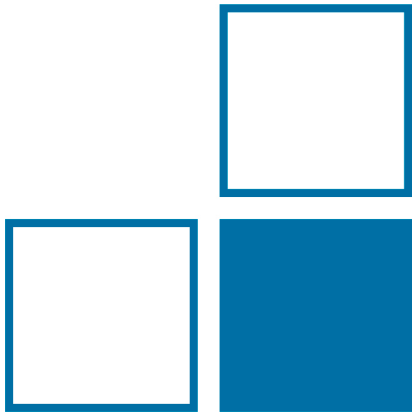
Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Nationales Metrologieinstitut

Risk Assessment for Software

in Legal Metrology

Dr.-Ing. Marko Esche, WG8.51



Overview

- Introduction and Motivation
- Formal Derivation of Security Requirements
- Algorithmic Description of the Risk Assessment Procedure
- Examples
- Graphical Representation using Attack Probability Trees
- Extension for Attacker Motivation
- Conclusion

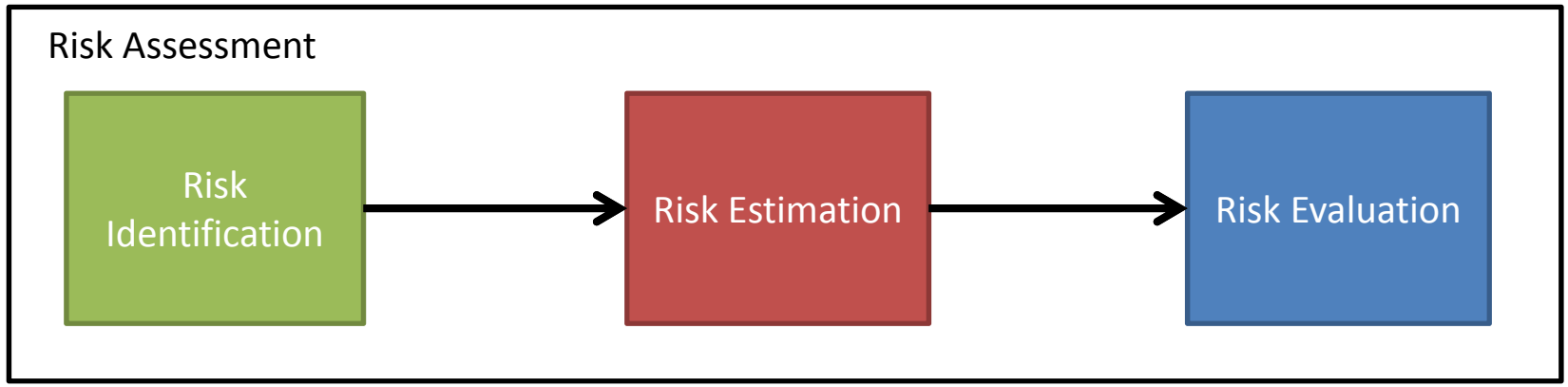
Motivation

- **Generic approach to assess the resistance** of measuring devices and measurement data to manipulations.
- MID (Directive 2014/32/EU) requires an **“analysis and assessment of the risks”** to be part of the documentation submitted for conformity assessment.
- Goal of this presentation: to propose a **framework for risk assessment** which could be used by manufacturers and Notified Bodies.
- The approach uses the structure of ISO/IEC 27005 for the analysis.
- Methods from ISO/IEC 15408 (Common Criteria) and 18045 (Common Evaluation Methodology) will be employed to **provide reproducible numerical risk scores**.

The term “risk” in the context of the MID

- ISO/IEC 27005: **“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.”**
- ISO/IEC 27005: Risk evaluation criteria
  - “legal and regulatory requirements, and contractual obligations”
- Impact in the context of the MID:
  - severity of a breach of the essential requirements.
  - Physical injuries, loss of life etc. are beyond the aims of protection of the MID.

Procedure according to ISO/IEC 27005



- Components needed to calculate risk:
  - list of unwanted events **(threats to assets)**
  - consequences resulting from such events **(impact/hazard/consequence)**
  - Probability of occurrence **(probability/likelihood)**

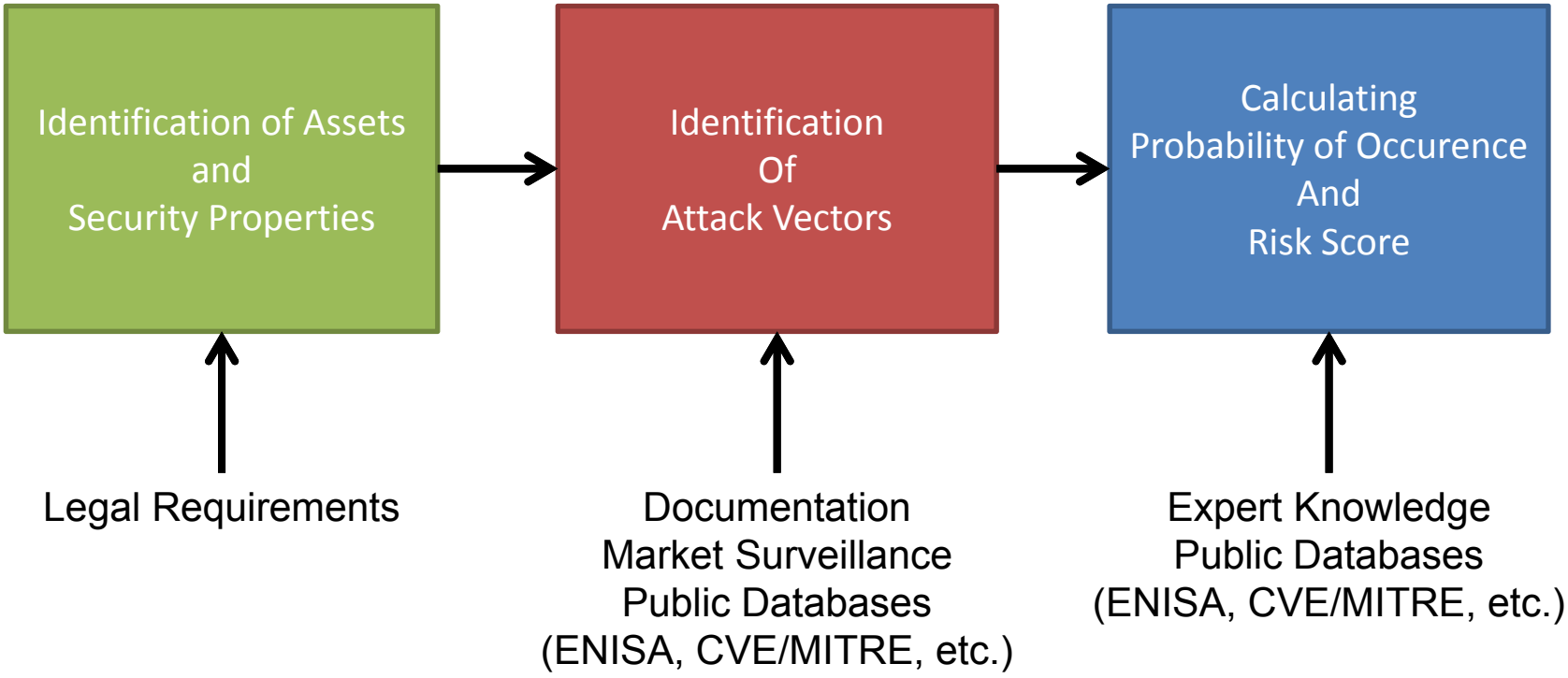
Software requirements in the MID (ex.)

- **Annex I, 8.3: Software (A1)** that is critical for metrological characteristics shall be **identified (A9)** as such and shall be secured. Software identification shall be easily provided by the measuring instrument. **Evidence of an intervention (A2)** shall be available for a reasonable period of time.
- **Annex I, 8.4: Measurement data (A3)**, **software (A1)** that is critical for measurement characteristics and **metrologically important parameters (A4)** stored or transmitted shall be adequately protected against accidental or intentional corruption.

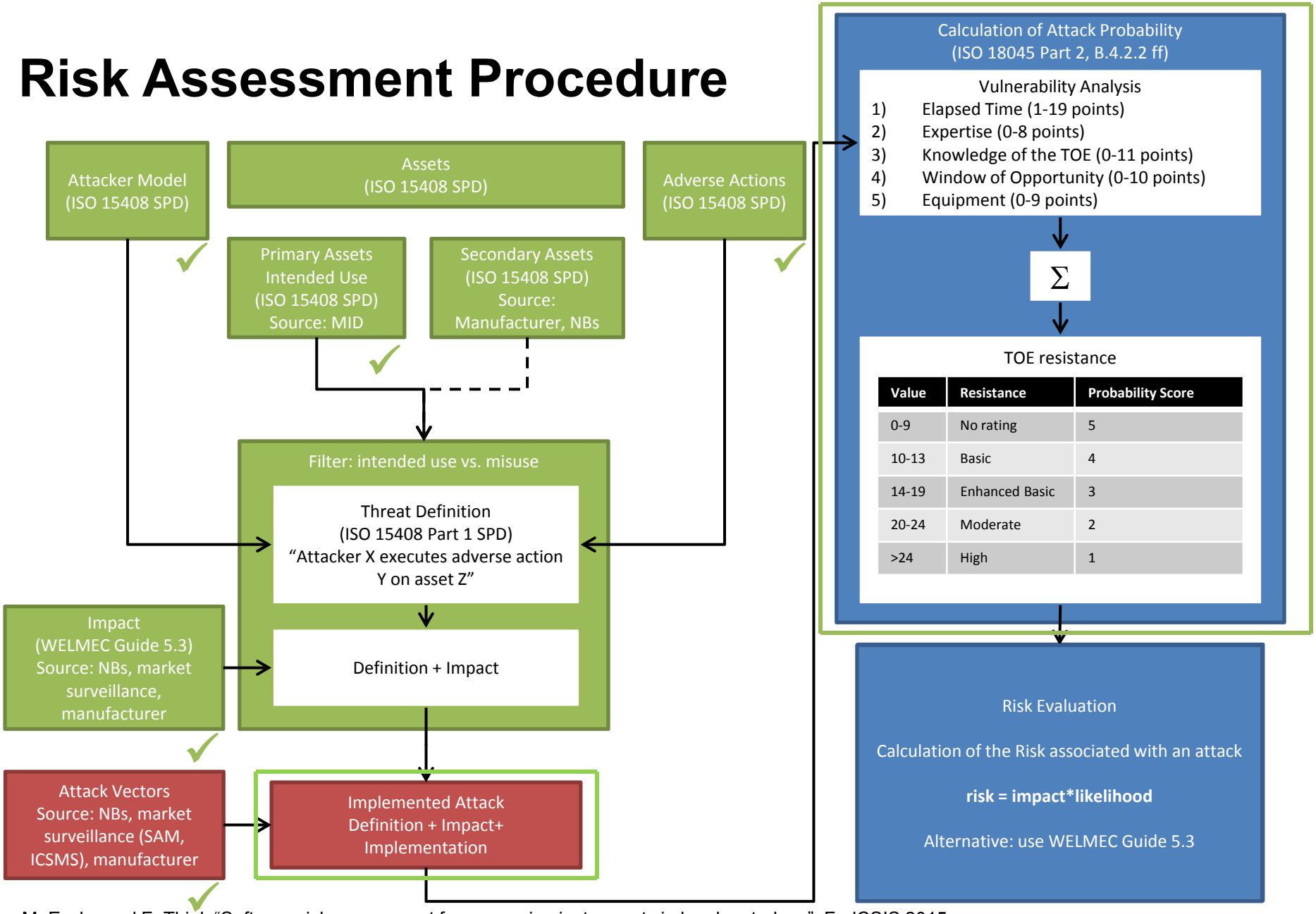
Software requirements in the MID

Primary Assets derived from the MID		
Number	Asset	Security Property
A1	metrological software	integrity, authenticity
A2	evidence of an intervention	availability, integrity
A3	measurement data	integrity
A4	metrological parameters	integrity
A5	inadmissible influence on the software	unavailability
A6	indication of the result	availability, integrity

Risk Assessment Procedure (ISO/IEC 27005)



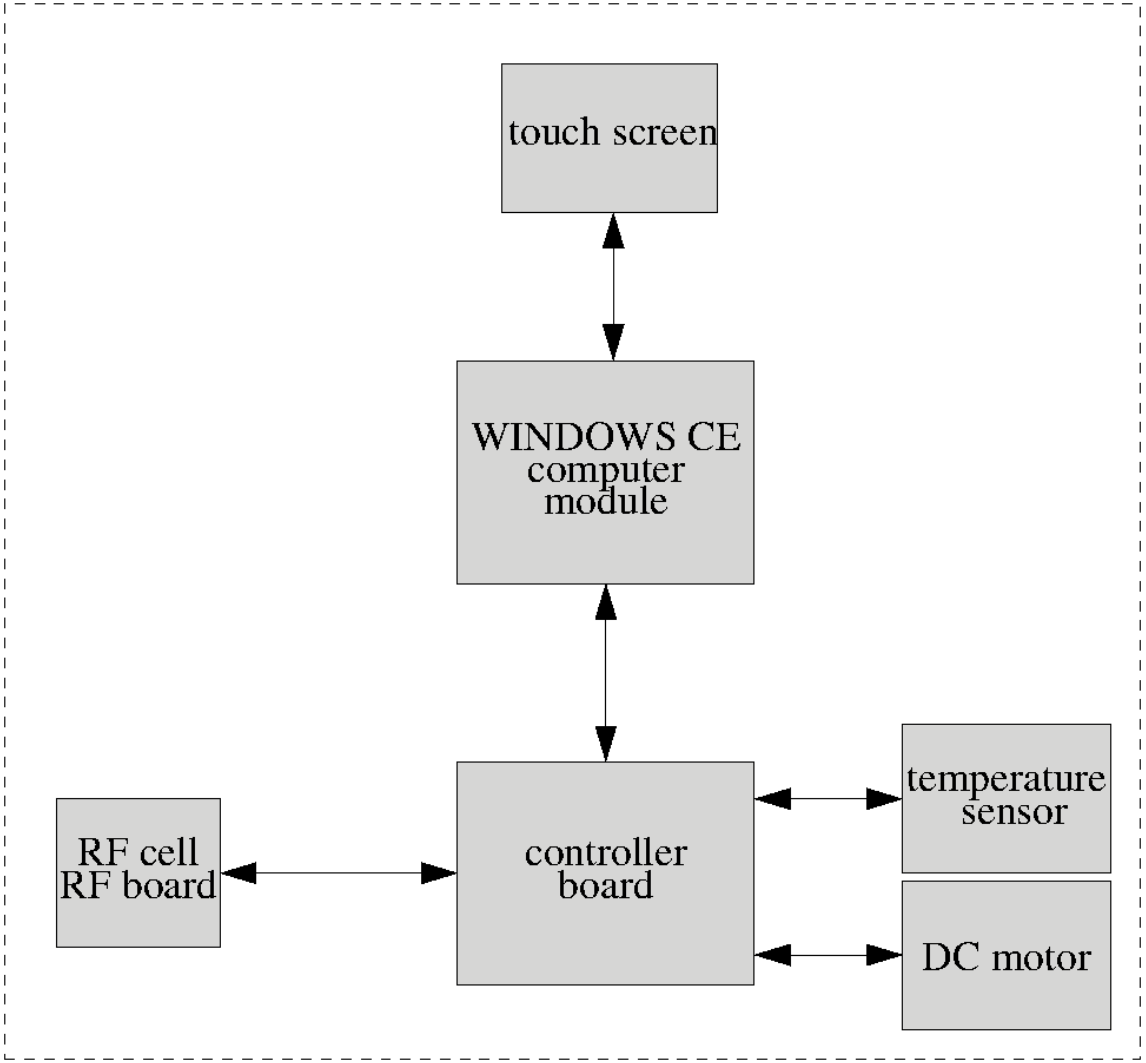
Risk Assessment Procedure



M. Esche and F. Thiel, "Software risk assessment for measuring instruments in legal metrology", FedCSIS 2015

Example No. 1: Grain Moisture Analyzer

- Initialization of measurement via serial port
- Setting of certain parameters via serial port
- Retrieval of results via serial port or USB
- Operating system protected by a 6-digit password
- All logbooks are stored on the same memory drive



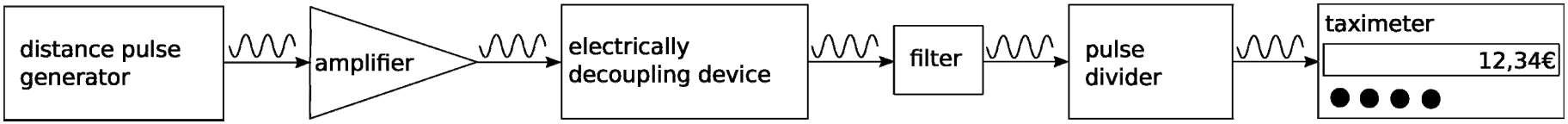
Example No. 1: Attack Vectors

- **A_PASSWORD:** An attacker retrieves the admin password by trying all 6-digit combinations.
- **A_SW_REPLACE:** An attacker retrieves the admin password and replaces the legally relevant software.
- **A_INT_SERIAL:** An attacker exploits a vulnerability of the proprietary serial protocol and causes the instrument to malfunction.
- **A_INT_SERIAL_VALUE:** An attacker exploits a vulnerability of the proprietary serial protocol and manipulates a measurement value.
- **A_INT_USB:** An attacker manages to install malicious code by disabling the USB-port‘s protection.

Example No. 1: Risk Score

Threat	Description	Impact	Attack Vector	Elapsed Time	Expertise	Knowledge of the TOE	Window of Opportunity	Equipment	Sum	Score	**Risk**
T1	Local admin (S2) invalidates integrity or authenticity of the metrological software (A1).	1	A_SW_ REPLACE	(>180d) **19**	(expert) **6**	(restricted) **3**	(unlimited) **0**	(standard) **0**	28	1	**1**

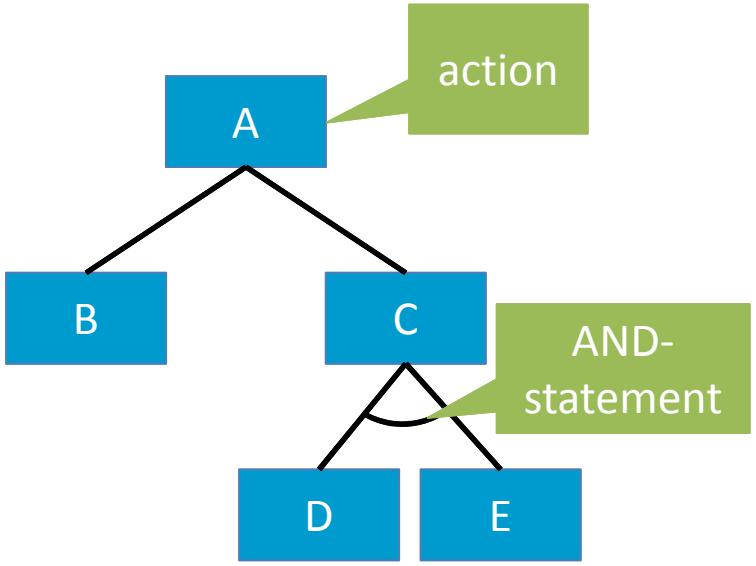
Example No. 2: Taximeter



- Purely analog signal path
- **Threat: An attacker increases the measurement result.**
- Possible attack vectors:
  - Feed pulses manually with a needle into the pulse line
  - Install different sensor or intermediary device
- Possible countermeasures:
  - armored cable
  - plausibility checks
  - second sensor

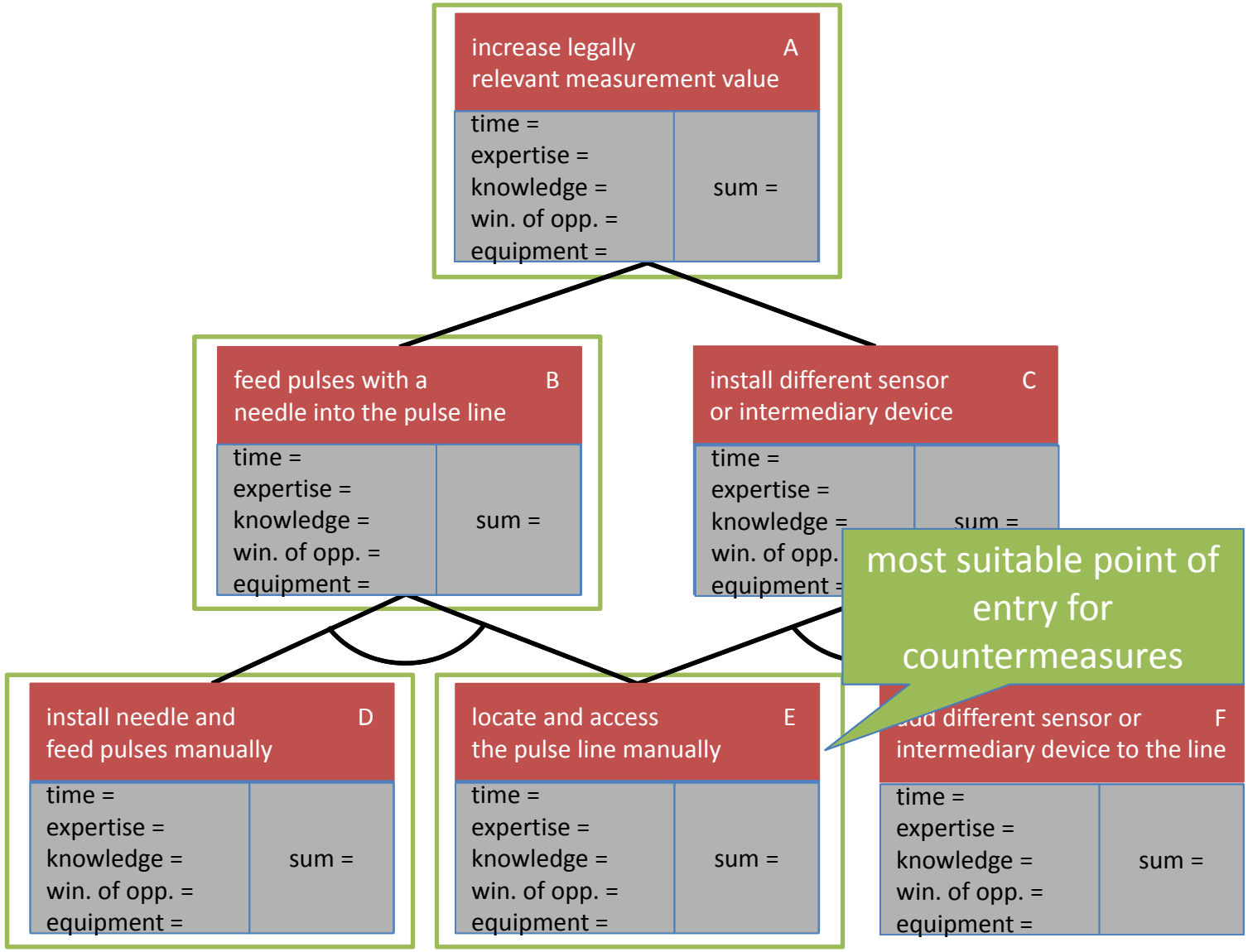
Attack Probability Trees (AtPT)

- Graphical way to express the whole risk assessment procedure. Has already been used for WELMEC WG12.
- Nodes in a tree represent actions or goals.
- Child nodes correspond to intermediate or sub-goals.
- Nodes may be linked by OR- and by AND-statements.



M. Esche and F. Grasso Toro, “Representation of Attacker Motivation in Software Risk Assessment Using Attack Probability Trees”, FedCSIS 2017 to be published

Example No. 2: Initialization of an AtPT



Extension for Attacker Motivation

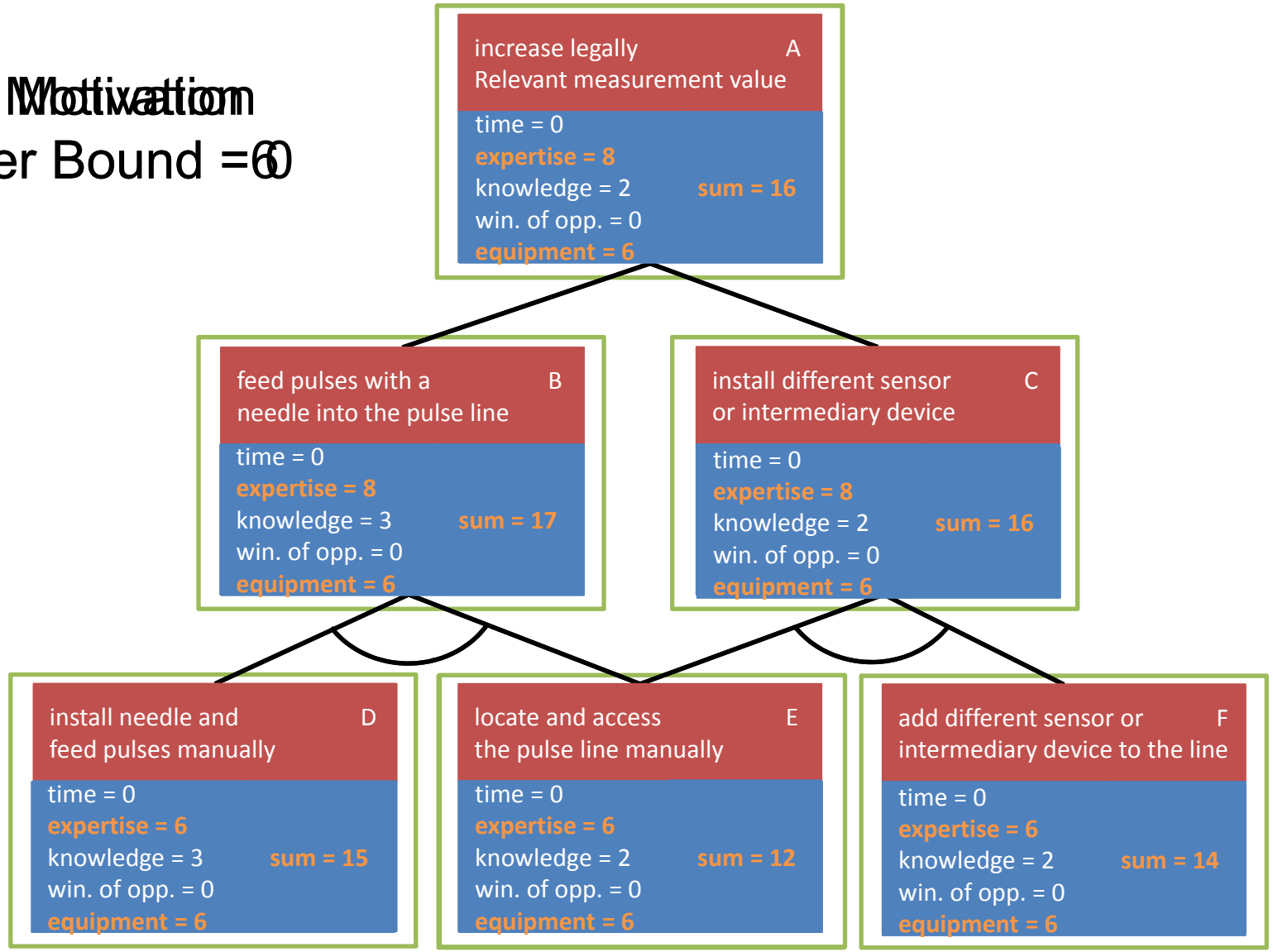
- **Problem:** Attacker motivation should have an impact on the likelihood of an attack.
- ISO/IEC 18045: Attacker motivation will have an influence on used resources (equipment and expertise).
- **Solution:**
  - A new motivation score is introduced.
  - This score acts as a lower bound for equipment and expertise as both may be acquired if monetary funds are available.
  - Original risk is considered to be a theoretical upper limit.

Motivation	Score
No motivation	9
Low	6
Moderate	3
High	0

M. Esche and F. Thiel, “Incorporating a measure for attacker motivation into software risk assessment for measuring instruments in legal metrology,” GMA/ITG-Fachtagung Sensoren und Messsysteme 2016

Ex. No. 2: Influence of attacker motivation

High Motivation
Lower Bound = 0

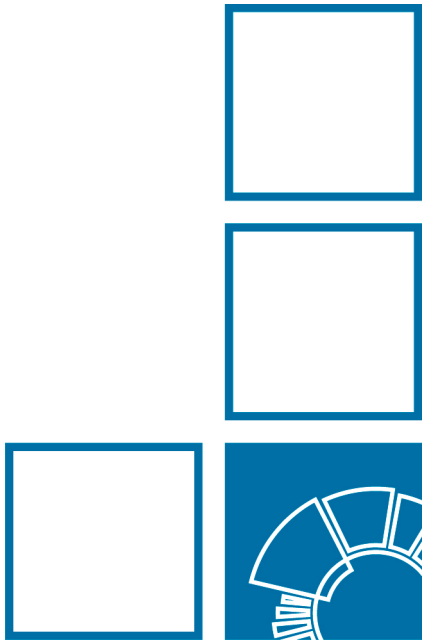


PTB Offer

- WELMEC WG7 has identified the approach as a suitable way for fulfilling requirements of the MID.
- WELMEC has included this approach in its official library: http://www.welmec.org/fileadmin/user_files/publications/Library/Software_Risk_Assessment_for_Measuring_Instruments_in_Legal_Metrology.pdf
- PTB invites manufacturers' associations to document typical (abstract) measuring instruments and submit them for risk assessment.
- Such instruments could be circulated among Notified Bodies in Europe for key comparison.
- The results will provide further insights on the reproducibility of the approach.

Conclusion

- By including the CC vulnerability analysis, a **well-recognized and established evaluation scheme** is used.
- High risks should be addressed by technical means or by informing the user accordingly.
- In contrast to many other approaches, an **easily reproducible score** is defined. This will be tested in a key comparison.
- Attacker motivation can have a significant impact on the risk.
- **Attack Probability Trees** may be used to **graphically represent attacks** and to identify promising countermeasures.
- A guidance document for manufacturers is available here: http://www.ptb.de/cms/fileadmin/internet/fachabteilungen/abteilung_8/8.5_metrologische_informationstechnik/8.51/PTB-8.51-MB04-RiskAnalyse-EN-V08.pdf



Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin
Abbestr. 2-12
10587 Berlin

Dr.-Ing. Marko Esche
Telefon: 030-3481-7975
E-Mail: marko.esche@ptb.de
www.ptb.de

Version: 06/17