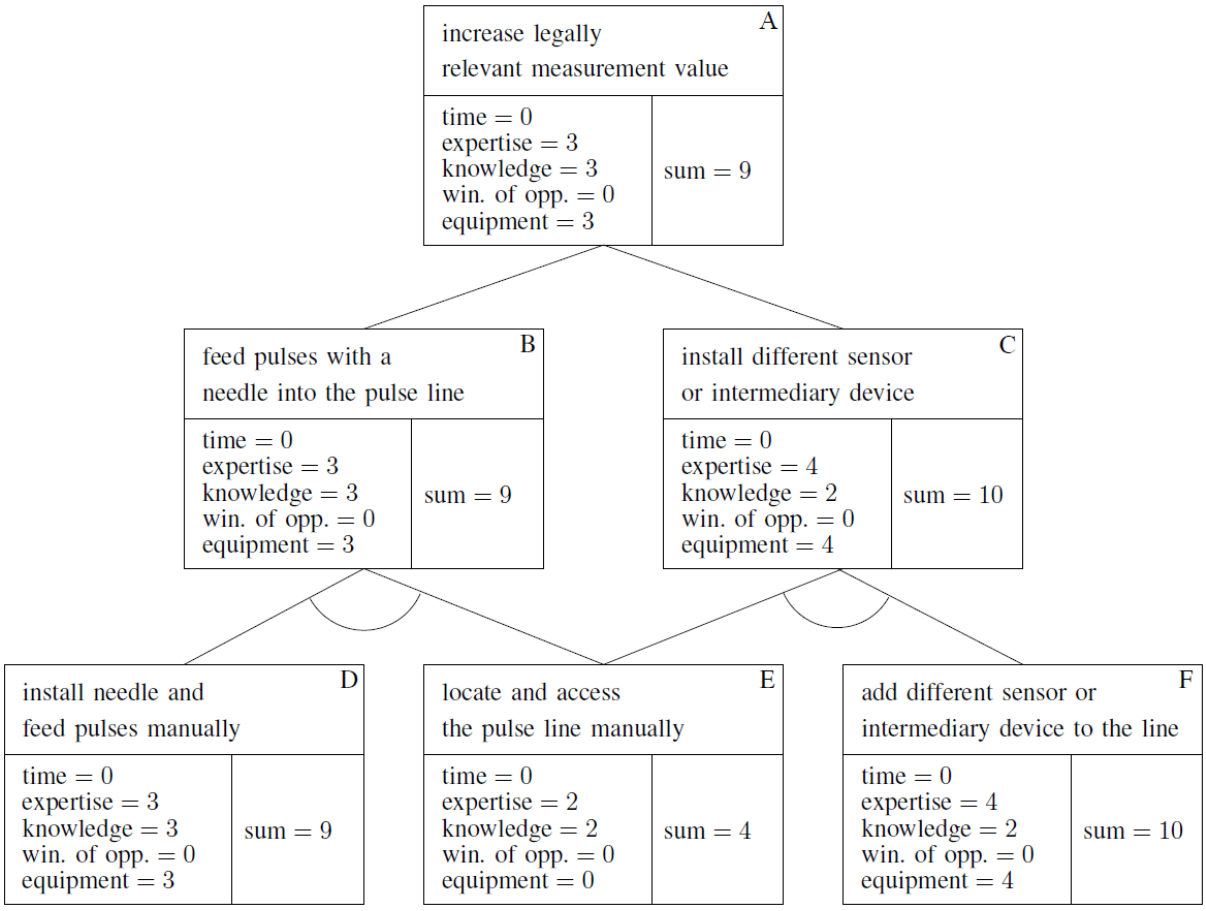

Figure 7-1: Exemplary attack probability tree for a taximeter connected to a pulse generator at a car's wheel by means of a pulse line

In the example, an attacker's possible strategies to manipulate the fare calculated by a taximeter are illustrated. Before exploring the meaning of the shown tree, it is necessary to explain the specifics of its graphical representation:

Child nodes are always logically connected to either form an AND- or an OR-expression. The AND-statement is illustrated by an arc connecting the respective child nodes and indicates that all of these need to be implemented to achieve the attack associated with the parent node. On the other hand, if child nodes represent alternative ways to reach the parent objective, they are connected via an OR-statement, in which case no arc is drawn.

There is no guarantee that an attack tree will be a binary tree. However, if more than two child nodes are identified, they can always be transformed into a binary structure by combining pairs of them into sub goals until only two child nodes remain. The exemplary attack tree given in **Figure 7-1** illustrates attacks on the analog signal path between pulse generator at a car’s wheel and taximeter.

For this scenario, two known attack vectors exist:

- the manual feeding of additional pulses into the pulse line by means of a needle (node (B) in **Figure 7-1**) and
- the installation of a different pulse generator or other intermediary device into the signal path (node (C) in **Figure 7-1**).

As these two attack vectors are alternatives of one another, they are linked to the parent node (A) by an OR-connection expressed by two simple edges. An arc between two or more edges would represent an AND-connection. Such AND-statements may be found in the next level of the AtPT. The feeding of pulses by means of a needle (node (B)) requires both access to the pulse line (node (E)) and the manual feeding of pulses itself (node (D)). If a different sensor is to be installed (node (C)), again access to the pulse line is required (node (E)). In addition, the installation itself needs to be realized (node (F)). Again nodes (E) and (F) are linked by an AND-statement. Interestingly, node (E) plays a role in both attacks and thus offers the possibility of functioning as a possible entry point for a countermeasure. To calculate the probability score of the original threat (A), the leaf nodes (D), (E) and (F) are each assigned point scores in the aforementioned five categories. It can be shown that the combination of two nodes into a summary node has no influence on the mathematical properties of the local sub-tree, such as likelihood of occurrence. Therefore, it is the evaluator's choice to limit the number of refinements of an attack as she sees fit.

In practice, a node needs no further refinement if the associated attack constitutes a simple technical task with a known scope and easily determinable properties. Each node can be assigned a set of predefined characteristics, e.g. time, expertise, knowledge, window of opportunity and equipment as a measure for the probability of occurrence. The attributes of any parent node can be determined by combining the information associated with the respective child nodes. It is important to note that there is no requirement for any node to only exist once within a tree. Instead, nodes may have multiple copies whose attributes are linked; therefore, a change in one part of an attack tree can also affect otherwise unconnected branches. The resulting attack probability trees (AtPTs) both represent the attack logic and the probability of occurrence (and subsequently risk) associated with a threat. This means that each attack vector is no longer evaluated individually, but only the atomic attacks at the leaf nodes are assessed. This reduces the possibility for misjudging an attack and makes it possible to re-use atomic attacks for different threats.

The attributes for the parent nodes and finally for the root node can be calculated in a bottom-up fashion by observing the following stated rules. To propagate the attributes up the tree, a number of rules specifically tailored for the characteristics of each attribute are introduced:

- Time
  - AND: Time representation in point scores is logarithmic (1 for more than a day, 2 for one to two weeks, 19 for half a year). Adding up times for two attacks can, therefore, be approximated by selecting the maximum of the two.
  - OR: The time score connected to the smaller sum-score is chosen.
- Expertise
  - AND: Normally, the maximum of both scores is chosen. Should expertise in both hardware and software (HW and SW) be needed, scores are added with a maximum value of 8, see ISO/IEC 18045 [10].
  - OR: The expertise score connected to the smaller sum-score is chosen.

- Knowledge of the TOE
    - AND: The maximum of both knowledge scores is chosen.
    - OR: The knowledge score connected to the smaller sum-score is chosen.
- Window of opportunity
    - AND: A smaller window of opportunity (higher score) for one node is the relevant limit. Therefore, the maximum is selected.
    - OR: The window of opportunity score connected to the smaller sum-score is chosen.
- Equipment
    - AND: The maximum of both equipment scores is chosen unless equipment from different areas is required (HW or SW), in which case the scores are added with a maximum of 9 according to the ISO/IEC 18045 [10].
    - OR: The equipment score connected to the smaller sum-score is chosen.