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

WELMEC Guide 7.6

Software Examination by Means of Risk Assessment

Version 2026

For information:

This Guide is made available for the Working Group Measuring Instruments (European Commission expert group E01349) for consideration for future referencing on the Europa Website.

WELMEC WG7 welcomes any kind of feedback on the WG7 Software Guides, which may be sent to the WG7 SG "Evolution of Software Guides" (wg7@welmec.org).

If problems are encountered during software examination due to fundamental changes in these Software Guides, WG7 suggests using Guide 7.2:2025 as an alternative for a **transition period of 18 months** after publication of these Guides.

WELMEC e.V. is a cooperation 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 e.V. 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 EU Directives. Alternative approaches may be acceptable, but the guidance provided in this document represents the considered view of WELMEC e.V. as to the best practice to be followed.

Published by:

WELMEC Secretariat

E-mail: secretary@welmec.org

Website: www.welmec.org

SOFTWARE EXAMINATION BY MEANS OF RISK ASSESSMENT

Contents

Foreword

This Guide applies to measuring instruments included in the Measuring Instruments Directive (MID, 2014/32/EU[1]) [1] and the Non-Automatic Weighing Instruments Directive (NAWID, 2014/31/EU) [2]. It is used to assess whether a solution implemented by the manufacturer to protect and secure the assets of his measuring instrument is adequate, and to demonstrate that protection against inadmissible influence on the assets is sufficient.

[1] **Please note**: This issue of the Guide remains valid for Directive 2004/22/EC, as well.

1 Terminology

The terminology explained in this chapter describes the vocabulary as used in this Guide. References to a standard or to any other source are given if the definition is completely or in essential parts taken from it.

Source	Term	Definition
Guide 7.2:2025	acceptable solution	A design or a principle of a software module or hardware unit, or of a feature that is considered to comply with a particular requirement. An acceptable solution provides an example of how a particular requirement may be met. It does not prejudice any other solution that also meets the requirement.
	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 that are not divided further are referred to as elementary attacks.
	assessor	In this Guide, assessor refers to the person(s) chosen by the manufacturer of a measuring instrument to perform the risk assessment.
ISO/IEC 27005:2022	asset	Anything that has value to the organization, and which therefore requires protection. Note 1: Assets are assigned one or more of the following security properties: availability, integrity, authenticity. Note 2: The essential requirements of the MID and NAWID must be examined to determine which assets are of value from a legal metrology perspective, see Guide 7.1. Note 3: Assets can be properties of measuring instruments which shall be protected.
D31:2023	audit trail	Continuous data containing a time stamped information record of events, e.g., changes in the values of the parameters of a measuring instrument or software updates, or other activities that are legally relevant and which are critical for the metrological characteristics.

D31:2023	authentication	Checking of the declared or alleged identity of a user, process, or measuring instrument. Note: This may be necessary when checking that downloaded software originates from the owner of the certificate.
	authenticity	The asset that was retrieved, received, or loaded corresponds to the same asset that was previously stored, transmitted or processed by the authorized entity. Note: The authorized entity is either the LR SW within the measuring instrument, or, when a software update is performed, the manufacturer.
	availability	The asset can be retrieved, received, or loaded within the required time frame when necessary for its metrological purpose.
D31:2023	checking facility	Facility that is incorporated in a measuring instrument and which enables a significant defect to be detected and acted upon. Note: "Acted upon" refers to any adequate response by the measuring instrument (luminous signal, acoustic signal, prevention of the measurement process, etc.).
Adapted from D31:2023	communication Interface	Physical part of an instrument that enables information to be passed between measuring instruments, components of measuring instruments or other external systems. Note 1: Communication interfaces can be wired, optical, radio, etc. communication and they are usually designed to use a specific protocol. Note 2: This definition does not include communication between software modules, see software interface.
Adapted from D31:2023	component	Identifiable hardware part of an instrument that performs a specific function or functions, and that can be separately evaluated in accordance with WELMEC Guide 8.8, and the specific metrological and technical performance requirements as specified in the relevant WELMEC Guide for that component.

	custom solution	A design or a principle of a software module or hardware unit, or of a feature that is considered to comply with a particular requirement. A custom solution can be implemented by the manufacturer if there is no acceptable solution available. The suitability is proven by a risk assessment.
D31:2023	data domain	Location in memory that each program needs for processing data. Note: Data domains may belong to one software module only, or to several.
D31:2023	device-specific parameter	Legally relevant parameter with a value that depends on the individual instrument, component and/or module(s) subject to legal control.
	event	Action that has an impact on a security property of an asset within a measuring instrument. Note: Examples for events are the change of a legally relevant parameter or the update of the legally relevant software.
D31:2023	fault	Difference between the error of indication and the intrinsic error of a measuring instrument. Note 1: Principally, a fault is the result of an undesired change of data contained in or flowing through an electronic measuring instrument. Note 2: From the definition it follows that a “fault” is a numerical value which is expressed either in a unit of measurement or as a relative value, for instance as a percentage.
	generic attack vector	Attack vector defined in Guide 7.2 to address most common attack paths for measuring instruments.
	integrity (of assets)	Property of maintaining the consistency of assets. Note 1: Assurance that assets have not been subjected to any unintentional, accidental or inadmissible changes, e.g., while in use, transfer, storage, repair or maintenance. Note 2: During repair and maintenance, the measuring instrument does not need to comply with essential requirements of MID.

D31:2023	interface	Shared boundary between two functional units, defined by various characteristics pertaining to the functions, physical interconnections, signal exchanges, and other characteristics of the units, as appropriate.
	legally relevant	Required to fulfill the essential requirements and/or having an impact on the compliance with the essential requirements of Annex I and the instrument-specific requirements of the MID and/or the essential requirements of Annex I and III of the NAWID.
ISO 27005:2022	level of risk	Significance of a risk expressed in terms of the combination of consequences and their likelihood. Note: This Guide uses the terms “risk” and “level of risk” interchangeably.
D31:2023	measuring instrument	Device used for making measurements, alone or in conjunction with one or more supplementary devices.
D31:2023	measurement data	Data used during the measurement process. Note: Measurement data includes the measured quantity value, measurement result relevant data and measurement process data, see D31:2023 Annex C.
D31:2023	measurement result	Set of quantity values being attributed to a measurand together with any other available relevant data. Note 1: The measurement result relevant data may consist of e.g. measurement uncertainty, date and time of measurement, number of measurement, identification of sensor and in the case where price calculation is part of the legally relevant software, unit price and price to pay. Note 2: The measurement result (including the measured quantity value according to OIML V 2:200:2012) is used for the legally relevant purpose, e.g. conclusion of a transaction.

	operating system	A collection of software, and firmware elements that control the execution of computer programs and provide services such as computer resource allocation, job control, input/output control, file management and hardware control in a computer system. Note 1: Other programs (such as editors, office programs etc.) not intended for these tasks do not count as part of the operating system. Note 2: An operating system may be legally relevant as a whole, or it is partly legally relevant, or not at all. Note 3: To collect legally relevant parts of the operating system, see Annex III of Guide 7.1, and imagine the "measurement chain". Note 4: In most cases, parts of the operating system like boot loader, kernel, interfaces, resource management, user administration, mathematical and cryptographic libraries, and configuration files are legally relevant.
	physical part	Any legally relevant physical property of a component that can be modified or removed.
	peripheral device	A specific type of a legally non-relevant component that adds functionally to the measuring system. Note: A keyboard or mouse are examples of peripheral devices.
Recast 7.2	prevention	Means that makes it impossible to change an asset.
Recast 7.2	protection	Means that either makes it impossible to change an asset or allows changes to an asset to be detected.
Recast 7.2	relevant documents	Instrument-specific WELMEC Guides, normative documents or harmonized standards.
D31:2023	remote verification	Set of procedures to support verification of an instrument during use, potentially without a person on site.
ISO/IEC 27005:2022	risk	Effect of uncertainty on objectives. Note: This Guide uses the terms "risk" and "level of risk" interchangeably.

ISO/IEC 27005:2022	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 31073:2022	risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
	risk class	Class that defines the level of risk assessment based on the software protection level, software examination level and software conformity that is applicable to a category of measuring instruments.
	risk estimation	Process to assign values to the probability and consequences of a risk.
ISO 31073:2022	risk evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk is acceptable or tolerable.
ISO 31073:2022	risk identification	Process of finding, recognizing and describing risks.
Adapted from D31:2023	sealing	Means intended to protect the assets of a measuring instrument. Note: This may be achieved by hardware, software or a combination of both.
	securing	Means of restricting access to assets; makes it impossible to change assets without proper credentials.
Adapted from Guide 7.2: 2023	software download	The process of automatically transferring software to a target measuring instrument or component using any technical means from a local or distant source (e.g., exchangeable storage media, portable computer, remote computer) via arbitrary connections (e.g., direct links, networks).
D31:2023	software examination	Technical operation that consists of determining one or more characteristics of the software according to the specific procedure (e.g., analysis of technical documentation or running the program under controlled conditions).
D31:2023	software identification	Sequence of readable characters (e.g., name, version number, checksum) that represents the software or software module under consideration. Note: Software identification can be checked on an instrument whilst in use.

D31:2023	software interface	Program code and dedicated data domain; receiving, filtering, or transmitting data between software modules. Note 1: A software interface is not necessarily legally relevant. Note 2: A software interface is an interface between two or more software modules, used to exchange data and transmit commands.
D31:2023	software module	Software entity such as a program, subroutine, library, parameter or data set, and other objects including their data domains that may be in relationship with other entities. Note: The software of measuring instruments consists of one or more software modules.
Adapted from MID	sub-assembly	A hardware device (hardware unit) that functions independently and makes up a measuring instrument together with other sub-assemblies (or a measuring instrument) with which it is compatible.
	threat	An unwanted event that may lead to the invalidation of one or more security properties of an asset.
D31:2023	time stamp	Unique value, e.g. in seconds or a date and time string denoting the date and/or time at which a certain incident (e.g. measurement or event) occurred.
D31:2023	type-specific parameter	Legally relevant parameter with a value that depends on the type of instrument, component and/or module subject to legal control. Note: Type-specific parameters are part of the legally relevant software.
D31:2023	user interface	Interface that enables information to be interchanged between the user/operator and the measuring instrument or its (hardware) components or (software) modules. Note: Typical examples of user interfaces are switches, keyboard, mouse, display, monitor, printer, touchscreen, software window on a screen including the software to generate it.

1.1 Abbreviations

AB	attacker’s benefit
ARC	attacker’s risk when getting caught
ARS	attacker’s risk of being suspected
AtPt	attack probability tree
CRC	cyclic redundancy check
EMC	electro-magnetic compatibility
HW	hardware
MID	Measuring Instruments Directive
NAWID	Non-Automatic Weighing Instruments Directive
RC5	Rivest cipher 5
RSA	Rivest–Shamir–Adleman cryptosystem
TOE	target of evaluation

2 How to use WELMEC Software Guides

Guide 7.1 is the central starting point for readers who are new to software examination. It explains the basic concept of risk-based requirements and provides an overview of the software examination procedure. The Guide also defines structures and procedures to be used by WELMEC members when updating any of the WELMEC Software Guides.

Guide 7.2 implements the core requirements based on the essential requirements of the MID and NAWID detailing that all assets need to be adequately protected. It is the starting point for any software examination.

During such an examination, an examiner first collects all assets that are present in the measuring instrument, then he or she checks that all these assets are protected. Protection means must address all applicable generic attack vectors listed in Annex II of Guide 7.2. For the examination, typically a checklist can be used, see Annex I of Guide 7.2. After that, an examiner has to assess whether the protection means are adequate. To demonstrate this, the manufacturer can either use known acceptable solutions or perform a risk assessment. To document and examine the identified assets and implemented solutions for the attack vectors, see Annex IV of Guide 7.2.

Guide 7.3 provides a collection of acceptable solutions that are suitable for different risk classes of measuring instruments. If a manufacturer implements an acceptable solution in accordance with Guide 7.3, it can be assumed that a corresponding risk assessment has already been performed by WELMEC WG7, see also Guide 7.1, subchapter 5.3.

Acceptable solutions are not mandatory. A manufacturer can implement his own solution. In that case, the appropriateness of the solution has to be shown with a risk assessment.

Guide 7.4 offers an informative overview of examples of how risk-based examination is applied to various measuring instrument designs.

Guide 7.5 contains a gap analysis between EN 45501 and WELMEC Guide 7.2, Version 2019 and has not yet been updated to reflect the recast of the WELMEC Software Guides.

Guide 7.6 describes the risk assessment method that applies to all measuring instruments. It also provides a procedure for additional attack vectors that have to be addressed when a measuring instrument belongs to risk class D or higher.

Acceptable solutions and generic attack vectors only need to be considered for assets that are present in a measuring instrument and that are legally relevant.

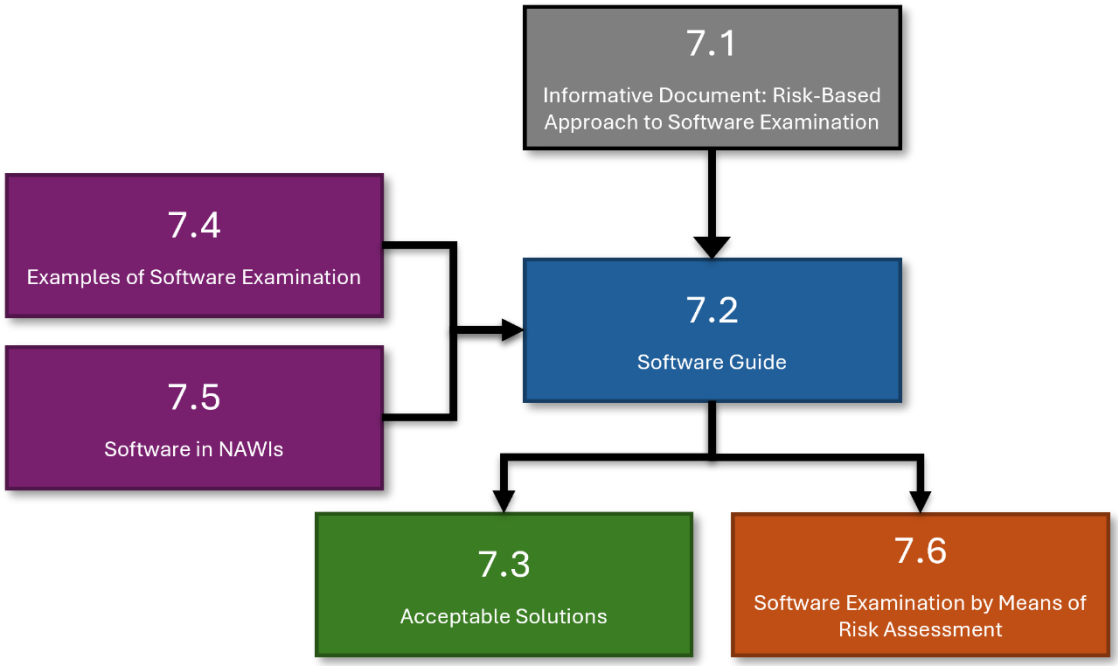

Figure 1: Relationship between the WELMEC Software Guides

The new risk-based approach, which is further described and used in Guides 7.2, 7.3, 7.4 and 7.6, may seem comparable to the traditional requirement-based approach in WELMEC Guide 7.2:2025.

However, there are differences that are discussed in Annex V of Guide 7.1.

Although not specifically mentioned in the text, if a notified body examines the software in accordance with the WELMEC Software Guides, the use of Guide 7.2 is required to ensure that the assets are protected. When the manufacturer applies an acceptable solution, Guide 7.3 is required to examine the correct implementation of the acceptable solution, and Guide 7.6 is required if the manufacturer chooses to use his own solution to assess the adequacy of that solution, taking into account, where applicable, the guidance in Guide 7.4.

The software examination results in a report combining the outcome of the software examinations with regard to the requirements in Guide 7.2, the acceptable solutions in Guide 7.3 and the risk assessment procedure in Guide 7.6. A template for a test report is given in Guide 7.2, Annex V.

The workflow of the software examination described above is visualized in Figure 2.

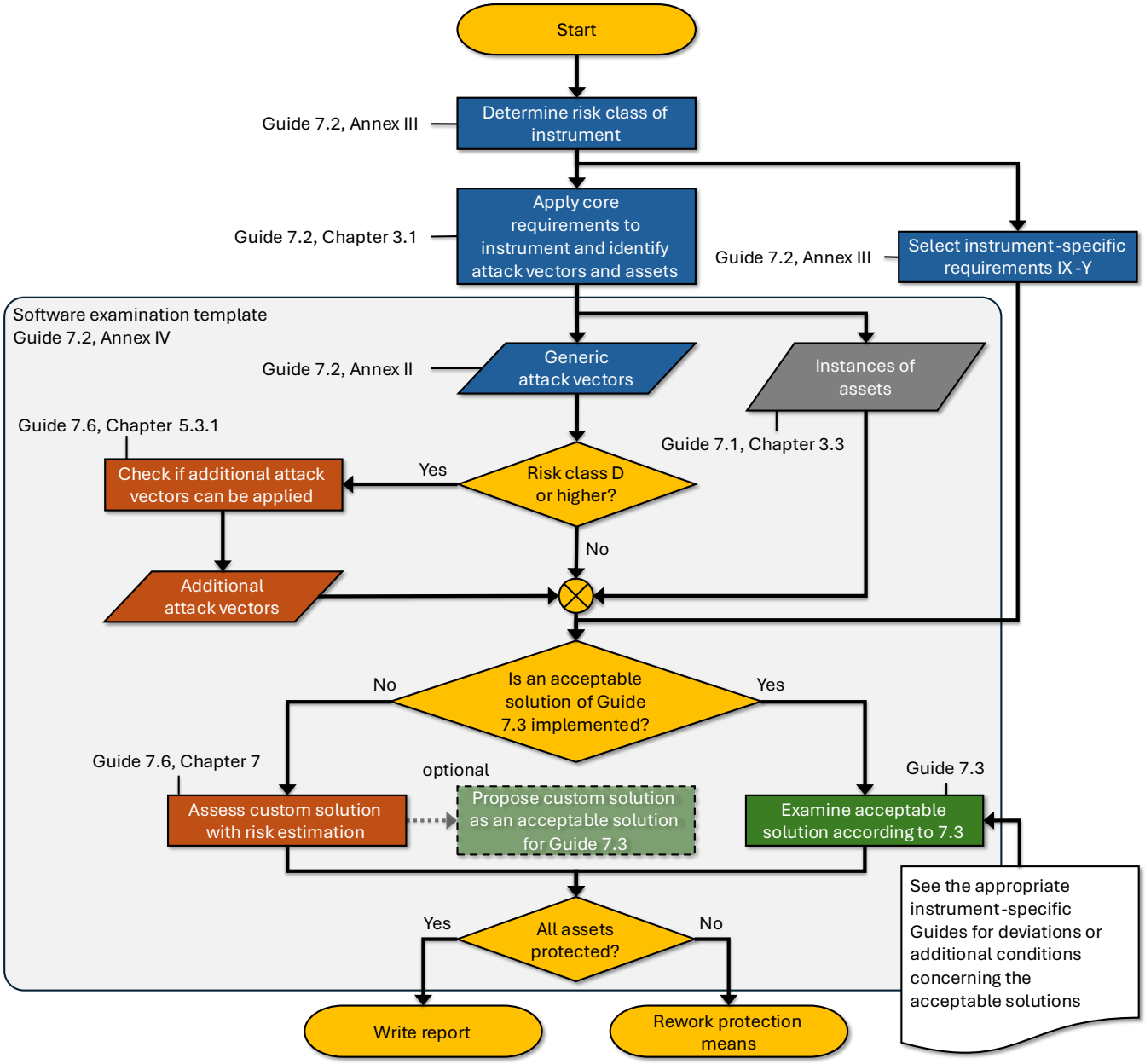

Figure 2: Workflow of the examination of the requirements using Guides 7.1, 7.2, 7.3, 7.6, and instrument-specific Guides (see the WELMEC website).

3 Introduction

Within the frame of a conformity assessment for measuring instruments in accordance with the MID or NAWID, a risk assessment shall be performed and documented by the manufacturer to demonstrate conformity of the measuring instrument with the essential requirements described in MID annex II, Module B 3c and NAWID annex II, Module B 1.3c. If a manufacturer implements an acceptable solution in accordance with WELMEC Guide 7.3, it can be assumed that a corresponding risk assessment has already been performed by WELMEC WG7. In all other scenarios, the manufacturer shall use the method described here to assess the risks resulting from the chosen implementation.

It is the responsibility of the notified body to analyze the submitted risk assessment and to determine whether 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 or NAWID. This Guide does not deal with other risks, such as EMC, health issues, risk of electrical shock etc. Wherever MID or WELMEC Guide 7.2 [3] is referred to, this also applies to NAWID and WELMEC Guide 7.5 [4] which have equal or similar requirements. In both cases, this Guide provides a method to assess additional risks, especially for new technology not addressed by established acceptable solutions.

The method is targeted both at manufacturers of such measuring instruments to help them provide an adequate risk assessment report and at notified bodies, specifically the notified bodies under module B, G and H1 of the MID and the NAWID, to aid them in the task of analyzing the submitted report, i.e., whether the report covers all threats against the assets and whether the proposed means to mitigate the threat are 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 27005:2022 [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 – in legal metrology referred to as threats;
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.

4 Risk Assessment

4.1 Overall structure of this Guide

The method described here follows the framework and definitions provided by ISO/IEC 27005:2022, that divide the process of risk assessment into three distinct stages:

1. Risk identification and identification of attack vectors (see chapter 5): By default, generic attack vectors (see Guide 7.2, Annex II) should be investigated, see guidance in Guide 7.2 and Guide 7.3. For risk class D and higher, additional attack vectors should be investigated, see chapter 5.3. For complex attacks, attack probability trees (AtPTs) can be used to help with the assessment.
2. Risk analysis (see chapter 6): If custom solutions that deviate from the acceptable solutions in Guide 7.3 are used, threats are assigned a quantitative risk measure by analysis of the attack vectors.
3. Assessment of custom solutions (see chapter 7): Here, the risk is calculated in the context of the examined measuring instrument and its anticipated field of application to determine whether the residual risk (after risk mitigation) is acceptable. The chapter also provides a method to account for attacker motivation during risk assessment.

4.2 How to perform the assessment

As a precondition for working with this Guide, the manufacturer shall have supplied and documented a solution for a core requirement from Guide 7.2 (see chapter 3 in Guide 7.2). The objective of the assessment is to check whether the proposed custom solution is adequate for the applicable attack vector.

Chapter 8 provides guidance for examiners on how to check risk assessments.

The process is also depicted in Figure 3.

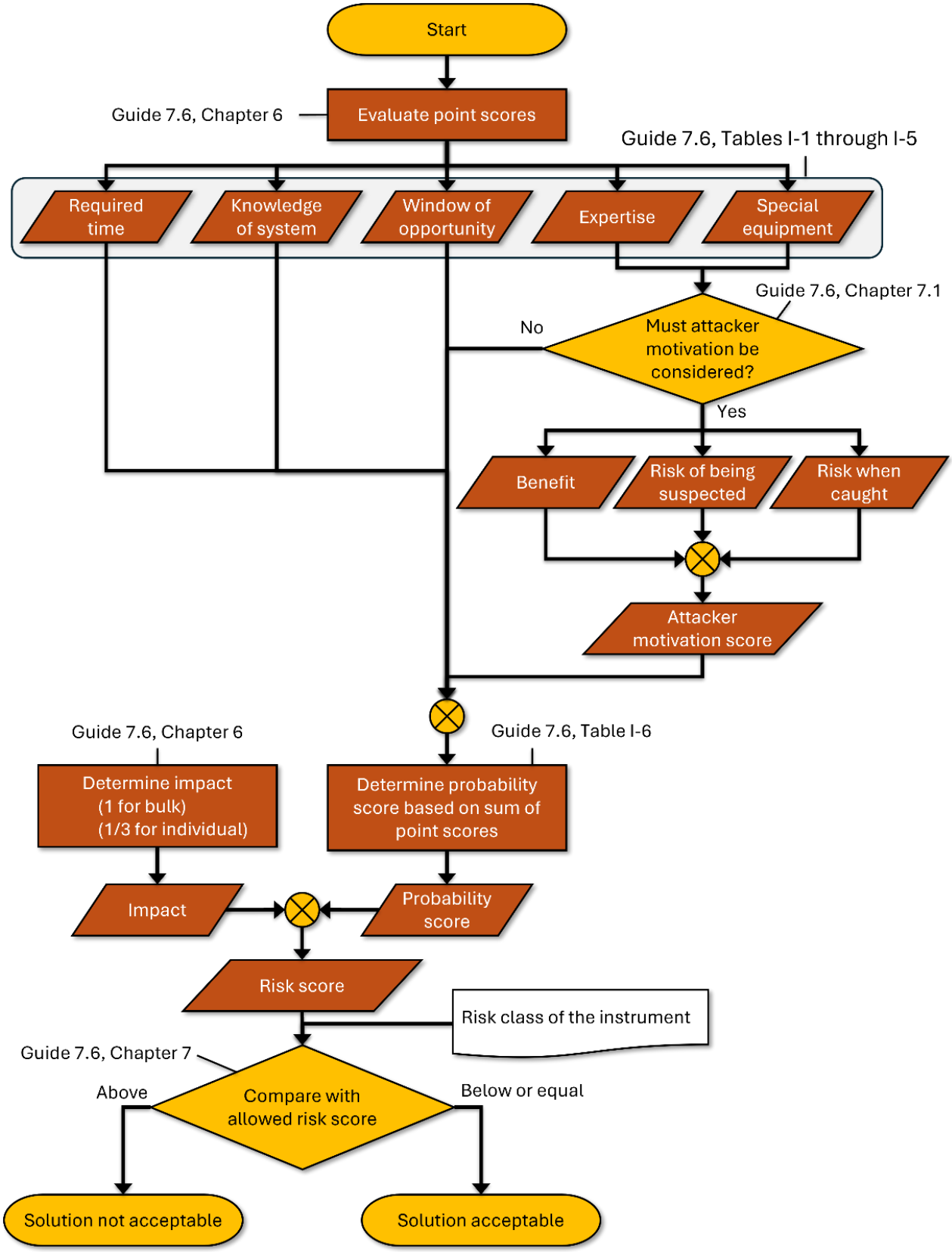

Figure 3: Workflow of the risk assessment.

5 Risk Identification and Identification of Attack Vectors

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

5.1 Assets

The assets and their security properties are defined in Guide 7.1.

5.2 General remarks regarding threats and assets

Threats consist of at least one asset and one corresponding statement about which security property (availability, integrity and/or authenticity) can be invalidated by the threat. With the aim of quantifying the risk associated with each threat, distinctions must be made between the individual instance of an asset and the attack vectors applicable to each individual instance of an asset. Attack vectors provide the technical steps necessary to implement a threat, which can be objectively quantified with the help of this Guide, see chapter 6.

5.3 Attack vectors

Any software examination/risk assessment shall take into account at least the generic attack vectors as described in Guide 7.2, Annex II, and consider additional attack vectors for risk class D and above.

5.3.1 Additional attack vectors

Based on the attack vectors from Guide 7.2, Annex II, additional attack vectors can be defined for risk class D and above. The aim of these additional attack vectors is to assess attacks which may only be possible in a specific instrument design and are not covered by the generic attack vectors.

However, if an attack vector cannot be realized, it might not be necessary to define additional attack vectors at all.

Examples for additional attack vectors include:

- generating fake visual input for optical length measurements;
- manipulation of the time source connected to an electricity meter used for tariffing.

5.3.2 Complex attack vectors based on attack probability trees

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 [6].

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 (risk class D and above). The root node of an attack probability tree represents an attacker's target and/or goal, while the child nodes are refinements of such an attack. Leaf nodes of the tree then represent elementary attacks that can no longer be refined. To allow for the comparability of assessment results for such threats, it is important to document the respective attack probability trees fully, see Annex IV.

Examples for AtPTs may be found in [6]. Within the context of this document, AtPTs are used to estimate the probability of occurrence for complex attack vectors by means of attribute propagation (see chapter 6.2).

6 Risk Analysis: Analysis of Attack Vectors

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

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

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

The fact that the software of one module is adequately protected does not necessarily mean that the measuring instrument as a whole is adequately protected, i.e. software on the other modules might be inadequately protected.

6.1 Probability of occurrence and risk for simple attack vectors

In order to estimate the probability of occurrence of an attack vector, a method called vulnerability analysis from ISO/IEC 18045 [7] 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. Reference values for point scores and corresponding examples are given in Annex I and Annex II.

The sum of all point scores for an attack vector shall then be used to obtain a score for probability of occurrence for the attack according to the mapping provided in Table I-6 in Annex I.

A high value of the sum score (total) indicates a high security of the proposed solution. This will result in a low probability score indicating a low probability for the attack vector on a device implementing the proposed solution.

A low value of the sum score (total) indicates low security of the proposed solution. This will result in a high probability score indicating a high probability for the attack vector on a device the proposed solution has been implemented in.

Regarding the impact of the individual attack vector on compliance with the core requirements, a score of 1 shall be assigned if the attack impacts a large number of measurements. If the attack must manually be repeated for each measurement, a score of ⅓ shall be assigned. The product of probability score and impact rounded to the next integer number then yields the risk associated with the attack vector.

The point scores for Expertise and Equipment can be modified according to the attacker motivation, see chapter 7.1.

[2] It might be helpful that producers of modules and/or peripherals 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.

Attack vector ID	Attack vector description	Time	Expertise	Knowledge of the system	Window of opportunity	Equipment	Total	Probability score	Impact (see 6.1)	Risk	Justification (see 8)
AVx1											
AVx2											
AVx3											

Table 1: Aid for documenting point scores, sum score, probability score, impact, and risk.

6.2 Probability of occurrence and risk for attacks based on attack probability trees

Nodes within an attack probability tree may be linked with each other to either form an AND- or an OR-statement. Information will enter the AtPT only via the leaves. The attributes for the parent nodes and finally for the root node can be calculated in a bottom-up fashion by observing the following rules. The rationale for each rule is also given.

Attribute	Propagation rule for point score for AND-/OR-connections
Time	AND: Time scores are logarithmic (1 for more than a day, 2 for a one week to two weeks, 17 for half a year), therefore the maximum of both scores needs to be chosen which is a good approximation for the logarithm of two added time spans. OR: The smaller sum-score indicates which time score is to be chosen.
Expertise	AND: If expertise in different areas is required (HW/SW), the scores are added with a maximum of 8 in accordance with ISO/IEC 18045. Otherwise, the maximum is chosen. OR: The smaller sum-score indicates which expertise score is to be chosen.
Knowledge of the TOE	AND: The maximum of both knowledge scores is chosen. OR: The smaller sum-score indicates which knowledge score is to be chosen.
Window of Opportunity	AND: A smaller window of opportunity (higher score) for one node will also affect the other node. Therefore, the maximum is selected. OR: The smaller sum-score indicates which window of opportunity score is to be chosen.
Equipment	AND: If equipment from different areas is required (HW/SW), the scores are added with a maximum of 9 in accordance with ISO/IEC 18045. Otherwise, the maximum is chosen. OR: The smaller sum-score indicates which equipment score is to be chosen.

7 Assessment of Custom Solutions

In the final step of the risk assessment, the estimated risk scores are put into the context of the measuring instrument type.

The acceptable risk scores for each risk class may be found in Table 2 as well as in Guide 7.1, chapter 5.2.3. If the assessed risk is higher than these scores, the instrument design needs to be revised to mitigate the applicable attack vectors adequately.

Risk Class	Software Protection	Software Examination	Software Conformity	Risk score
A	low	low	low	≤ 5
B	middle	middle	low	≤ 4
C	middle	middle	middle	≤ 3
D	high	middle	middle	≤ 2
E	high	high	middle	1
F	high	high	high	1

Table 2: Link between risk classes and risk scores.

7.1 Attacker motivation

The following procedure may be applied in order to account for the purpose of the measuring instrument type. The procedure adds upper bounds on attacker capabilities in case of low motivation. This may be used to justify a lower sum score/resistance to attacks if the instrument is used for a specific purpose.

7.1.1 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

Table 3: Illustration of the score for attacker's benefit.

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".

7.1.2 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 or she 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 people (e.g., staff of a particular company)	2
III	Large, but limited group of people	1
IV	Literally anyone	0

Table 4: Illustration of the score for attacker's risk of being suspected.

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

7.1.3 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, 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

Table 5: Illustration of the score for attacker's risk when getting caught.

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

7.1.4 Taking into account the attacker's motivation

The point scores from 7.1.1 to 7.1.3 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 [8], 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 7.1.1 to 7.1.3 yields 6, the point scores for "expertise" and "equipment" should not be chosen lower than 6.

8 Examination Guidance for Risk Assessments

This chapter is intended to provide guidance on how to check a risk assessment during software examination for a proposed technical solution, taking into account a combination of

- instance of an asset,
- security property, and
- attack vector.

8.1 Inclusion of additional attack vectors

Based on the risk assessment submitted, the examiner shall decide whether the manufacturer has investigated additional attack vectors and, if such an investigation has been neglected, whether he has provided proper justification for doing so.

The list of additional attack vectors shall be checked for completeness: Has at least one additional attack vector been formulated for each asset instance and each security property?

For each additional attack vector, the following examination steps shall be performed:

- For risk class D and higher, the examiner shall check the manufacturer's justification for not including additional attack vectors, if applicable.
- Together with the examiner for the metrological characteristics, the software examiner shall check that the choice of the attack vectors is plausible or whether there exist simpler alternatives.

8.2 Attacker motivation score

If the manufacturer has decided to modify point scores according to the attacker motivation, the calculation of the attacker motivation score shall be checked first. This step only has to be performed once per risk assessment since the motivation score will be identical for all threats and attack vectors.

With respect to the motivation score, the examiner shall check that valid assumptions have been made for the three subscores AB, ARS and ARC, see tables in 7.1.1, 7.1.2 and 7.1.3.

The manufacturer's choice with respect to AB, ARS and ARC shall be checked with the help of Annex I. If the assigned point score appears to be too high, the manufacturer is to be asked for additional justification. Basically, there is no wrong motivation score. The important thing is that the decision for a specific score and, if applicable, the justification is properly documented.

Afterwards, the examiner shall check that the attacker motivation scores have been correctly calculated by adding the three subscores:
attacker motivation score = AB + ARS + ARC

8.3 General examination guidance

The following steps shall be performed for each attack vector:

- Check that the manufacturer has examined and assessed all applicable generic attack vectors from Guide 7.2, Annex II for each asset.
- Check that the assigned point scores (see Annex I) match the individually given justification and the technical specification of the measuring instrument.
- If the manufacturer has chosen to accommodate an attacker motivation score

(see 8.2), the examiner shall check that the motivation score has been used correctly as a lower bound for expertise and equipment in the assessment of all attack vectors.

- The examiner shall check that the sum score of the point scores has been calculated correctly and whether the choice of the impact factor is plausible. If only a single measurement is affected by an attack, the impact score must be ⅓, otherwise it shall be 1.
- The examiner shall check that the sum score has been correctly turned into a probability score in accordance with Table I-6 from Annex I.
- Finally, the examiner shall check that probability score and impact score have been correctly multiplied to calculate the risk score.

If the risk score is within the limit defined in chapter 5.2.3 in Guide 7.1, the attack vector is considered to be sufficiently mitigated. Otherwise, the manufacturer shall amend the design.

8.4 Source Code Checks

For measuring instruments in risk class E, the examiner shall check that the countermeasures to individual attack vectors have been correctly implemented in the source code.

9 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 (recast) Text with EEA relevance, OJ L 96, 29.3.2014, p. 149–250.

[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 (recast) Text with EEA relevance, OJ L 96, 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 27005:2022(e) Information security, cybersecurity and privacy protection — Guidance on managing information security risks, Geneva, CH, Standard

[6] 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

[7] “ISO/IEC 18045:2022 Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation”, International Organization for Standardization, Geneva, CH, Standard

[8] 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

Annex I. Tables and Examples

Table I-1 to Table I-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 measuring 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 measuring 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 measuring 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 measuring 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 measuring 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 measuring 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 measuring 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 measuring 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 measuring 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 measuring 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 I-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 I-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 a measuring 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 I-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 measuring 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 measuring 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 measuring 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 measuring 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 I-4: Points scores for window of opportunity

Equip-ment	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.
Special-ized	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 measuring 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 I-5: Point scores for equipment

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

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

A selection of exemplary fully assessed attack vectors is given in the following table:

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 measuring 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 I-7: Exemplary assessed attack vectors

Complete example including risk assessment:

An implementation for protection of parameters shall serve as an illustrative example: In this example, the parameters are transmitted between components that are part of a distributed measuring instrument. To ensure the authenticity of the parameters during transmission, they are encrypted with a symmetric RC5 algorithm.

- Instance of asset: parameters transmitted between components
- Security property: authenticity
- Generic attack vector: IIT1 (inadmissible influence through man-in-the-middle attacks)
- Proposed solution: encryption with a symmetric RC5 cipher
- Risk assessment for the RC5 cipher:

Attack vector ID	Attack vector description	Time	Expertise	Knowledge of the system	Window of opportunity	Equipment	Total	Probability score	Impact (see 6.1)	Risk	Justification (see 8)
AVx1	An attacker manipulates parameters during transmission after having calculated the private key from the public RSA key.	1	6	3	10	4	24	2	1	2	

Breaking RC5 can be done, and generating false parameter sets requires writing a specific tool (equipment score of 4) by an expert within a few days (score 1 for time). The window of opportunity is limited, because data can only be modified during transmission. Once the symmetric key has been extracted, all future parameters can be modified or falsely injected (impact score of 1).

The sum score of 24 results in a probability score of 2, see Table I-6 and a subsequent risk of 2. Thus, the solution is acceptable for risk classes B to D.

Annex II. Checklist

See software examination template on the WELMEC website here[3].

[3] https://www.welmec.org/welmec/documents/guides/7.2/2026/WELMEC_Guide_7.2_2026_Annex_IV_Software_Examination_Template.xlsm

Annex III. Test Report Template

A unified test report template for software examination, also applicable for risk assessments in accordance with Guide 7.6, is available as a separate Excel file on the WELMEC website here[4]. This template may be used by manufacturers and examiners alike.

[4] https://www.welmec.org/welmec/documents/guides/7.2/2026/WELMEC_Guide_7.2_2026_Annex_V_Test_Report_Template.docx

Annex IV. Assessment of Attack Probability Trees

The most basic properties of any attack probability 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 that need to be achieved in order to reach said main goal. Following this interpretation, the leaf nodes of an attack probability tree constitute atomic attacks, for which no further refinement is possible. An exemplary tree that only consists of six nodes is given in Figure V-1.

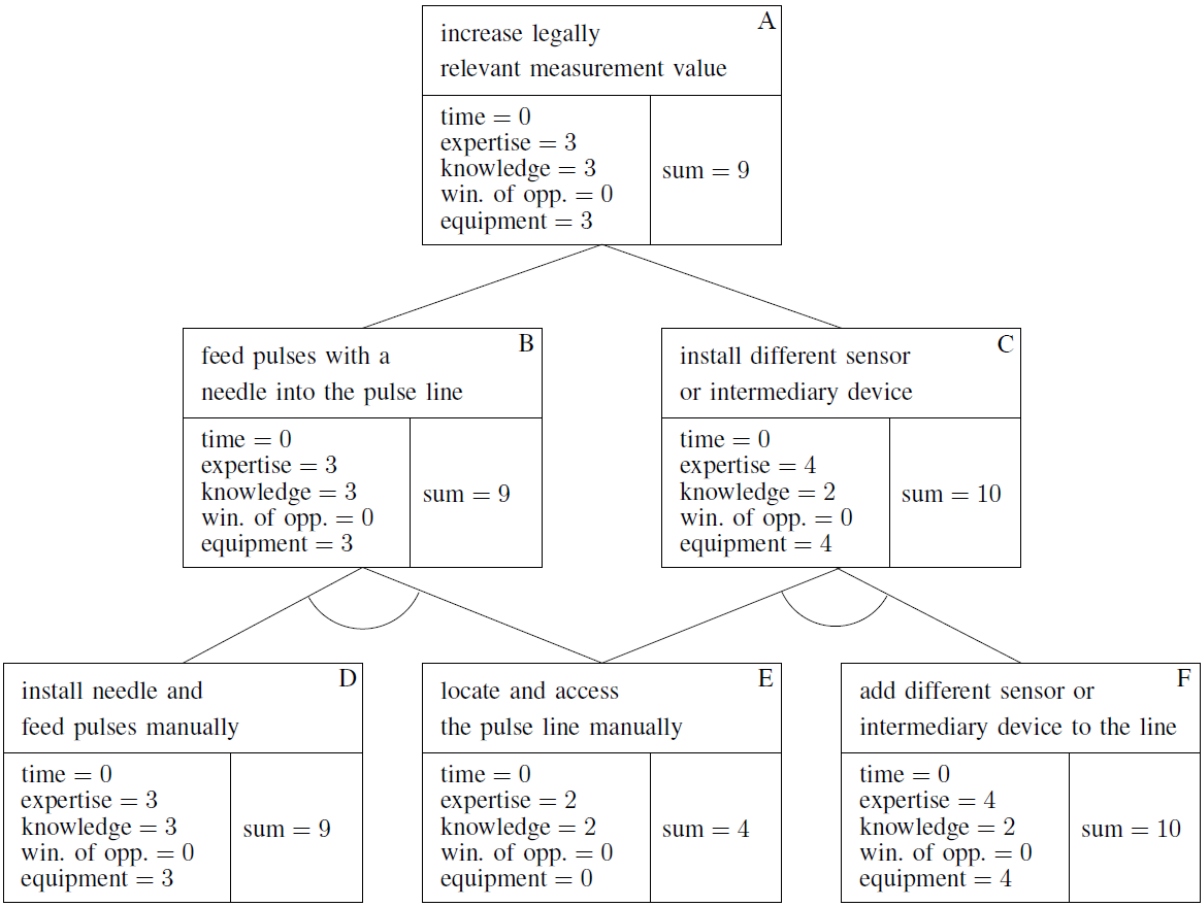

Figure V-1: Exemplary attack probability tree for a taximeter connected to a pulse generator at a car's wheel by means of a pulse line

In the example, an attacker's possible strategies to manipulate the fare calculated by a taximeter are illustrated.

Before exploring the meaning of the tree shown, it is necessary to explain the specifics of its graphical representation:

Child nodes are always logically connected to form either 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 probability 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 probability tree given in Figure V-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 V-1) and
- the installation of a different pulse generator or other intermediary device into the signal path (node (C) in Figure V-1).

As these two attack vectors are alternatives to 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 examiner'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 probability 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 assessed 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.
    - 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.
    - OR: The equipment score connected to the smaller sum-score is chosen.

Annex V. Revision History

No.	Date	Significant Changes
1	June 2026	A recast of the Guide has been carried out to evaluate the risk-based requirements in WELMEC Guide 7.2 taking into account the acceptable solutions listed in WELMEC Guide 7.3.