WELMEC Guide 7.6

recast

Software Evaluation

For measuring instruments

Draft Version 1.0.1

WELMEC e.V., Bundesallee 100, 38116 Braunschweig, Germany.
Phone: +49 531 592 1980 E-mail: secretary@welmec.org

WELMEC

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: welmec.org

Software Guide
Contents

Deleted: 5
Deleted: 10
Deleted: 10
Deleted: 12
Deleted: 13
Deleted: 14
Deleted: 15
Deleted: 19
Deleted: 20
Deleted: 22
Deleted: 24

Foreword

This Guide is oriented on instruments included in the Measuring Instrument Directive (MID) (2014/32/EU[1]) and the Non-Automatic Weighing Instrument Directive (NAWID) (2014/31/EU) and is used to evaluate if the solution implemented by the manufacturer to protect and secure the assets of their 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 also valid for Directive 2004/22/EC.

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. If a manufacturer implements an acceptable solution in accordance with WELMEC 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 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 **Error! Reference source not found.** describes the general workflow of the software risk assessment method.

Section **Error! Reference source not found.** introduces threat definitions for the assets derived in Guide 7.x and lists attack vectors to be addressed during risk assessment.

Section 2.2 deals with estimation of risk scores for a given technical implementation.

Section **Error! Reference source not found.** places the estimated risk scores in the context of the measuring instrument type and its field of application.

A template test report is available as a separate document on the WELMEC website.

Deleted: 2

Deleted: 3

Deleted: 4

Deleted: 5

1 Terminology

Source	Term	Definition
Guide 7.2:2023	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, 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.
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: Assets can be properties of measuring instruments which must 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
D31:2023	authenticity	result of the process of authentication (passed or failed).
Guide 7.2:2023	category 1 component	components that are part of the measuring process i.e., that handle measurement data to construct the measurement result including the primary indicator device.
Guide 7.2:2023	category 2 component	components that further process the measurement result without modification to finalize the transaction.
D31:2023	checking facility	facility that is incorporated in a measuring instrument and which enables 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.).

Source	Term	Definition
D31:2023	communication Interfaces	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. and they are usually designed to use a specific protocol. Note 2: This definition does not include communication between software parts, 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 according to WELMEC Guide 8.8, and the specific metrological and technical performance requirements as specified in the relevant WELMEC Guide for that component.
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.
D31:2023	event	action in which a modification of a measuring instrument parameter, adjustment factor or update of software module is made. Note: For the purpose of this Document, events are considered changes in the value of the legally relevant parameters, or a modification or update of the legally relevant software, or other activities that are legally relevant and which may influence the metrological data and/or characteristics.
~~**D31:2023**~~	~~event counter~~	~~non-resettable counter that increments each time an event occurs.~~
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.
Adapted from D31:2023	integrity (of assets)	assurance that the software, measurement data, parameters, inscriptions, indications or evidence of intervention have not been subjected to any unintentional, accidental or inadmissible changes while in use, transfer, storage, repair or maintenance.
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.

Deleted: records

Source	Term	Definition
Drafting group recast Guide 7.2	legally relevant	required to fulfil 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. Note: See also Annex II of this Guide.
	MID	Measuring Instrument Directive, 2014/32/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014
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 Annex I.
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 V 2:200:2012) is used for the legally relevant purpose, e.g. conclusion of a transaction.
	NAWID	Non-Automatic Weighing Instrument Directive, 2014/31/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 26 February 2014
Guide 7.2:2023	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, and file management 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: For category 1 components or complete measuring instruments the legally relevant parts of the operating system, usually, at least consist of the boot loader, the kernel, the interfaces (hardware and inter-process communication), the (background) services, administration of user privileges, cryptographic libraries as well as the configuration files of those parts. Note 3: For category 2 components the legally relevant parts of the operating system, usually, at least consist of the interfaces (hardware and inter-process communication), administration of user privileges, cryptographic libraries as well as the configuration files of those parts.
D31:2023	protective interface	legally relevant software module that handles all data flow to the legally relevant software modules(s) in order to prevent inadmissible influences.

Source	Term	Definition
	relevant document for a specific measuring instrument	WELMEC Guide, harmonised standards, and/or normative documents aimed at that particular measuring instrument.
D31:2023	remote verification	set of procedures to support verification of an instrument during use, potentially without a person on site.
ISO/IEC 27005	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 Guide 73:2009	Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation
7.2: 2022	risk class	Class of *measuring instrument* types with almost identical risk assessments.
ISO Guide 73:2009	Risk Estimation	Process to assign values to the probability and consequences of a risk
ISO Guide 73:2009	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
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.
D31:2023	securing	means of restricting access to assets and 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., version number, checksum) that represents the software or software module under consideration. Note: Software identification can be checked on an instrument whilst in use~~, see 6.2.1~~
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.

Source	Term	Definition
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 D31:2023	protection	protection of assets or data domain by a hardware or software implemented seal with the intention of making an intervention impossible or evident.
D31:2023	software separation	separation of the software in measuring instruments, which can be divided into legally relevant module(s) and legally non-relevant module(s). Note: These module(s) communicate via a software interface.
D31:2023	storage device	device used for storing measurement data that is necessary to construct the measurement result.
7.2: 2022	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 [MID, Article 4].
	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.

2 How to use this Guide

This Guide is used to evaluate the adequacy of the solutions provided by the manufacturer to protect and secure the assets of a measuring instrument and to prevent inadmissible influences on the assets, as defined in WELMEC Guide 7.2.

2.1 Overall structure of the Guide

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 **Error! Reference source not found.**): 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 2.2): 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 **Error! Reference source not found.**): 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.

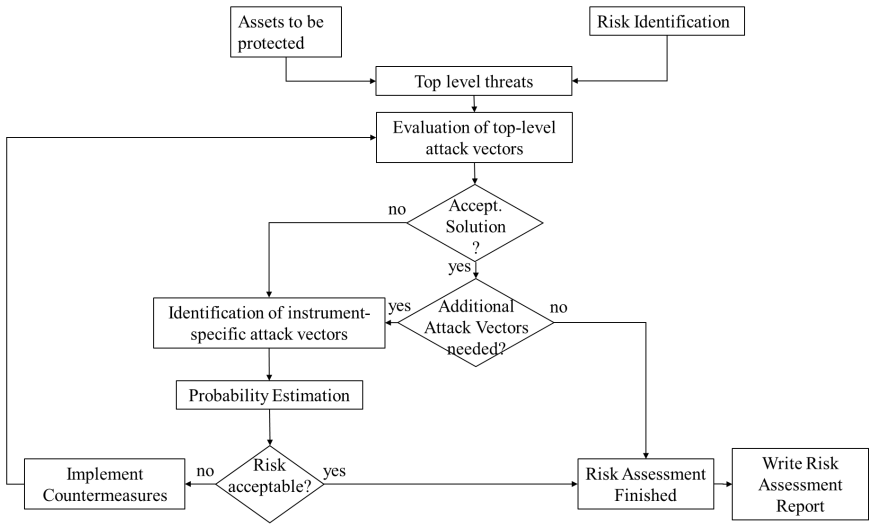

Figure 2-1: Workflow of the risk assessment procedure.

The risk assessment can be performed in two phases.

1. In the first phase, risk assessment takes place with the defined high-level threats given in **Error! Reference source not found.**
2. Depending on the complexity of the measuring instrument or its risk class, instrument-specific attack vectors have to be defined, see **Error! Reference source not found.**, 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.

Deleted: 3

Deleted: 4

Deleted: 5

Deleted: Figure 2-1

Formatted: Font: 10 pt, Not Bold

Deleted: 3.3.1

Deleted: 3.3.4

2.2 How to perform the assessment

As a precondition for working with this Guide, the manufacturer shall have supplied and documented a solution for a protection or securing requirement from Guide 7.2 (see chapter 3.2 in Guide 7.2). The objective of the assessment is to evaluate if the proposed solution is adequate taking into account known generic as well as instrument-specific and complex attack vectors.

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, see Annex V.

The risk associated with each threat is calculated and forms the basis for the evaluation of the solution. Acceptable risk scores per risk class are detailed in chapter 5.

Deleted: 4

For risk class D and higher the evaluator can take the purpose of the measuring instrument into consideration. This can result into a lower acceptable risk score, see chapter 4.2.

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.

3.1 Main assets

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

3.2 General remarks regarding threats and assets

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. With the aim of quantifying the risk associated with each threat, distinctions must be made regarding the individual instance of an asset and the attack vectors applicable to the individual instance of an asset. Attack vectors provide the necessary technical steps to implement a threat, which can be objectively quantified with the help of this Guide, see chapter 4.

3.2.1 Typical instances of assets

The following typical instances of assets shall be taken into account when performing a risk assessment in accordance with this Guide. Other instances may exist depending on the instrument design. For each instance, the applicability of the generic attack vectors detailed in chapter 3.3 shall be considered.

TIAP: During processing

AI1	Assets are loaded into volatile memory and processed, e.g., by a CPU.
Specifying Notes:	
AI1/N1	For processed assets, availability implies the capability of loading and asset into volatile memory and accessing the asset in volatile memory.
AI1/N2	For processed assets, authenticity implies authenticity of the asset source.

TIAS: Storage

AI1	Assets are stored on a storage device.
Specifying Notes:	
AI1/N1	The indication of the result is an asset that is typically not stored.
AI1/N2	For stored assets, attacks on availability include preventing mandatory storage of measurement data or evidence of intervention, and losing stored measurement data or evidence of intervention.
AI1/N3	This includes cases where the storage is full, or the storage is not available.
AI1/N4	For stored assets, authenticity implies authenticity of the storing entity.

Deleted: records

Deleted: records

TIAT: Transmission

AI1	Assets are transmitted between components or modules.

Specifying Notes:
AI1/N1 For transmitted assets, attacks on availability include inadmissible influence through transmission delays.
AI1/N2 This includes inadmissible influence on parameters that have to be available in the instrument before the measurement starts, e.g., product type. For example, in the case of liquids other than water, the type of petrol.
AI1/N3 For transmitted assets, attacks on availability include inadmissible influence due to unavailability of network services.

3.3 Attack Vectors

Any software evaluation/risk assessment shall take into account at least the following generic attack vectors, see **Error! Reference source not found.**, and if applicable consider additional instrument-specific attack vectors, see 3.3.2.

Deleted: 3.2.1

Deleted: 3.2.2

The following chapter lists generic attack vectors which are mirrored by corresponding acceptable solutions in Chapter 3.3 in Guide 7.3.

3.3.1 High-level attack vectors

The Equipment under Test can either be a complete instrument or a component (which can be tested separately). The evaluation first focus on the software and parts within the Equipment under Test (EUT), followed by an evaluation of external influences, through the available interfaces or by replacing LR-components for not-LR-components. External influence is also possible during transmission or by random errors.

3.3.1.1 Inadmissible influence on assets through software or parts within the Equipment under test

IIP1: Inadmissible influence on the measurement process through executing other functions

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1	An attacker inadmissibly influences the assets and their security properties by using system resources for other functions of the measuring instrument.		
Specifying Notes:			
AV1/N1	This covers functions of the LR-SW and functions of the OS.		
AV1/N2	Functions other than the measurement function are, for example, checking-, durability– and backup-facilities, securing and protection measures, software updates and remote verifications.		
AV1/N3	Other functions of the OS are for example cleaning-up storage, updating the OS, defragmenting.		
AV1/N4	This implies that there are enough resources for the operation of the legally relevant application.		
Functional Checks:			
AV1/F1	Try to access functions, e.g., from the user interface, that can influence the measurement process or have a negative impact on storage capacity, battery life or resources for the operation of the legally relevant application and check that they are secured.		
AV1/F2	Perform spot checks by sequentially initiating several functions of the measuring instrument and check if each function has no inadmissible influence on the measurement process, e.g., if a measurement can be performed the result has to be within the MPE or critical change value.		
AV1/F3	Initiate several functions of the LR-SW and OS to run simultaneously and check if there is no inadmissible influence on the measurement process, e.g., if a measurement can be performed the result has to be within the MPE or critical change value.		

III1: Inadmissible influence through the User interface

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1 An attacker inadmissibly influences the assets and their security properties through the user interfaces.			
Specifying Notes: AV1/N1 This includes the user interface of the measuring application and the operating system. AV1/N2 This includes modification of the access rules realized by the implemented securing measures for all assets. AV1/N3 This includes modification of the implemented protection measures without evidence of an intervention. AV1/N4 This includes the inadmissible influence on the assets by trying to modify, remove or replace assets, including software modules of the LR-SW-application or the LR-OS.			
Functional Checks: AV1/F1 Try some combinations of keys to check that they are not having an effect on the assets and their security properties. AV1/F2 Try some not documented standard commands to check that they are not accepted.			

IIB1: Inadmissible influence through the boot process

<table>
<tr><th>Risk Class B</th><th>Risk Class C</th><th>Risk Class D</th><th>Risk Class E</th></tr>
<tr><td colspan="4">AV1 An attacker inadmissibly influences the provision of the same environment for the execution of legally relevant software</td></tr>
<tr><td colspan="2">AV2 An attacker inadmissibly influences the assets and their security properties through the boot process.</td><td colspan="2">AV2 An attacker inadmissibly influences the individual modules involved in the boot process up to the legally relevant application.</td></tr>
<tr><td colspan="4">Specifying Notes:
AV1/N2 This applies to all elements of the boot process.
AV1/N3 This implies that the boot process of the operating system is unambiguous and reproducible.
AV1/N4 This implies that any module involved in creating the same environment for the execution of legally relevant software is adequately protected.</td></tr>
<tr><td colspan="4">Functional Checks:
AV1/F1 Try interrupting the boot process through the user interface.</td></tr>
<tr><td colspan="2">-</td><td colspan="2">AV1/F2 Attempt to access the BIOS or UEFI settings through the user interface and modify the boot order.

AV1/F2 Try modifying the BIOS or UEFI settings through the user interface to boot from an open interface.</td></tr>
</table>

IIA1: Inadmissible influence through the administration of the O.S.

<table>
<tr><th>Risk Class B</th><th>Risk Class C</th><th>Risk Class D</th><th>Risk Class E</th></tr>
<tr><td colspan="4">AV1 An attacker inadmissibly influences the assets and their security properties through the administration of the O.S..</td></tr>
<tr><td colspan="4">Specifying Notes:
AV1/N1 This includes basic tasks such as file, memory and process management, handling input and output, and controlling peripheral devices such as disk drives and printers.
AV1/N2 This includes influence through protection and securing measures realized by the operating system.</td></tr>
<tr><td colspan="4">Functional Checks:
AV1/F1 Try to access administration account to check that access is secured.
AV1/F2 Use the administration account and check if any changes in the administration settings produce evidence of an intervention.</td></tr>
<tr><td colspan="2">-</td><td colspan="2">Check that
AV1/F3 user and group privileges, administrator account,
AV1/F4 configuration of the application control,
AV1/F5 mounted storage media as well as partitions or media with access attributes,
AV1/F6 policies for storage media and auxiliary devices correspond to the information contained in the documentation and are correctly configured.</td></tr>
</table>

IIN1: Inadmissible influence through not-LR-software

<table>
<tr><th colspan="2">Risk Class B</th><th>Risk Class C</th><th>Risk Class D</th><th>Risk Class E</th></tr>
<tr><td colspan="5">AV1 An attacker inadmissibly influences the assets and their security properties through executing functions of the not legally relevant software.
AV2 An attacker directly influences the assets and their security properties through the functionalities of the not legally relevant software.</td></tr>
<tr><td colspan="5">Specifying Notes:
AV1/N1 This implies that there are enough resources for the operation of the legally relevant application.
AV1/N2 This includes inadmissibly influences on the assets and their security properties through scheduling and runtime of the not-legally relevant software.
AV2/N1 This includes the software modules of the LR-SW-application or the LR-OS.</td></tr>
<tr><td colspan="5">Functional Checks:
AV1/F1 Perform spot checks using functions of any known not legally relevant software and check if there is no inadmissible influence on the measurement process, e.g., if a measurement can be performed the result has to be within the MPE or the critical change value.
AV1/F2 Check if any interface for exchanging not legally relevant software cannot be used to exchange legally relevant software.</td></tr>
<tr><td colspan="3">AV2/F3 Try to influence the assets with a text editor, by modifying, deleting or replacing assets.</td><td colspan="2">AV2/F3 Try to influence the assets with sophisticated software tools by modifying, deleting or replacing assets.</td></tr>
</table>

III3: Inadmissible influence through software interfaces

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1 An attacker inadmissibly influences the assets and their security properties through software interfaces.			
Specifying Notes: AV1/N1 Software interfaces include interfaces between legally relevant and not legally relevant software, interfaces between legally relevant software and the operating system and inter-process communication interfaces. AV1/N2 This includes modification of the access rules realized by the implemented securing measures for all assets. AV1/N3 This includes modification of the implemented protection measures without evidence of an intervention. AV1/N4 This includes the use of measurement data by the not-LR-SW to spoof LR-SW.			
Functional Checks: -		Functional Checks: AV1/F1 Perform spot checks on the available software interfaces of the legally relevant software, e.g., API calls, inter process communication, and check these for potential inadmissible influence on the assets and their security properties.	

IIC1: Inadmissible influence through obtaining confidential information

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1 An attacker inadmissibly influences the assets through access to confidential information.			
AV2 An attacker introduces fake confidential information into the instrument.			
Specifying Notes:			
AV1/N1 Depending on the protection means the confidential information may consist of keys, generator polynomials, initial vectors / start values, seeds, etc.			
AV1/N2 This includes the storing of cryptographic material during processing, e.g., the storage of cryptographic material in volatile memory.			
Functional Checks:			
AV1/F1 Try to retrieve the confidential information through the interfaces or by using not-LR-SW.			
AV2/F1 Try to introduce fake confidential information through, e.g., the user interfaces or by using not-LR-SW .			

IIP2: Inadmissible influence through replacing parts within the Equipment under test

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1 An attacker inadmissible influence the assets through replacing parts.			
Specifying Notes: AV1/N1 This includes parts within a complete measuring instrument or within a component.			
Functional Checks: AV1/F1 Try to replace parts within the measuring instrument or component and check if this leads to evidence of an intervention and if this is detected and acted upon if software is used to protect parts from being replaced.			

3.3.1.2 Inadmissible influence on assets through external influence on the EUT.

III2: Hardware interfaces

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1 An attacker inadmissibly influences the assets and their security properties through hardware interfaces.			
Specifying Notes: AV1/N1 Hardware interfaces include direct memory access, open interfaces and communication interfaces. AV1/N2 This includes the influence of operating system functions accessible via open interfaces. AV1/N3 This includes the possibility to boot through open interfaces. AV1/N5 This includes the influence through the connection of auxiliary devices such as exchangeable media. AV1/N6 This includes modification of the access rules realized by the implemented securing measures for all assets. AV1/N7 This includes modification of the implemented protection measures without evidence of an intervention.			
Validation Guidance: Functional Checks: AV1/F1 Perform spot checks of the functions available through hardware interfaces and check these functions for potential inadmissible influence on the assets and their security properties. AV1/F2 Carry out practical tests (spot checks) by connecting peripheral equipment and check if false measurement data can be introduced by such equipment.			

IIC3: Inadmissible influence through replacing or removing LR-components.

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1 An attacker inadmissibly influences the assets through replacing or removing complete components.			
~~AV2 An attacker inadmissible influence the assets through replacing parts.~~			
Specifying Notes:			
AV1/N1 This includes influencing the input of the EUT by replacing the LR-component.			
AV1/N2 This includes the replacement of LR-components outside the scope of the MID, i.e., the distance measurement sensor of a Taximeter.			
AV1/N3 This includes availability of measurement data to not legally relevant components, which may create a fake instance of the indication.			
AV1/N4 Typically, removing components that are directly involved in the measurement process makes it impossible to perform a measurement, this may be acceptable in the case of non-continuous measurements, in which case no further action is required. But there are peripheral devices that are mandatory and removing these components has to be detected and acted upon, these include for example printers, data storage devices for storing measurement results.			
Functional Checks:			
AV1/F1 Try to replace individual components and check if this leads to evidence of an intervention and if this is detected and acted upon if software is used to protect authenticity.			
AV1/F2 Try to remove individual LR-components and check if this is detected and acted upon.			

IIT1: Inadmissible influence through man in the middle

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1 An attacker inadmissibly influences the assets and their security properties through capture-replay attacks. AV2 An attacker inadmissibly influences the assets and their security properties by capturing the assets during transmission and modifying them.			
Specifying Notes: AV1/N1 This includes any influence not resulting from random errors, such as: AV1/N1.1 An attacker captures and deletes transmitted assets. AV1/N1.2 An attacker captures and delays or surpress the transmitted assets. AV1/N1.3 An attacker introduces fraudulent asset instances during transmission. AV4/N1.4 An attacker captures transmitted assets and modifies them and sends them to the receiver.			
Functional Checks: AV1/F1 Attempt to modify assets during transmission, check if this is detected and acted upon. AV1/F2 Attempt to interrupt or prevent transmission of the assets and check if this is detected and acted upon. AV1/F3 Attempt to introduce fraudulent assets into the transmission and check if these are detected and discarded. AV1/F4 Attempt to introduce copies of assets into the transmission and check if these are detected and discarded.			

IIR1: Inadmissible influence through random errors

Risk Class B	Risk Class C	Risk Class D	Risk Class E
AV1 The assets and their security properties are influenced by random errors.			
Specifying Notes: AV1/N1 This includes any influence not resulting from intentional manipulation, such as accidental bit flips, influence of background radiation, influence of faulty storage media, transmission disturbances, etc. AV1/N2 This includes stored and transmitted assets.			
Functional Checks: AV1/F1 Attempt to generate bit errors in the assets and check if this is detected and acted upon. AV1/F2 Interrupt transmission services and check if this is detected and acted upon.			

3.3.2 Instrument-specific attack vectors for instruments

Based on the high-level attack vectors 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 at all.

Notes for the assessors:

- *On a built-for-purpose 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 can be 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 **Error! Reference source not found.**).*

In that case, justification for the shorter selection of threats should be provided in the Risk Assessment Report (see section **Error! Reference source not found.**).

3.3.3 Attack probability tree-based attack vectors

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 two purposes:

- to model additional threats for identifying applicable attack vectors for complex instruments (see Section **Error! Reference source not found.**),
- to estimate the probability of occurrence for complex attack vectors by means of attribute propagation (see Section **Error! Reference source not found.**).

3.3.4 Attack probability tree based on instrument-specific attack vectors

Instrument-specific threats can be represented by attack probability trees (see **Figure 3-1**). These allow an examiner to split certain attacks 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.

Deleted: 3.2

Deleted: 6

Deleted: 3.3.4

Deleted: 4.2.2

Deleted: Figure 3-7

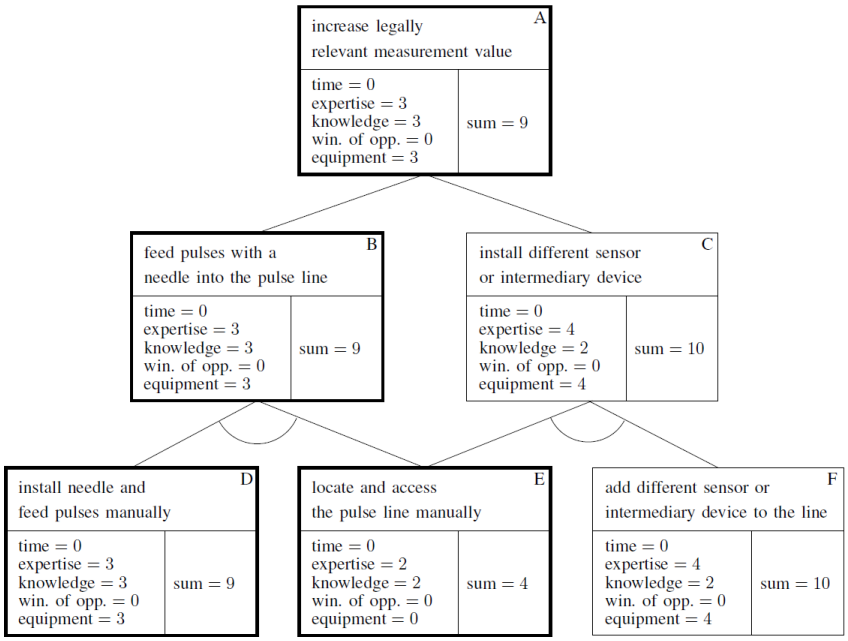

Figure 3-1: Exemplary Attack Probability Tree with assigned scores for all nodes for manipulation of a taximeters measurement value by tampering of the analog signal path. In this scenario, two known attack vectors exist: the manual feeding of additional pulses into the pulse line by means of a needle (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]

Deleted: 7

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 necessarily mean that the complete instrument is adequately protected, i.e. software on the other modules might be inadequately protected.

[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.

4.1 Risk analysis on instrument-specific attack vectors

4.1.1 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:

1. For instrument that do not use an acceptable solution listed in WELMEC Guide 7.3 instrument-specific attack vectors shall be considered.
2. For complex instruments, it might be necessary to consider additional instrument-specific attack vectors, see **Error! Reference source not found.**
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 **Error! Reference source not found.** 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).

Deleted: 3.3.4

Deleted: 3.3.1

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 Probability of occurrence

In order to estimate the probability of occurrence of an attack vector, a method called vulnerability analysis from ISO/IEC 18045 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. When inadmissible influence of random errors is evaluated (see **Error! Reference source not found.**), the method from Section 4.3 shall be used.

Deleted: 3.2.1.7

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

4.3 Probability of occurrence for random errors

For random errors, the quality of the protection mechanism, e.g., CRC-32 or SHA-256, may be expressed by means of their bit error detection probability or the likelihood of such errors not being detected.

Protection mechanism for random errors shall be assigned an error probability score based on the following categories:

Detection Capability	Description	Probability score
Very high	error detection probability that is higher than the detection capability of "high"	**1**
High	error detection probability between $1 - p^2 \cdot 0.23 \cdot 10^{-60}$ and $1 -$	**2**

	$p^2 \cdot 0.23 \cdot 10^{-65}$for input bitstreams of length p, i.e., corresponding to the properties of SHA-256	
Middle	error detection probability greater than 99.9999% regardless of the message length, i.e., corresponding to the properties of CRC-32	**3**
Low	error detection probability greater than 99.9984% regardless of the message length, i.e., corresponding to the properties of CRC-16	**4**
Very low	error detection probability that is lower than the detection capability of "low"	**5**

Each individual random error attack vector must have an assigned impact score, which can be either 1 for random errors affecting all future (or past) measurements, or ⅓, for random errors only affecting individual measurement events. Afterwards, the risk associated with each random error is calculated by multiplying impact and probability score.

5 Evaluation of Solutions

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

5.1 Risk class C and lower

For instruments in risk class C , a risk score of three is generally acceptable. If the calculated risk score is higher than three, the assessor should request the manufacturer to implement additional protective measures and to repeat the assessment. The following table gives a proposal for a mapping between calculated risk score and risk class.

Risk class	Risk score
B	≤ 4
C	≤ 3
D	≤ 2
E	1

5.2 Risk class D and higher

The following procedure may be applied in order to account for the purpose of the measuring instrument type.

5.2.1 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".

5.2.2 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.

5.2.3 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.

5.2.4 Taking into account the attacker's motivation

The point scores from 5.2.1 to 5.2.3 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 5.2.1 to 5.2.3 yields 6, the point scores for "expertise" and "equipment" should not be chosen lower than 6.

6 Validation Guidance for Risk Assessments

This chapter is intended to provide guidance on how to evaluate a risk assessment for a combination of attack vector and asset instance.submitted for software examination.

6.1 Inclusion of instrument-specific attack vectors

Based on the submitted risk assessment, the evaluator shall decide if the manufacturer has investigated instrument-specific attack vectors and if he has provided proper justification for neglecting such an investigation.

The list of instrument-specific threats shall be checked for completeness: Has a threat been formulated for each asset instance and each security property?

6.2 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 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 if valid assumptions have been made for the three subscores AB, ARS and ARC, see tables in 5.2.1, 5.2.2 and 5.2.3.

The manufacturer's choice with respect to AB, ARS and ARC shall be checked with the help of the Die Auswahl des Herstellers für AB, ARS und ARC ist mittels der Tabellen auf Plausibilität zu prüfen. Sollten die ausgewählten Punktescores zu hoch erscheinen, so ist beim Hersteller eine Begründung zu erfragen. Grundsätzlich gibt es keinen falschen Motivationsscore, wichtig ist, dass die Entscheidung und ggf. Begründung dokumentiert ist.

Afterwards, the examiner shall check that the attacker motivation scores has been correctly calculated by adding the three subscores:

attacker motivation score = AB + ARS + ARC

6.3 Instrument-specific attack vectors

For each instrument-specific attack vector the following validation steps shall be performed:

- For risk class D and higher, the examiner shall check the manufacturer's justification for not includin
- Together with the examiner for the metrological characteristics, the software examiner shall check if the choice of the attack vectors is pausible or if there exist simple alternatives.

6.4 Instrument-specific attack vectors

The following validation steps shall be performed for each instrument specific attack vector and each high-level attack vector derived from the MID

- Check if the manufacturer has examined and evaluated all applicable attack vectors from **Error! Reference source not found.** for each threat.
- Check if the assigned point scores (see tables in the Annex) match the individually given justification and the technical specification of the instrument.
- If the manufacturer has chosen to accomodate an attacker motivation score (see 6.2), the examiner shall check if the motivation score has been used correctly as a lower bound for expertise and equipement in the evaluation of all attack vectors.
- The examiner shall check if the sum score of the point scores has been calculated correctly and if the choice of the impact factor is plausible. If only a single measurement is affected by an attack, the impact score must be ⅓, otherwse it shall be 1.
- The examiner shall check if the sum score has been correctly turned into a probability score in accordance with table 7-6 from the Annex.
- Finally, the examiner shall check if probability score and impact score have been correctly multiplied to calculate the risk score.

If the risk score is within the limit defined in section 5.1 the attack vector is considered to be sufficiently mitigated. Otherwise, the manufacturer shall amend the design.

6.5 Source Code Checks

For measuring instruments in risk class E, the examiner shall check that the countermeasures to individual attack

Deleted: 3.3.1

Deleted: 6.3

vectors have been correctly implemented in the source code.

Annex I: Relationship with other WG7 Guides

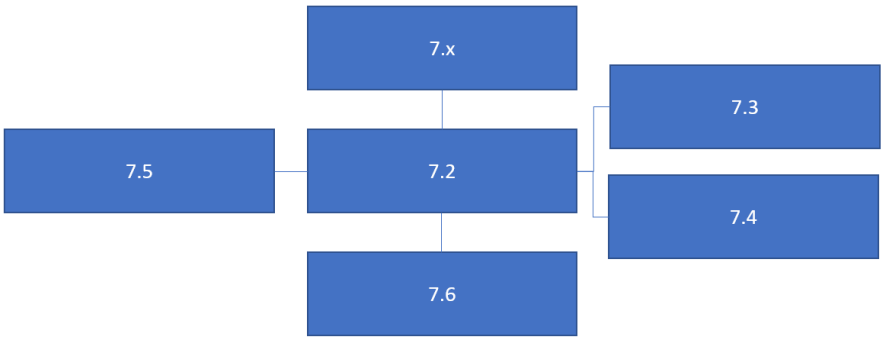

Figure 2: Relationship with other WG7 Guides

Deleted: 3

WELMEC WG7 has issued a number of Guides that are related to each other. These Guides should not be read without taking into consideration all relevant aspects in all the Guides related to software.

- WELMEC Guide 7.1 contains information on where the Risk-based Requirements are derived from and how they are implemented in Guide 7.2.
- WELMEC Guide 7.2 contains the actual Risk-based Requirements, specifying notes, required documentation and validation guidance.
- WELMEC Guide 7.3 contains acceptable solutions and the conditions under which certain acceptable solutions can be used to fulfil the requirements of Guide 7.2, with the required documentation and validation guidance to check if the implementation of the acceptable solution complies with the conditions.
- WELMEC Guide 7.4 contains guidance to the evaluation and application of the requirements of 7.2 for complex measuring instruments, e.g., web-based applications, measuring instrument built out of separate components.
- WELMEC Guide 7.5 contains a cross-reference between the EN45501 and Guide 7.2. Guide 7.5 can be used to convert NAWI software evaluations into AWI evaluations, and vice-versa if a manufacturer wants to use the harmonized standard for his NAWI.
- WELMEC Guide 7.6 contains the guidance on how to perform a Risk Assessment to evaluate if a proposed solution of the manufacturer is adequate to either protect the asset or prevent inadmissible influence on the assets.

Annex II Tables and Examples

Table 0-1 to Table 0-5 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.

Deleted: Table 7-1

Deleted: Table 7-5

Formatted: Font: 10 pt

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 0-1: 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 0-2: 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 0-3: 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 0-4: 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 0-5: 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 0-6: Mapping of point scores to probability score

A selection of exemplary fully evaluated attack vectors is given in Table 0-7.

Deleted: 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 0-7: Exemplary evaluated attack vectors

Annex III Check list

To be provided.

Annex IV Report Format

Commented [ME1]: Will be replaced by a new Excel-Template for all software guides.

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 high-level attack vectors

Here, the filled-in checklist from Annex III 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 **Error! Reference source not found.**) the following Tables shall be completed.

Deleted: 3.3.4

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 Description	Time	Expertise	Knowledge	Window of opportunity	Equipment	Total	Impact	Justification
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	Probability 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 2.2.

Deleted: 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.

5) Checklist Acceptable Solutions

Annex V 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 0-1**.

Deleted: Figure 7-1

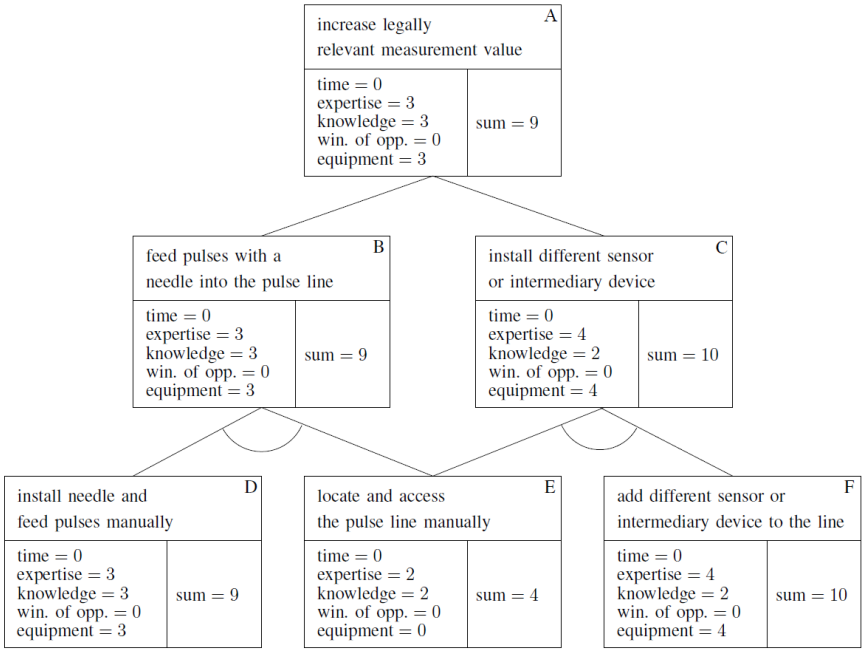

Figure 0-1: Exemplary attack probability tree for a taximeter connected to a pulse generator at a car's wheel by means of a pulse line

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 0-1** illustrates attacks on the analog signal path between pulse generator at a car's wheel and taximeter.

Deleted: Figure 7-1

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 0-1) and
- the installation of a different pulse generator or other intermediary device into the signal path (node (C) in Figure 0-1).

Deleted: Figure 7-1

Deleted: 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.

Annex VI: Revision History

No.	Date	Significant Changes
1	June 2025	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.