UKWF Technical Webinar – Thursday 18 July 2022

WELMEC Working Group 7 – Software approvals and risk assessments

Hosted by Ian Turner

Introduction

- As a European Working Group – WELMEC's mission is to develop and maintain confidence in legal metrology in Europe
- WELMEC covers all aspects of software
- UKWF sit on the group and play an active role
- The group works closely with CECIP to provide support and gather industry views
- The group is driving a number of key projects – although each one can take time to resource and deliver

WG7 Guides

- Guide 7.2 - Software Guide (Measuring Instruments) (Version 2021)
- Guide 7.3 - Reference Architectures based on WELMEC Guide 7.2 (Version 2020)
- Guide 7.4 - Exemplary Applications of WELMEC Guide 7.2 2020 (Version 2020)
- Guide 7.5 - Software in NAWI's (Non-automatic Weighing Instruments Directive 2014/31) (Version 2020)
- Guide 7.6 - Software risk assessment for Measuring Instruments 2021 (Version 2021)

WG7 Guides – Guide 7.2

- The Guide 7.2 is the ‘base guide’ and all of the others exist to help understand this one
- Quite old and has developed in a piecemeal fashion
- Can appear complicated but when the structure and the meanings are understood, it works well
- Aimed primarily at the type examination stage but is used by market surveillance officers
- Re –issued regularly to make sure it is kept up to date

WG7 Guides

- Historically NAWI's were covered by the Guide 2.3
- This has been revoked and now the Guide 7.2 is the default guide – this will be clarified more clearly in future editions
- A new extension has been approved - extension O-General purpose operating systems
- Software is described as a *general-purpose operating system* if system resources of a measuring instrument (CPU, memory, interfaces) are administrated by that software and are made available to the legally relevant application. In addition, the operating system has a multi-user capacity and an administration mode (multi-user operating system)

Recent changes in the Guide 7.2

- The extension O has been approved by WG7 and the revised Guide will be published shortly
- It has been decided to review the Guide to ensure it is for for the future
- Will be a number of working groups that will be operating
- Sub-group on “New Technologies” – this is a group which discusses the opportunities for the future
- Horizon Scanning
- Two sub-groups on the review of the Guide 7.2
- Evolution of WELMEC Software Guides
- Recast of the Guide 7.2

Guide 7.3

- Reference architectures based on the Guide 7.2

- The aim of the Guide is to provide an architectural template for mapping measuring instrument
- Designs based on new technological developments to the requirements of WELMEC Guide 7.2.
- Outlines a set of reference architectures that are in the market
- Lists the boundary conditions for the architecture
- Lists specific attack vectors that would need to be considered when undertaking the risk assessments
- Specific about the extensions that will apply to each architecture
- Well thought out and put together document

Guide 7.4

- Exemplary applications of WELMEC Guide 7.2

- The Guide provides specific technical solutions for selected general architectures of instruments
- Indicates how these acceptable solutions fulfil the requirements laid down in WELMEC Guide 7.2.
- In doing so, it also illustrates the requirements laid down in WELMEC Guide 7.2 on a technical level
- Should be seen as the sister Guide for 7.3

Guide 7.5 - Software in NAWIs

- This document is intended to provide guidance on the software requirements in accordance with the Non-automatic Weighing Instruments Directive (NAWID) 2014/31/EU
- It is a cross reference table between the Guide 7.2 (2019) and the EN45501 (2015)
- Useful as a gap analysis between the two as NAWIs are effectively subject to the requirements of the Guide 7.2
- Will need to be updated for the new extension O and any changes to the review of the Guide 7.2

Guide 7.6

- Software risk assessments for Measuring Instruments

- Outlines how notified bodies shall assess the risks relating to the essential requirements and software
- Describes a method of making that assessment
- Targeted at manufacturers to help them undertake an adequate risk assessment
- Includes and element of understanding the attackers motivation
- Fundamental to a proper understanding of risk with software
- Must always fight against the notion of more and more regulation for perceived rather than actual risk
- Complicated document but does lead to transparency

Guide 7.6

- Software risk assessments for Measuring Instruments

- MID and NAWID require to submit "*…an adequate analysis and assessment of the risk(s).*" for Modules B, D1, F1, G (NAWID) or Modules A, A2, B, D1, E1, F1, G, H, H1 (MID)
- No particular format or procedure required
- A harmonized procedure according to Guide 7.6 allows for comparable extents and results
- Guide 7.6 is NOT mandatory!

Guide 7.6

- Software risk assessments for Measuring Instruments

Structure of Guide 7.6

- Follows the idea of ISO/IEC27005:

*"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"*

- Sections:
  - 1 Terminology
  - 2 Workflow of Risk Assessment
  - 3 Risk Identification
  - 4 Risk Analysis: Analysis of Attack Vectors
  - 5 Risk Evaluation
  - 6 Risk Assessment Report
  - 7 References

Guide 7.6

- Software risk assessments for Measuring Instruments

Section 2: Workflow of Risk Assessment

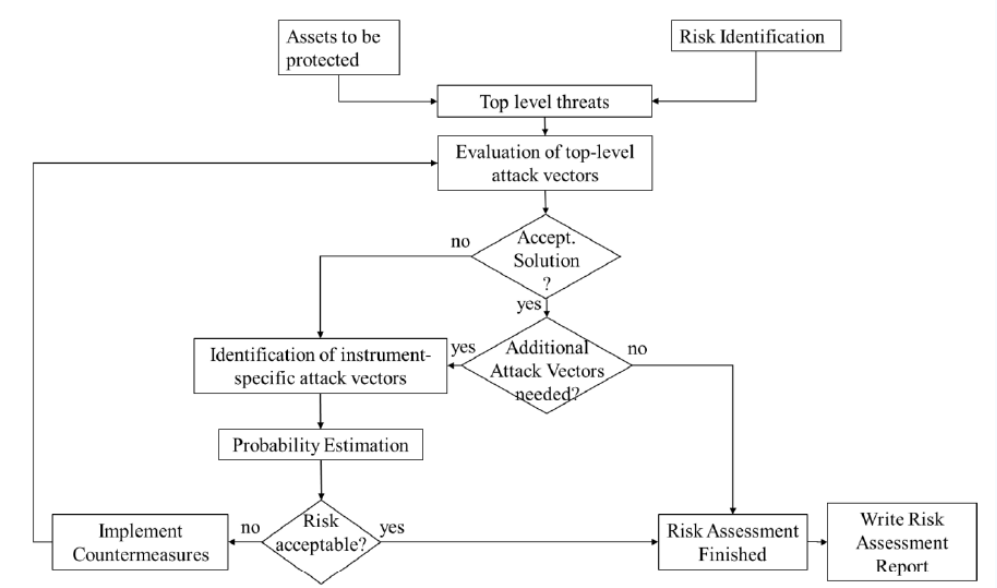


Figure 2-1: Workflow of the risk assessment procedure.

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

Guide 7.6

- Software risk assessments for Measuring Instruments

Section 3: Risk Identification

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

Nr.	Asset	Security properties	Requirement (Annex I, MID [1])*
1	legally relevant software	• availability • integrity • authenticity	• 7.1 • 7.2 • 7.6 • 8.3 • 8.4
	identification of the legally relevant software	• availability • integrity • authenticity	• 7.6 • 8.3
	evidence of an intervention of the legally relevant software	• availability • integrity • authenticity	• 8.2 • 8.3
	Adequate protection of the legally relevant software	• availability	• 8.1
2	legally relevant parameters	• availability • integrity • authenticity	• 7.1 • 8.4
	Adequate protection of the legally relevant parameters	• availability • integrity • authenticity	• 8.2 • 8.3
	Evidence of an intervention[1] of the legally relevant parameters	• availability • integrity • authenticity	• 8.1
3	measurement result, including the measurement result relevant data	• availability • integrity	• 7.1 • 8.4
	Adequate protection	• availability • integrity • authenticity	• 8.1
4	record of a measurement result	• availability • integrity	• 11.1 • 11.2
	Adequate protection	• availability • integrity • authenticity	• 8.2 • 8.3
	Evidence of an intervention[1]	• availability • Integrity • authenticity	• 8.1
5	indicating the measurement result: • markings • Indication of the measurement result: clear and unambiguous	• availability • integrity • authenticity	• 7.1 • 9 • 10.2 • 7.1 • 10.1 • 10.2 • 10.4
	Adequate protection	• availability • integrity • authenticity	• 8.1

Main assets derived from Essential Requirements in MID/NAWID

Guide 7.6

- Software risk assessments for Measuring Instruments

Section 3: Risk Identification (section 3.4.1 gives a graphical representation of high-level attacks on the main assets)

3.4.1.1 Attacks on legally relevant software

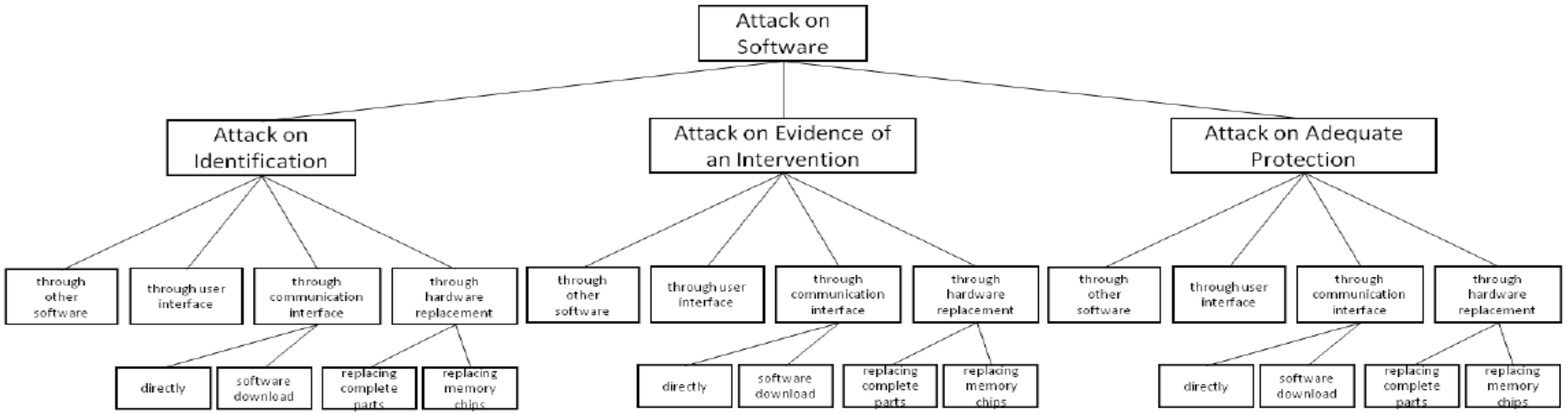
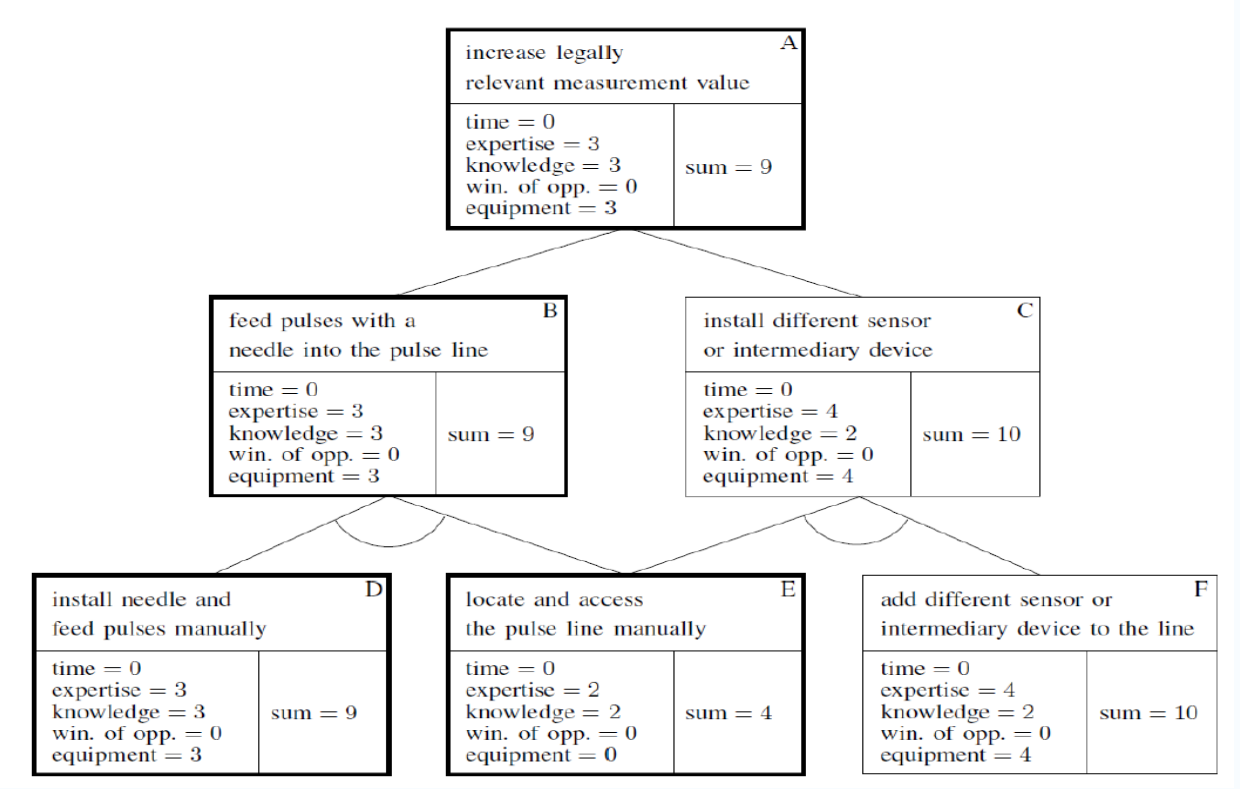


Figure 3-2: Generic AtPT for threats pertaining to the manipulation of software and its derived assets.

Guide 7.6

- Software risk assessments for Measuring Instruments

Section 3: Risk Identification (section 3.4.1 gives an example of an instrument specific attack vector and to how to calculate the risk score)



Guide 7.6

- Software risk assessments for Measuring Instruments

Section 4: Risk Analysis-Analysis of attack vectors

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

Guide 7.6

- Software risk assessments for Measuring Instruments

Section 5: Criteria to be assessed

- Time, Expertise, Knowledge, Window of Opportunity, Equipment
- Additional: Assessment of the impact - impact score is 1 for attacks executed once affecting all future (or past) measurements, or 1/3 for attacks needing to be repeated for each individual measurement event
- ANNEX B gives a clear description how to assess the criteria

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.

Guide 7.6

- Software risk assessments for Measuring Instruments

Section 5: Risk Evaluation

For risk class C and lower: risk score <4 acceptable.
No score needed in case of countermeasures for all attack vectors.
For risk class D and higher: tbd by assessor

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

- 5.1.1: Attacker’s Benefit
- 5.1.2: Attacker’s risk of being suspected
- 5.1.3: Attacker’s Risk, when getting caught

Guide 7.6

- Software risk assessments for Measuring Instruments

Section 5: Risk Evaluation

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

- 5.1.1: Attacker's Benefit
- 5.1.2: Attacker's risk of being suspected
- 5.1.3: Attacker's Risk, when getting caught

- This takes into account that if something is possible, it does not necessarily mean that somebody would try to do it…

Guide 7.6

- Software risk assessments for Measuring Instruments

- Annexes
- Annex A: Checklist (Excel file)
- Annex B: Tables (e.g. point scores) and Examples
- Annex C: Report Format
- Annex D: Assessment of Attack Probability Trees

Guide 7.6

- Software risk assessments for Measuring Instruments

Harmonization:

- CECIP presented an “Artificial cloud-based weighing device” for risk assessment comparison (by different NBs)
- Results were “interesting”
- Another workshop (comparison?) planned by PTB

Any questions?