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

WELMEC-Leitfaden 7.6

Software-Risikobewertung

für Messgeräte

Version 2021

Zur Information:

Dieser Leitfaden wird der Arbeitsgruppe Messinstrumente zur Berücksichtigung für zukünftige Referenzierung auf der Europa-Webseite zur Verfügung gestellt.

Der WELMEC e.V. ist eine Kooperation zwischen den Behörden des gesetzlichen Messwesens der Mitgliedstaaten der Europäischen Union und der EFTA. Das vorliegende Dokument ist einer von zahlreichen Leitfäden, die der WELMEC e.V. als Anleitung für Messgerätehersteller und Benannte Stellen, die für die Konformitätsüberprüfung ihrer Produkte verantwortlich sind, herausgegeben hat. Die Leitfäden haben rein empfehlenden Charakter und führen ihrerseits keinerlei Beschränkungen oder zusätzliche technische Anforderungen ein, die über die in den entsprechenden EG-Richtlinien enthaltenen Festlegungen hinausgehen. Alternative Ansätze sind akzeptabel, jedoch repräsentiert die in diesem Dokument bereitgestellte Anleitung die aus Sicht des WELMEC e.V. beste Vorgehensweise, die verfolgt werden kann.

Herausgeber:
WELMEC Sekretariat

E-Mail: secretary@welmec.org

Website: https://www.welmec.org

Software-Risikobewertung für Messgeräte

Inhalt

Vorwort

Dieser Leitfaden dient der Software- und IT-Risikobewertung von Messgeräten im Rahmen der Messgeräterichtlinie (Measuring Instruments Directive, MID) [1] und der Richtlinie für nichtselbsttätige Waagen (Non-Automatic Weighing Instruments Directive, NAWID) [2].

Dieser Leitfaden hat rein empfehlenden Charakter und führt seinerseits keinerlei Beschränkungen oder zusätzliche technische Anforderungen ein, die über die in der MID [1] oder der NAWID [2] enthaltenen Festlegungen hinausgehen.

Alternative Ansätze sind akzeptabel, jedoch repräsentiert die in diesem Dokument bereitgestellte Anleitung die aus Sicht des WELMEC e.V. beste Vorgehensweise, die genutzt werden kann.

Andere WELMEC-Arbeitsgruppen verlangen möglicherweise zusätzliche formelle oder technische Voraussetzungen für die Risikobewertung.

Obwohl sich dieser Leitfaden auf Messgeräte im Geltungsbereich der MID- und NAWID-Richtlinien bezieht, ist die Methode allgemeiner Natur und lässt sich darüber hinaus anwenden.

Einleitung

Im Rahmen einer Konformitätsbewertung nach MID [1] oder NAWID [2] ist vom Hersteller eine Risikobewertung durchzuführen und zu dokumentieren, um die Konformität des Messgeräts mit den wesentlichen Anforderungen aus MID [1] Anhang II, Modul B 3c bzw. NAWID [2] Anhang II, Modul B 1.3c nachzuweisen.

Die Analyse der eingereichten Risikobewertung hinsichtlich der angemessenen Erfüllung der wesentlichen Anforderungen obliegt der Benannten Stelle.

Dieses Dokument beschreibt eine Methode zur Feststellung der softwarebezogenen Risiken für Messgeräte, die den Regelungen von MID [1] und NAWID [2] unterliegen. Der vorliegende Leitfaden geht nicht auf andere Risiken ein, wie bspw. elektromagnetische Kompatibilität, Gesundheitsrisiken oder das Risiko eines elektrischen Schocks. Immer, wenn auf MID [1] oder WELMEC-Leitfaden 7.2 [3] Bezug genommen wird, trifft dies auch auf NAWID [2] und WELMEC-Leitfaden 7.5 [4] zu, die gleichwertige oder ähnliche Anforderungen stellen. In jedem Fall bietet der vorliegende Leitfaden eine Methode zur Bewertung gerätespezifischer Risiken, insbesondere für neue Technologien, die noch nicht von etablierten akzeptablen Lösungen behandelt wurden.

Die Methode richtet sich zum einen an Hersteller solcher Geräte als Hilfestellung bei der Erstellung eines angemessenen Berichts zur Risikobewertung, zum anderen an Benannte Stellen, insbesondere an jene unter Modul B, G und H1 der MID [1] und der NAWID [2], um ihnen als Unterstützung bei der Analyse eines eingereichten Berichts zu dienen, zum Beispiel bei den Fragen, ob der Bericht alle Bedrohungen gegen schützenswerte Güter abdeckt und ob die vorgeschlagenen Maßnahmen zur Minderung der Bedrohung akzeptabel sind.

Es wird dringend empfohlen, dass die Risikobewertung von einer Gruppe von Menschen mit unterschiedlichen Verantwortlichkeiten durchgeführt wird (bspw. Marketing, Support, Design, Test).

Laut ISO/IEC 27005 [5] ist ein Risiko eine Kombination aus den Folgen, die sich aus dem Eintreten eines unerwünschten Ereignisses ergeben würden, und der Wahrscheinlichkeit des Eintretens des Ereignisses.

Daraus ergeben sich drei Elemente, die zur Einschätzung softwarebezogener Risiken für Messgeräte benötigt werden:

1. eine Liste unerwünschter Ereignisse - auch als Bedrohungen bezeichnet -, im gesetzlichen Messwesen eine Bedrohung für schützenswerte Güter, die sich aus den entsprechenden Anforderungen der MID [1] ergeben,
2. ein Maß für die Konsequenzen - auch als Auswirkung bezeichnet -, die aus einer realisierten Bedrohung entstehen und
3. eine Abschätzung der Eintrittswahrscheinlichkeit.

Kapitel 1 erläutert die in diesem Leitfaden verwendeten Begriffe.
Kapitel 2 beschreibt den allgemeinen Ablauf der Methodik der Software-Risikobewertung.
Kapitel 3 leitet anwendbare schützenswerte Güter von der MID [1] ab und stellt Definitionen von Bedrohungen vor.
Kapitel 4 beschreibt die Risikoanalyse aus Kapitel 3 mithilfe von elementaren Angriffsvektoren.

158 Kapitel 0 setzt die bestimmten Risikowerte in Kontext zur Bauart des Messgeräts und
159 seines Anwendungsgebietes.
160 Kapitel 0 enthält eine Vorlage für das Format eines Berichts zur Risikobewertung.

1. Begriffe

Einige Begrifflichkeiten stammen aus ISO/IEC 27005:2011 [5], ISO Guide 73:2009 [6] und ISO/IEC Guide 73:2002 [7].

Angriffsvektor *(attack vector)*: Technische Schritte, die ein Angreifer/eine Angreiferin unternimmt, um eine Bedrohung zu realisieren.

Angriffswahrscheinlichkeitsbaum (AWB) *(Attack Probability Tree (AtPT))*: Grafische Darstellung einer Bedrohung und ihrer entsprechenden Angriffsvektoren; es wird hervorgehoben, wie ein Angriff in Zwischenziele/Zwischenangriffe aufgeteilt werden kann.

Anmerkung 1: Wie detailliert der AWB ausfällt, hängt von der prüfenden Person ab.

Anmerkung 2: Blattknoten des Baums, die sich nicht weiter verzweigen, werden als Elementarangriffe bezeichnet.

Prüferin/Prüfer *(assessor)*: In diesem Leitfaden ist damit die Person bzw. die Personengruppe gemeint, die vom Hersteller des Messgeräts für die Durchführung der Risikobewertung ausgewählt wurde.

Schützenswertes Gut *(asset)*: Alles, was für die Organisation von Wert ist und somit Schutz benötigt [ISO/IEC 27005:2011].

Anmerkung: Schützenswerten Gütern sind eine oder mehrere der folgenden Sicherheitseigenschaften zugewiesen: Verfügbarkeit, Integrität, Authentizität.

Anmerkung: Schützenswerte Güter können Eigenschaften von Messgeräten sein, die geschützt werden müssen.

MID: Richtlinie 2014/32/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Messgeräten auf dem Markt (Neufassung) (Messgeräterichtlinie).

NAWID: Richtlinie 2014/31/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend die Bereitstellung nichtselbsttätiger Waagen auf dem Markt (Neufassung).

Risikoanalyse *(risk analysis)*: Prozess zum Verstehen von Risiken und zum Bestimmen des Risikoniveaus.

Anmerkung 1: Die Risikoanalyse liefert die Grundlage für die Risikobewertung und für Entscheidungen zur Risikobehandlung.

Anmerkung 2: Risikoanalyse beinhaltet Risikoeinschätzung [ISO/IEC 27005].

Risikobewertung *(risk assessment)*: Der gesamte Prozess der Risikoidentifikation, Risikoanalyse und Risikobewertung [ISO Guide 73:2009].

Risikoeinschätzung *(risk estimation)*: Der Prozess, der Wahrscheinlichkeit und den Konsequenzen eines Risikos Werte zuzuweisen [ISO/IEC Guide 73:2002].

Risikobewertung *(risk evaluation)*: Der Prozess, die Ergebnisse der Risikoanalyse mit den Risikokriterien zu vergleichen, um festzustellen, ob das Risiko und/oder sein Ausmaß akzeptabel oder tolerierbar ist [ISO Guide 73:2009].

Risikoidentifikation *(risk identification)*: Der Prozess des Findens, Erkennens und Beschreibens von Risiken [ISO Guide 73:2009].

Bedrohung *(threat)*: Ein unerwünschtes Ereignis, das dazu führen kann, dass eine oder mehrere Sicherheitseigenschaften eines schützenswerten Guts verletzt werden.

2. Ablauf der Software-Risikobewertung

Die hier beschriebene Methode folgt dem Grundgerüst und den Definitionen der ISO/IEC 27005 [5], wonach der Prozess der Risikobewertung in drei Stufen unterteilt ist:

1. Risikoidentifikation (siehe Kapitel 3): Dieser Prozess liefert eine Liste von unerwünschten Ereignissen (Bedrohungen für schützenswerte Güter), die sich aus den rechtlichen Anforderungen der MID [1] ergeben.
2. Risikoanalyse (siehe Kapitel 4): In dieser Phase wird den identifizierten Bedrohungen ein quantitatives oder qualitatives Risikomaß durch die Beurteilung sogenannter Angriffsvektoren zugewiesen. Je nach zugewiesener Risikoklasse für die Bauart (siehe WELMEC-Leitfaden 7.2 [3]) sollten entweder nur einfache, generische Angriffe (bei den meisten Geräten der Risikoklassen C und niedriger) oder komplexere Angriffe (hauptsächlich Risikoklassen D und höher) untersucht werden. Bei komplexen Angriffen können Angriffswahrscheinlichkeitsbäume (AWB) zur Unterstützung bei der Bewertung genutzt werden.
3. Risikobewertung (siehe Kapitel 5): Hier wird das Risiko im Kontext des untersuchten Messgeräts und seines geplanten Anwendungsbereichs berechnet, um zu beurteilen, ob das verbleibende Risiko (nach der Risikominderung) akzeptabel ist.

Abbildung 2-1 zeigt den angenommenen Arbeitsablauf der Risikobewertung.

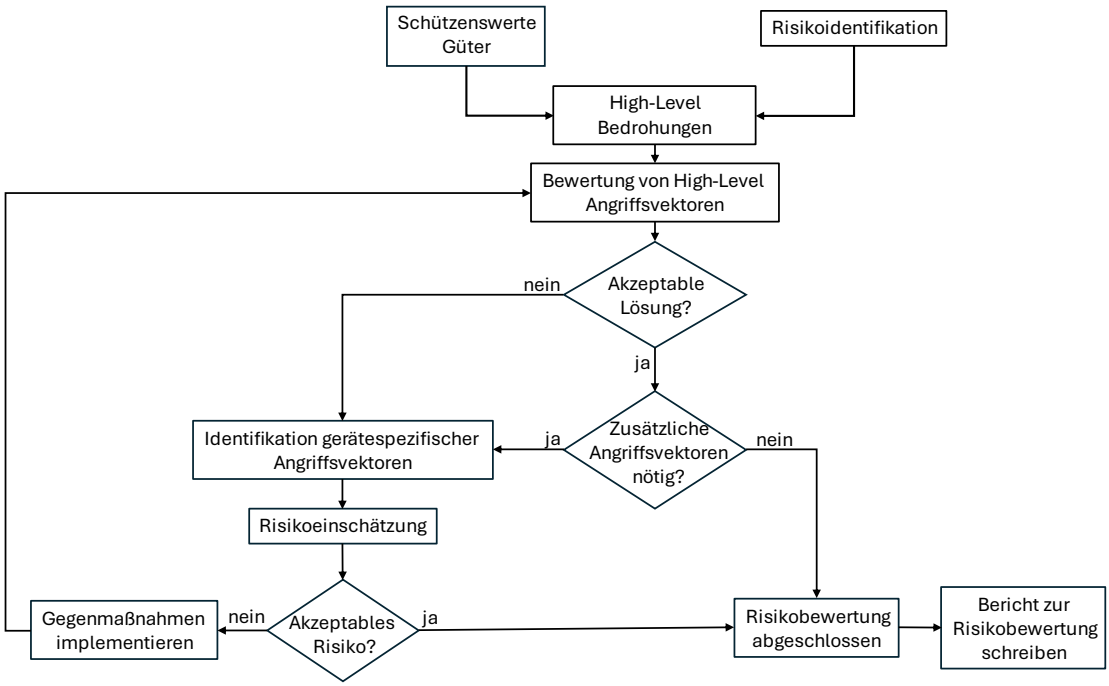


Abbildung 2-1:: Arbeitsablauf einer Risikobewertung

Es wird empfohlen, die Risikobewertung in zwei Phasen durchzuführen:

1. In der ersten Phase findet die Risikobewertung mit den definierten High-Level-Bedrohungen statt, die in 3.3.1 genannt werden.
2. Je nach Komplexität des Messgeräts bzw. seiner Risikoklasse müssen gerätespezifische Angriffsvektoren (siehe 3.3.4) definiert und weitere Bewertungen auf Grundlage dieser gerätespezifischen Angriffsvektoren durchgeführt werden. Zu beachten ist, dass die Prüfung zusätzlicher Angriffsvektoren unabhängig von der Risikoklasse des Messgeräts erforderlich sein kann.

3. Risikoidentifikation

Im Rahmen dieses Dokuments beziehen sich alle Risiken auf eine mögliche Nichtkonformität mit den wesentlichen Anforderungen der MID [1].

Anmerkung: Die Anforderungen der MID [1] müssen erfüllt sein, auch wenn das Risiko für das Auftreten eines Ereignisses sehr niedrig ist (z.B.: die MID [1] verlangt angemessenen Schutz gegen Veränderungen an Software. Folglich werden bei Fehlen dieses Schutzes die wesentlichen Anforderungen nicht erfüllt.)

Anmerkung: Allein der Nachweis eines Eingriffs ist kein angemessener Schutz gegen Änderungen an der Software. Die Software sollte gegen unbeabsichtigte und absichtliche Änderungen geschützt sein (MID Anhang I, Punkt 8.4) und es sollte der Nachweis eines Eingriffs vorhanden sein (MID Anhang I, Punkt 8.3). Für Anleitungen siehe WELMEC-Leitfaden 7.2 [3], P5, P6 und U5, U6 (auch P5, P6 und U5, U6 im WELMEC-Leitfaden 7.5 [4]).

3.1 Übergeordnete schützenswerte Güter

*Die Anforderungen von Anhang I der MID [1] ähneln denen des Anhangs I der NAWID [2], siehe insbesondere Anforderungen 8-10, 14.

Nr.	Schützenswertes Gut	Sicherheitseigenschaften	Anforderung (Anhang I, MID [1])*
1	Rechtlich relevante Software	• Verfügbarkeit • Integrität • Authentizität	• 7.1 • 7.2 • 7.6 • 8.3 • 8.4
	Identifikation der rechtlich relevanten Software	• Verfügbarkeit • Integrität • Authentizität	• 7.6 • 8.3
	Nachweis eines Eingriffs in die rechtlich relevante Software	• Verfügbarkeit • Integrität • Authentizität	• 8.2 • 8.3
	Angemessener Schutz der rechtlich relevanten Software	• Verfügbarkeit	• 8.1

Nr.	Schützenswertes Gut	Sicherheitseigenschaften	Anforderung (Anhang I, MID [1])*
2	Rechtlich relevante Parameter	• Verfügbarkeit • Integrität • Authentizität	• 7.1 • 8.4
	Angemessener Schutz der rechtlich relevanten Parameter	• Verfügbarkeit • Integrität • Authentizität	• 8.2 • 8.3
	Nachweis eines Eingriffs[1] in die rechtlich relevanten Parameter	• Verfügbarkeit • Integrität • Authentizität	• 8.1
3	Messergebnis, einschließlich der messergebnisrelevanten Daten	• Verfügbarkeit • Integrität	• 7.1 • 8.4
	Angemessener Schutz	• Verfügbarkeit • Integrität • Authentizität	• 8.1
4	Speicherung des Messergebnisses	• Verfügbarkeit • Integrität	• 11.1 • 11.2
	Angemessener Schutz	• Verfügbarkeit • Integrität • Authentizität	• 8.2 • 8.3
	Nachweis eines Eingriffs[1]	• Verfügbarkeit • Integrität • Authentizität	• 8.1
5	Anzeige des Messergebnisses: • Kennzeichnungen • Anzeige des Messergebnisses: klar und eindeutig	• Verfügbarkeit • Integrität • Authentizität	• 7.1 • 9 • 10.2 • 7.1 • 10.1 • 10.2 • 10.4
	Angemessener Schutz	• Verfügbarkeit • Integrität • Authentizität	• 8.1

[1] Auch wenn der Nachweis eines Eingriffs im Fall von Parameterschutz oder Schutz gespeicherter Messergebnisse nicht gefordert wird, ist er eine häufig genutzte Form von Schutz und sollte bei der Bewertung der Integrität von Parametern und gespeicherter Messergebnisse beachtet werden.

3.2 Definition der Bedrohung

Bedrohungen bestehen aus mindestens einem schützenswerten Gut und einer zugehörigen Aussage darüber, welche Sicherheitseigenschaft (Verfügbarkeit, Integrität und/oder Authentizität) durch die Bedrohung verletzt werden kann. Theoretisch müsste mindestens eine Bedrohung pro schützenswertem Gut formuliert werden.

3.3 Allgemeine Bedrohungen mit aus der MID abgeleiteten High-Level-Angriffsvektoren

Die von der MID [1] abgeleiteten übergeordneten Güter, siehe 3.1, wie Software, Parameter, Messergebnis, Anzeige und gespeichertes Ergebnis können als allgemeiner, von den übergeordneten Gütern unabhängiger Bedrohungssatz mit High-Level-Angriffsvektoren (bspw. Einfluss durch andere Software oder durch die Nutzer- bzw. Kommunikationsschnittstelle, Einfluss durch den Austausch von Hard- oder Software) abgebildet werden, indem nur die Art des Angriffs betrachtet wird und nicht zwischen Angriffen auf Software, Parameter etc. unterschieden wird.

Jeder dieser High-Level-Angriffsvektoren kann in alternative untergeordnete Angriffsvektoren unterteilt werden.

- Bezüglich des Einflusses durch die Kommunikationsschnittstelle sollten direkter Einfluss oder Einfluss während der Übertragung berücksichtigt werden.
- Bezüglich des unzulässigen Einflusses durch den Austausch von Hardware sollte unzulässiger Einfluss durch den Austausch (kompletter) Teile oder von Komponenten bzw. Einfluss durch das Verbinden eines Geräts mit dem Messgerät berücksichtigt werden.

Zweck dieser Unterteilung ist es, dabei zu helfen, den Basisknoten eines Angriffsbaums zu definieren, der das Hauptziel eines Angriffs darstellt, während untergeordnete Knoten Verfeinerungen eines solchen Angriffs sind. Die Blätter des Baumes repräsentieren dann Elementarangriffe, die nicht weiter unterteilt werden können. Ein einfaches Beispiel ist in **Abbildung 3-1** gegeben.

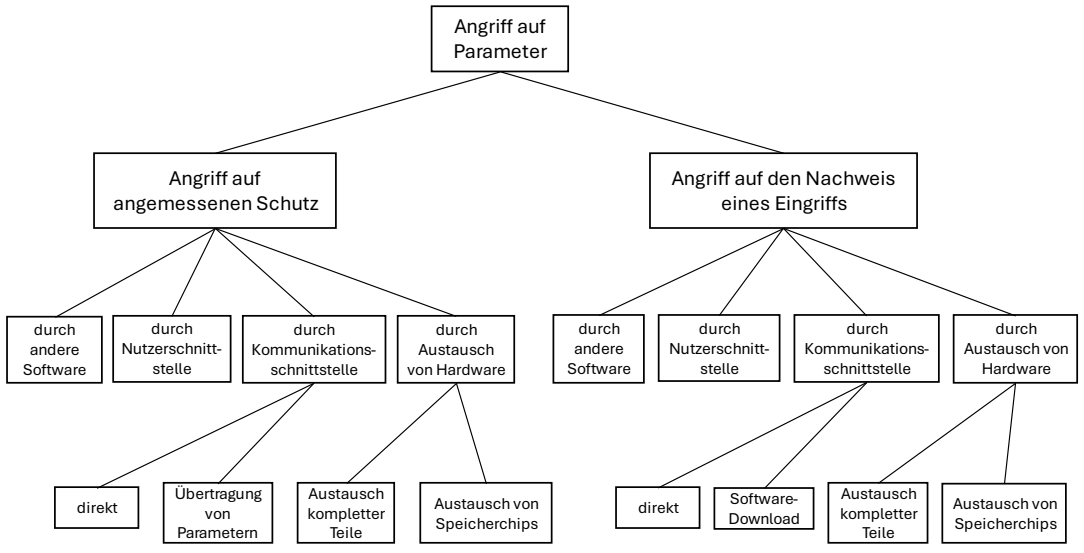


Abbildung 3-1: Einfache Darstellung von Angriffen auf „Parameter“, die schützenswerte Güter sind.

Eine detaillierte Erklärung findet sich in [8].

In Kapitel 3.4 ist eine Implementierung durch AWB beschrieben.

3.3.1 Von übergeordneten Gütern unabhängige High-Level-Angriffsvektoren

Nr.	High-Level-Angriffsvektor	Anforderung (Anhang I, MID [1])
1	unzulässiger Einfluss auf die übergeordneten Güter* **durch andere Software**	• 7.1 • 7.2 • 7.6 • 8.3 • 8.4
2	unzulässiger Einfluss auf die übergeordneten Güter **durch die Nutzerschnittstelle**	• 7.1 • 7.2 • 8.3 • 8.4
3	unzulässiger Einfluss auf die übergeordneten Güter **durch die Kommunikationsschnittstelle**	• 7.1 • 7.2 • 8.1 • 8.3 • 8.4
4	unzulässiger Einfluss auf die übergeordneten Güter **durch den Austausch von Hardware des Messgeräts**	• 7.1 • 8.2
5	unzulässiger Einfluss auf die übergeordneten Güter **durch den Austausch von Software**	• 8.3 • 8.4

3.3.2 Untergeordnete Angriffsvektoren, abgeleitet aus 3.3.1

In Bezug auf „Einfluss durch die Kommunikationsschnittstelle“

Nr.	Untergeordneter Angriffsvektor	Anforderung (Anhang I, MID [1])
1	unzulässiger Einfluss direkt durch die Kommunikationsschnittstelle, indem ein Gerät mit dem Messgerät verbunden wird	• 8.1 • 8.3 • 8.4
2	unzulässiger Einfluss während einer Übertragung, einschließlich Software-Download	• 8.1 • 8.3 • 8.4

In Bezug auf „Einfluss durch den Austausch von Hardware“:

Nr.	Untergeordneter Angriffsvektor	Anforderung (Anhang I, MID [1])
1	unzulässiger Einfluss durch den Austausch kompletter Teile	• 7.1 • 8.2
2	unzulässiger Einfluss durch den Austausch von Komponenten	• 7.1 • 8.2

3.3.3 Zusammenfassung von allgemeinen Bedrohungen mit High-Level-Angriffsvektoren für Messgeräte

Basierend auf der MID [1] oder NAWID [2] und dem WELMEC-Leitfaden 7.2 [3], können die folgenden High-Level-Bedrohungen definiert werden. Diese beinhalten Nr. 6 aus Kapitel 3.3.1 als Einfluss durch andere Software und Nr. 4 als Einfluss durch Kommunikationsschnittstellen.

Eine Person greift Software, Parameter, Messergebnis, gespeichertes Ergebnis oder die Anzeige an durch

- *andere Software*
- *Nutzerschnittstelle*
- *Kommunikationsschnittstelle*
  - *Direkter Einfluss, indem ein Gerät mit dem Messgerät verbunden wird*
  - *Durch Übertragung (einschließlich Software-Downloads)*
- *Verbinden eines Geräts mit dem Messgerät*
- *Austausch von Hardware*
  - *Austausch kompletter Teile*
  - *Austausch von Komponenten*
- *Austausch von Software (für Messgeräte von Typ U*)*

**Anmerkung für Prüfende: „Typ U“ Messgeräte oder nach WELMEC-Leitfaden 7.2 [3] „Messgeräte mit Universalgerät“. Siehe WELMEC-Leitfaden 7.2 [3] für weitere Details: „Typ U“ ist in Kapitel 5.1 genauer erklärt, entsprechend beschreibt Kapitel 4.1 „Typ P“ Messgeräte oder „eingebettete Software in einem Messgerät mit zweckgebundener Hard- und Software“.*

3.3.4 Gerätespezifische Angriffsvektoren für Messgeräte

Auf Grundlage der High-Level-Bedrohungen können gerätespezifische Angriffsvektoren definiert werden.

Wenn allerdings eine Bedrohung auf der obersten Ebene nicht realisiert werden kann, ist es nicht unbedingt nötig, gerätespezifische Angriffsvektoren zu definieren.

Wenn andererseits ein Messgerät auf einem Universalgerät basiert oder wenn einige Hardwaremodule „in der Cloud platziert“ sind, könnte es nötig sein, gerätespezifische Angriffsvektoren zu definieren (selbst für Geräte der Risikoklassen B oder C).

Des Weiteren ist die Extraktion von geheimen Startwerten/Schlüsseln im Fall von Geräten der Risikoklassen D oder E während der Übertragung ein gerätespezifischer Angriffsvektor, abgeleitet von „*kein unzulässiger Einfluss während der Übertragung*“. Es muss eine geprüfte Erklärung vorhanden sein, in der erläutert wird, warum gerätespezifische Risiken/Angriffsvektoren existieren oder nicht.

Anmerkung für Prüfende:

- *Bei einem Messgerät mit zweckgebundener Hard- und Software (siehe 3.3.1) der Risikoklasse B, das nicht mit anderen Geräten verbunden ist und dessen sämtliche Module sich im selben Gehäuse befinden, werden Angriffe auf die Software durch die Nutzerschnittstelle abgemindert, solange ein Softwaremodul vorhanden ist, das Befehle von der Nutzerschnittstelle empfängt und interpretiert.*
- *Dieses Softwaremodul leitet ausschließlich zugelassene Befehle an die anderen rechtlich relevanten Softwaremodule weiter. Alle unbekannten oder nicht erlaubten Sequenzen von Schalter- oder Tastenbetätigungen werden abgewiesen und haben keine Auswirkung auf die rechtlich relevante Software, die gerätespezifischen Parameter, das Messergebnis, das gespeicherte Ergebnis oder die Anzeige.*
- *Vorausgesetzt, dieses Softwaremodul wurde korrekt implementiert, besteht für dieses Messgerät keine Notwendigkeit, gerätespezifische Angriffsvektoren, die sich mit Angriffen über die Nutzerschnittstelle befassen, zu spezifizieren (siehe auch 3.2).*
- *In diesem Fall sollte die Entscheidung für die kürzere Auswahl an Bedrohungen im Bericht zur Risikobewertung begründet werden (siehe Kapitel 6).*

3.4 Bedrohungen basierend auf Angriffswahrscheinlichkeitsbäumen

Angriffswahrscheinlichkeitsbäume (AWB) sind grafische Darstellungen von Bedrohungen und deren Angriffsvektoren, die genutzt werden können, um sowohl komplexe Bedrohungen als auch Angriffsvektoren zu untersuchen (hauptsächlich in den Risikoklassen D und E). Der Basisknoten steht dabei für das Hauptziel eines Angriffs, während untergeordnete Knoten Verfeinerungen eines solchen Angriffs sind. Die Blattknoten des Baumes repräsentieren dann Elementarangriffe, die nicht weiter unterteilt werden können.

Beispiele für Angriffswahrscheinlichkeitsbäume können in [8] gefunden werden. Im Kontext dieses Dokuments werden AWB für drei bestimmte Zwecke genutzt:

- zur grafischen Darstellung der High-Level-Bedrohungen für Messgeräte (siehe Kapitel 3.3.1),
- um zusätzliche Bedrohungen zu modellieren, mit denen anzuwendende Angriffsvektoren für komplexe Geräte identifiziert werden (siehe Kapitel 3.3.4)
- um die Wahrscheinlichkeit des Auftretens komplexer Angriffsvektoren mithilfe von Attributvermehrung einzuschätzen (siehe Kapitel 4.2.2).

3.4.1 Angriffswahrscheinlichkeitsbäume basierend auf generischen Bedrohungen mit High-Level-Angriffsvektoren

Alle folgenden Beispiele beziehen sich auf die genannten übergeordneten Güter (Software, Parameter, Messergebnis, gespeichertes Ergebnis und Anzeige) aus Kapitel 3.1 und auf die generischen Bedrohungen aus Kapitel 3.3.1.

3.4.1.1 Angriffe auf rechtlich relevante Software

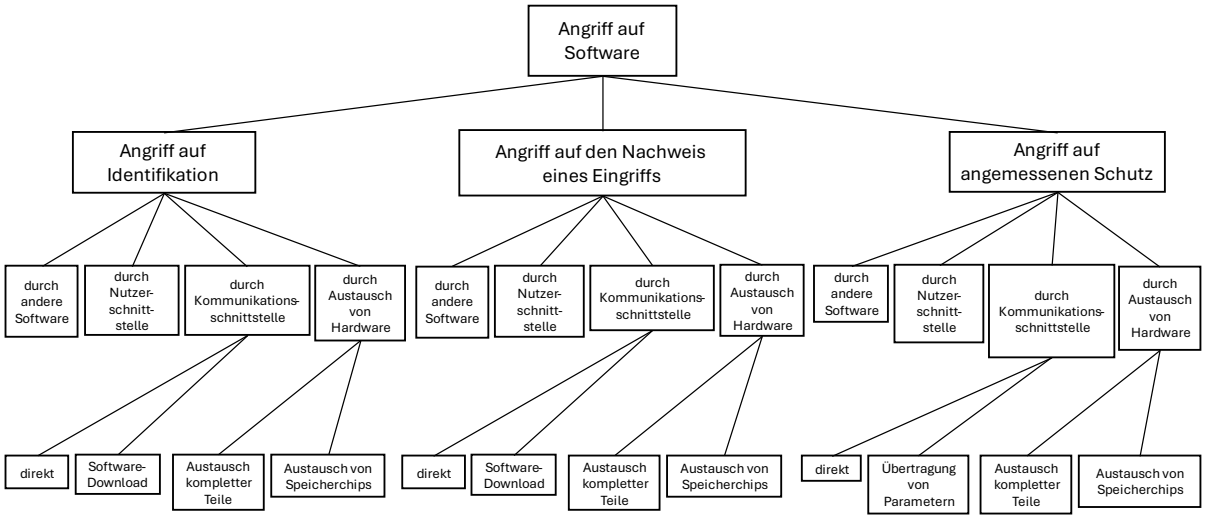


Abbildung 3-2: Generischer Angriffswahrscheinlichkeitsbaum für Bedrohungen, die sich auf die Manipulation von Software und die von ihr abgeleiteten Güter beziehen.

Ein Angriff kann Auswirkungen auf die Identifikation, den Nachweis eines Eingriffs oder den allgemeinen Schutz der Software während der Verarbeitung haben (unzulässiger Einfluss).

Die drei Teilbäume zeigen (basierend auf der Messgerätearchitektur des WELMEC-Leitfadens 7.2 [3]), wie ein Angriff implementiert werden könnte, ohne auf technische Details einzugehen.

3.4.1.2 Angriffe auf rechtlich relevante Parameter

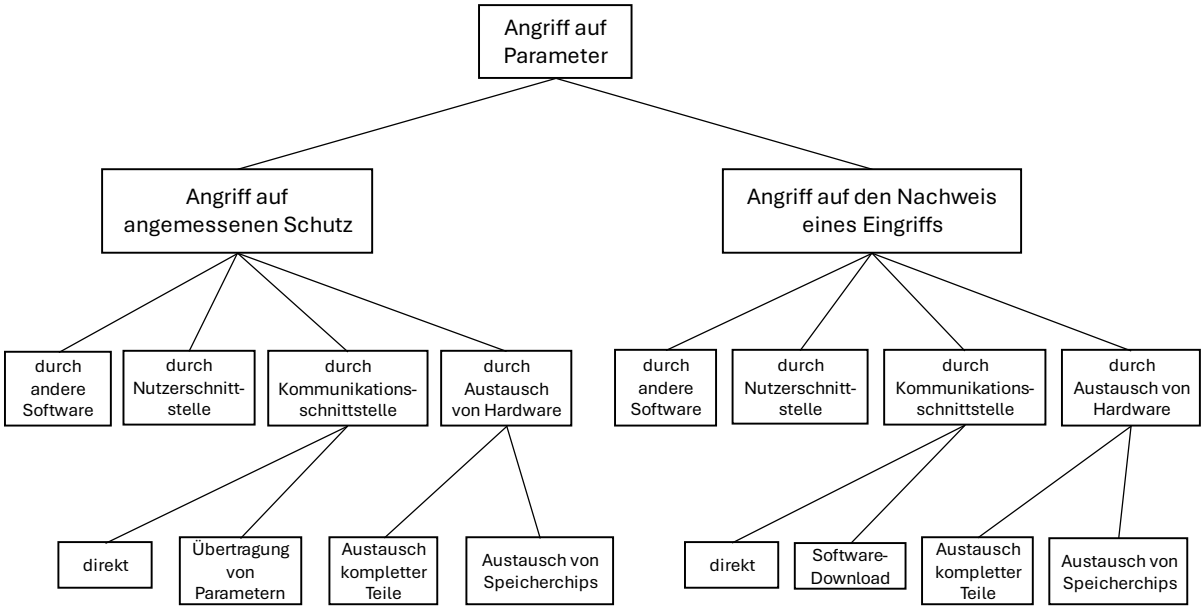


Abbildung 3-3: Generischer Angriffswahrscheinlichkeitsbaum für Bedrohungen, die sich auf die Manipulation von Parametern beziehen.

3.4.1.3 Angriffe auf rechtlich relevante Messergebnisse während der Verarbeitung

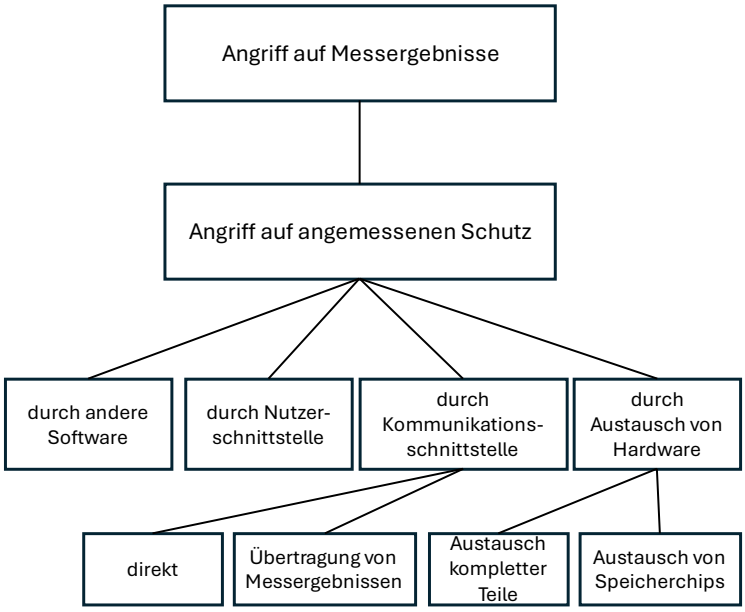


Abbildung 3-4: Generischer Angriffswahrscheinlichkeitsbaum für Bedrohungen, die sich auf die Manipulation von Messergebnissen beziehen.

3.4.1.4 Angriffe auf gespeicherte Messergebnisse

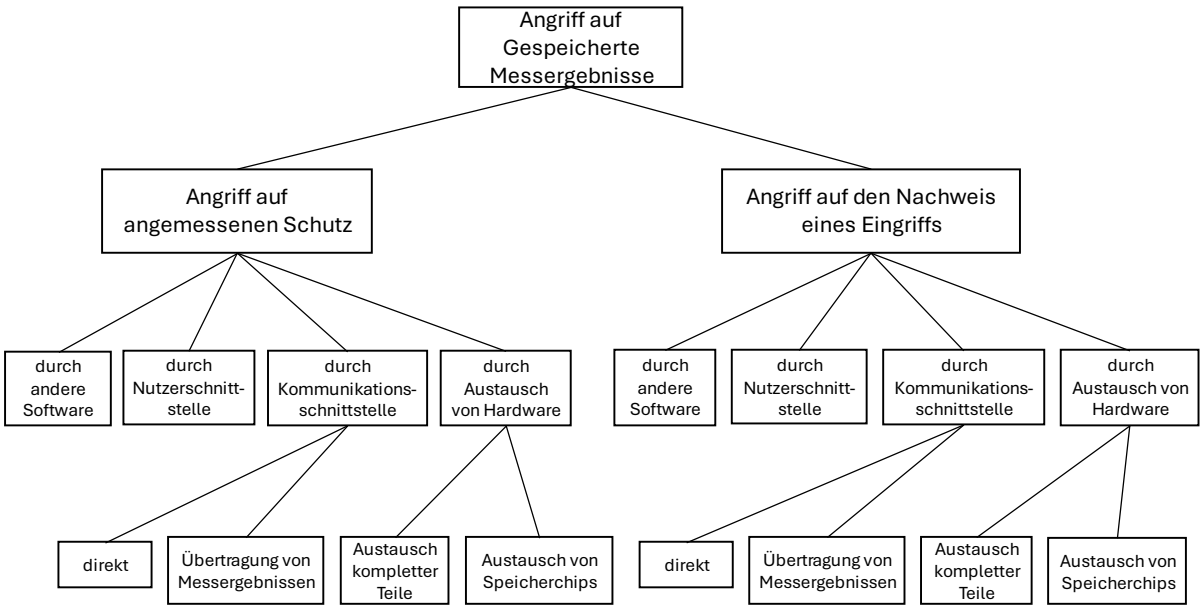


Abbildung 3-5: Generischer Angriffswahrscheinlichkeitsbaum für Bedrohungen, die sich auf die Manipulation von gespeicherten Messergebnissen beziehen.

3.4.1.5 Angriffe auf die rechtlich relevante Anzeige des Messergebnisses

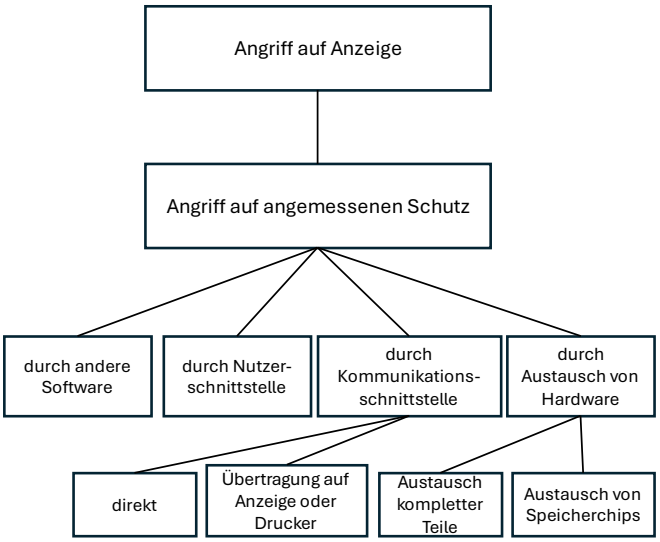


Abbildung 3-6: Generischer Angriffswahrscheinlichkeitsbaum für Bedrohungen, die sich auf die Manipulation der rechtlich relevanten Anzeige beziehen.

3.4.2 Angriffswahrscheinlichkeitsbäume basierend auf gerätespezifischen Angriffsvektoren

Gerätespezifische Bedrohungen können durch Angriffswahrscheinlichkeitsbäume dargestellt werden (siehe **Abbildung 3-7**). Diese erlauben es der prüfenden Person, gewisse Bedrohungen je nach Geräteeigenschaften in verschiedene Teilziele zu unterteilen. Um die Vergleichbarkeit der Bewertungsergebnisse für solche Bedrohungen zu gewährleisten, ist es wichtig, die entsprechenden Angriffswahrscheinlichkeitsbäume vollständig zu dokumentieren, siehe Anhang C.

Die folgende Abbildung ist ein Beispiel für ein Taxameter, entnommen aus [8]. Das Beispiel wird in Anhang D ausführlich beschrieben.

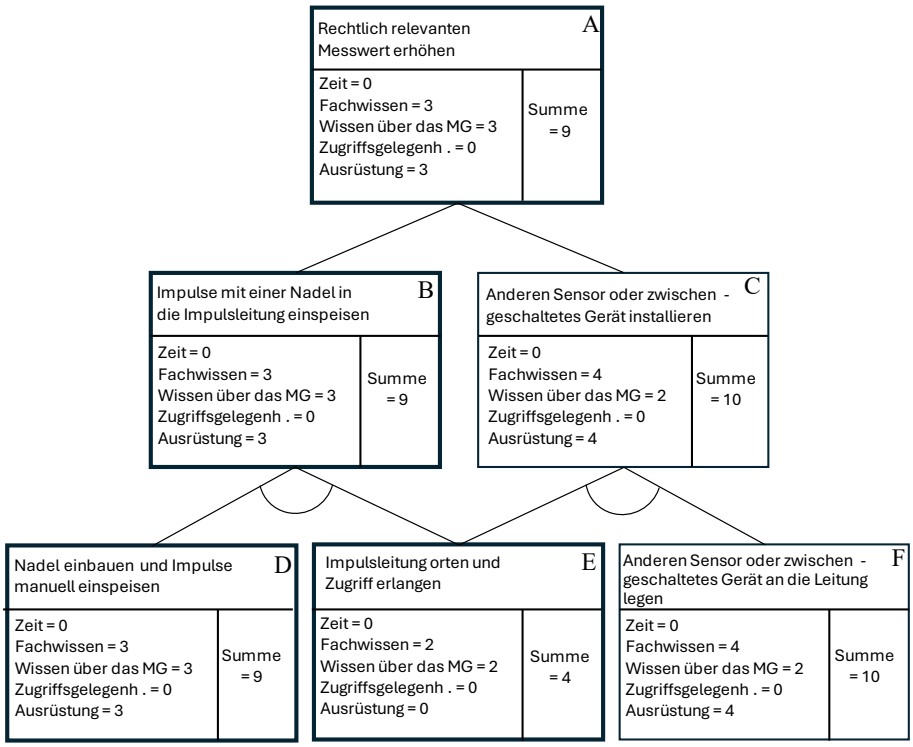


Abbildung 3-7: Beispielhafter Angriffswahrscheinlichkeitsbaum mit zugewiesenen Werten für alle Knoten zur unzulässigen Einflussnahme auf den Messwert von Taxametern durch Manipulation am analogen Signalpfad. In diesem Szenario existieren zwei Angriffsvektoren: das manuelle Einspeisen zusätzlicher Impulse in die Impulsleitung mithilfe einer Nadel (Knoten (B)) und die Installation eines anderen Wegstreckensignalgebers bzw. eines anderen zwischengeschalteten Geräts in den Signalpfad (Knoten C)). Da diese beiden Angriffsvektoren Alternativen zueinander sind, werden sie mit dem übergeordneten Knoten (A) durch eine ODER-Verbindung, dargestellt durch zwei einfache Linien, verbunden. Ein Bogen zwischen zwei oder mehr Linien würde eine UND-Verbindung repräsentieren [8].

4 Risikoanalyse: Analyse von Angriffsvektoren

Bei der Risikoanalyse muss der Aufbau des Geräts mit in Betracht gezogen werden.

Wenn das Gerät bspw. aus zwei getrennten Modulen besteht und/oder wenn Peripheriegeräte in die Messkette eingebaut sind, muss das Risiko auf zwei Ebenen bewertet werden:

1. für jedes einzelne Modul oder Peripheriegerät[2];
2. für das komplette Gerät.

Dass die Software auf einem Modul adäquat geschützt ist, bedeutet nicht zwangsläufig, dass das komplette Gerät adäquat geschützt ist, d.h., Software auf den anderen Modulen kann unzureichend geschützt sein.

Die Integrität des kompletten Geräts kann gefährdet werden, wenn ein Modul oder die Schnittstelle zwischen Modulen des Geräts angegriffen werden.

4.1 Risikoanalyse zu High-Level-Angriffsvektoren

Die Risikobewertung der High-Level-Bedrohungen besteht aus zwei Schritten:

1. Die Prüferin / der Prüfer muss alle elementaren Angriffsvektoren aus den generischen Angriffswahrscheinlichkeitsbäumen (siehe Kapitel 3.4.1) entfernen, die nicht anwendbar sind, beispielsweise, wenn die behandelte Eigenschaft (z.B. andere Software oder Kommunikationsschnittstelle) nicht vorhanden ist. Diese Angriffsvektoren müssen nicht weiter untersucht werden.
2. Die Prüferin / der Prüfer muss ebenfalls begutachten, ob den High-Level-Angriffsvektoren mit einer Gegenmaßnahme nach einer der akzeptablen Lösungen aus dem WELMEC-Leitfaden 7.2 [3] begegnet wird. Diese Angriffsvektoren gelten nach der Implementierung einer dieser akzeptablen Lösungen als angemessen abgemindert.

Wenn das Messgerät der Risikoklasse C oder niedriger zugeordnet ist, die im WELMEC-Leitfaden 7.2 genannten akzeptablen Lösungen genutzt wurden und keine zusätzlichen gerätespezifischen Bedrohungen beachtet werden müssen (siehe 3.3.4), gilt die Risikoanalyse als abgeschlossen, wenn High-Level-Angriffsvektoren analysiert wurden.

Andernfalls muss die Eintrittswahrscheinlichkeit der verbleibenden Angriffsvektoren nach der in Kapitel 4.2 beschriebenen Methode abgeschätzt werden.

[2] Es kann hilfreich sein, wenn Hersteller von Modulen und/oder Peripheriegeräten ihr Equipment nach dem *freiwilligen System zur modularen Bewertung von Messgeräten* auf Risiko bewerten lassen, siehe WELMEC-Leitfaden 8.8 sowie die verschiedenen technischen Implementierungsleitfäden für das freiwillige System zur modularen Bewertung für spezifische Messgeräte auf der WELMEC-Webseite.

4.2 Risikoanalyse für gerätespezifische Angriffsvektoren

4.2.1 Identifikation zusätzlicher Angriffsvektoren

Diese Methode kann als Werkzeug dienen, um weitere Bedrohungen, Angriffsvektoren und schützenswerte Güter zu finden, zusätzlich zu den generischen, die in der MID [1]/NAWID [2] und dem WELMEC-Leitfaden 7.2 [3] genannt werden. Unabhängig von der Risikoklasse des Geräts muss die Prüferin/der Prüfer in Betracht ziehen, ob es zusätzliche Angriffsvektoren gibt, beispielsweise in Bezug auf komplexere Technologien wie Cloud-Computing oder dezentrale Geräte.

1. Bei Geräten, die keine im WELMEC-Leitfaden 7.2 [3] beschriebene akzeptable Lösung nutzen, müssen gerätespezifische Angriffsvektoren betrachtet werden.
2. Bei komplexen Geräten kann es nötig sein, gerätespezifische Angriffsvektoren zu betrachten, siehe 3.3.4.
3. Bei Geräten der Risikoklasse D und höher müssen zusätzlich zu den in Kapitel 3.3.1 beschriebenen Angriffen komplexere Angriffe einkalkuliert werden. Solche Angriffe könnten z.B. mehr als eine Schnittstelle nutzen (z.B. eine Kombination aus Nutzer- und Kommunikationsschnittstelle) oder ein kryptografischer Angriff auf Daten während der Übertragung sein (z.B. Extraktion geheimer Startwerte/Schlüssel).

Wenn die Angriffsvektoren zu komplex werden, um sie im Ganzen zu bearbeiten, können Angriffswahrscheinlichkeitsbäume genutzt werden, um darzustellen, welche elementaren Angriffsvektoren kombiniert werden können, um eine Bedrohung zu realisieren. Die Nutzung von Angriffswahrscheinlichkeitsbäumen im gesetzlichen Messwesen ist in [8] detailliert beschrieben.

4.2.2 Wahrscheinlichkeitsschätzung

Um die Eintrittswahrscheinlichkeit eines Angriffsvektors abzuschätzen, wird eine Methode namens Schwachstellenanalyse aus der ISO/IEC 18045 [9] genutzt. Bei der Analyse wird dem Angriffsvektor in fünf Kategorien jeweils ein Punktwert zugewiesen: abgelaufene Zeit, Fachwissen und Detailkenntnisse des Messsystems, Zugriffsgelegenheiten und benötigte Ausrüstung.

Angriffs-ID	Beschreibung des Angriffsvektors	Abgelaufene Zeit	Fachwissen	Wissen über das Messsystem	Zugriffsgelegenheiten	Ausrüstung	Gesamt	Auswirkung	Begründung
AVx1									
AVx2									
AVx3									

Tabelle 4-1: Bewertung der elementaren Angriffsvektoren

Jeder Angriffsvektor (AVxy) muss für eine einfache Evaluierung der Bewertungsergebnisse richtig beschrieben sein. Basierend auf dieser Beschreibung muss eine Begründung für die gewählten Punktwerte gegeben werden, um die Objektivität der Ergebnisse zu gewährleisten. Beispiele für bewertete Angriffsvektoren mit entsprechenden Begründungen der Punktwerte sind in Anhang D zu finden. Jeder einzelne

komplette Angriffsvektor (z.B. der Wurzelknoten des Angriffswahrscheinlichkeitsbaums) muss einen ihm zugewiesenen Auswirkungswert haben, der entweder 1 für Angriffe sein kann, die nach einmaliger Ausführung alle zukünftigen (oder vergangenen) Messwerte beeinflussen, oder $\frac{1}{3}$ für Angriffe, die für jedes einzelne Messereignis wiederholt werden müssen.

Die Zuordnung der berechneten Summenwerte zu den jeweiligen Wahrscheinlichkeitswerten ist in **Tabelle 0-6** in 0 dargestellt. Danach wird das Risiko, das jedem Angriffsvektor zugeordnet wurde, berechnet, indem die Scores der Auswirkung und der Wahrscheinlichkeit multipliziert werden.

Für den Fall, dass ein Angriffswahrscheinlichkeitsbaum zur Untersuchung eines komplexen Angriffsvektors genutzt wurde, befinden sich Regeln zur Berechnung der Eintrittswahrscheinlichkeit des Wurzelknotens aus den Scores der Blattknoten in [8]. Das dem Wurzelknoten zugeordnete Risiko wird dann wieder durch Multiplikation der Werte von Auswirkung und Wahrscheinlichkeit berechnet.

5 Risikobewertung

Im letzten Schritt der Risikobewertung werden die abgeschätzten Risiko-Scores in Kontext zur Messgerätebauart gesetzt. Für Geräte der Risikoklassen C und niedriger ist ein Risikowert unter 4 allgemein akzeptabel. Liegt der berechnete Risikowert darüber, sollte der Prüfer/die Prüferin den Hersteller auffordern, zusätzliche Schutzmaßnahmen zu implementieren und die Bewertung zu wiederholen. Für Risikoklassen D und höher sollte der Prüfer/die Prüferin je nach Anwendungsgebiet des Messgeräts entscheiden, ob die Obergrenze des Wertes für die Risikobewertung herabgesetzt wird.

Für einfache Geräte (allgemein Risikoklasse C und darunter) wird kein Risikowert benötigt, wenn es für alle Angriffsvektoren Gegenmaßnahmen laut einer akzeptablen Lösung gibt oder wenn keine gerätespezifischen Angriffsvektoren existieren, siehe 4.2.1 und **Abbildung 2-1** Arbeitsablauf.

5.1 Risikobewertung im Kontext vom Zweck des Messgeräts und entsprechende Motivation für einen Angriff

WELMEC-Leitfaden 7.2 [3] gibt in Erweiterung I Beispiele für einige Messgerätearten. Jedoch kann für Geräte, die dort nicht genannt werden und/oder für Geräte mit dediziertem Zweck das folgende Vorgehen angewandt werden, um dem Zweck der Messgerätebauart gerecht zu werden:
Der nach Anweisungen in Kapitel 4 berechnete „Risikopunktwert“ kann als Obergrenze genutzt und reduziert werden, wenn Folgendes betrachtet wird:

Bewerten Sie den Zweck des Geräts unter den folgenden drei Aspekten unter „Überlegungen eines Angreifers zur Risikobewertung“:

5.1.1 Nutzen für den Angreifer / die Angreiferin (NA) - was wird der Nutzen einer Manipulation sein?

Auch wenn Angriffe „einfach nur so“ natürlich nicht vollständig ausgeschlossen werden können, besteht doch eine höhere Wahrscheinlichkeit für einen bestimmten Angriff, wenn sich aus diesem ein gewisser Nutzen für eine Person ergibt. Dies kann bei der folgenden Klassifikation in Betracht gezogen werden:

	Nutzen	Punktwert
I	Keiner	3
II	Geringer finanzieller Nutzen oder Schaden für einen Konkurrenten	2
III	Mittelgradiger finanzieller Nutzen	1
IV	Hoher finanzieller Nutzen	0

Anmerkung: Die Unterscheidung zwischen geringem und hohem finanziellem Nutzen ist gewiss etwas subjektiv. Als Faustregel: Wenn der Angreifer/die Angreiferin genug Geld bekommt, um davon leben zu können, sollte von „hohem finanziellem Nutzen“ ausgegangen werden.

5.1.2 Risiko auf Verdächtigung nach dem Angriff - wie offensichtlich ist es, wer einen Nutzen aus der Manipulation zieht?

Wenn es wahrscheinlich ist, dass der Angreifer/die Angreiferin unter Verdacht gerät, weil er oder sie die einzige Person ist, die aus einem bestimmten Angriff einen Nutzen zieht, wird dieser Angriff weniger wahrscheinlich sein als einer, bei dem man sich hinter Anonymität verstecken kann.

	Profiteure	Punktwert
I	Nur eine einzige Person würde von der Manipulation profitieren	3
II	Kleine Personengruppe (z.B. Angestellte eines bestimmten Unternehmens)	2
III	Große, aber begrenzte Personengruppe	1
IV	Buchstäblich alle	0

Anmerkung: Dieser Punkt ähnelt dem „Risk of Sanction“ im WELMEC-Leitfaden 5.3, Anhang I, 10.

5.1.3 Risiko für den Angreifer/die Angreiferin nach Entdeckung - was wären die Konsequenzen, wenn die Person entdeckt wird?

Je höher die potenzielle Strafe für eine bestimmte Manipulation, desto geringer die Wahrscheinlichkeit, dass jemand dieses Risiko eingehen würde.

	Potenzielle Bestrafung	Punktwert
I	Lange Haftstrafe	3
II	Kurze Haftstrafe	2
III	Hohe Geldstrafe	1
IV	Geringe Geldstrafe	0

Anmerkung: Dieser Punkt ähnelt dem „Risk of Sanction“ im WELMEC-Leitfaden 5.3, Anhang I, 11.

5.1.4 Die Motivation für einen Angriff in Betracht ziehen

Die Punktwerte aus 5.1.1 bis 5.1.3 können summiert werden, um ein Maß der Motivation eines Angreifers oder einer Angreiferin zu erstellen. Es ergibt sich ein Wert zwischen 0 (hohe Motivation) und 9 (geringe Motivation).
Entsprechend der Argumentation in [10] kann dieser Wert als untere Grenze für die Punktwerte für „Fachwissen“ und „Ausrüstung“ für jeden Angriffsvektor angesehen werden. Das bedeutet beispielsweise, wenn die Summe von 5.1.1 bis 5.1.3 6 ergibt, sollten die Punktwerte für „Fachwissen“ und „Ausrüstung“ nicht niedriger als 6 gewählt werden.

6 Bericht zur Risikobewertung

Für einfache Geräte, bei denen akzeptable Lösungen genutzt werden, kann die Checkliste aus Anhang A genutzt werden, um den Bericht über die Ergebnisse der Risikobewertung zu erstellen.0

Für alle anderen Geräte steht eine Berichtsvorlage in Anhang C zur Verfügung.

7 Referenzen

[1] „Richtlinie 2014/32/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Messgeräten auf dem Markt (Neufassung)“, *Amtsblatt der Europäischen Union, L 96,* S. 149 - 250, 29. März 2014.

[2] „Richtlinie 2014/31/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 zur Angleichung der Rechtsvorschriften der Mitgliedstaaten betreffend die Bereitstellung nichtselbsttätiger Waagen auf dem Markt“, *Amtsblatt der Europäichen Union, L 96,* S. 107 - 148, 2014.

[3] „WELMEC-Leitfaden 7.2: Softwareleitfaden (Europäische Messgeräterichtlinie 2014/32/EU)“, *WELMEC,* 2023.

[4] „WELMEC-Leitfaden 7.5: Software in NAWIs (Non-automatic Weighing Instruments Directive 2014/31/EU)“, *WELMEC,* 2020.

[5] „ISO/IEC 27005:2011(E) Information technology - Security techniques - Information security risk management“, International Organization for Standardization, Genf, CH, Juni 2011.

[6] „ISO Guide 73:2009 Risk management — Vocabulary“, International Organization for Standardization, Genf, CH, November 2009.

[7] „ISO/IEC Guide 73:2002 Risk management — Vocabulary — Guidelines for use in standards“, International Organization for Standardization, Genf, CH, Januar 2002.

[8] M. Esche, F. Grasso Toro und F. Thiel, „Representation of Attacker Motivation in Software Risk Assessment Using Attack Probability Trees“, in *Proceedings of the Federated Conference on Computer Science and Information Systems (FedCSIS) https://annals-csis.org/Volume_11/drp/pdf/112.pdf*, Prag, Tschechien, 2017.

[9] „ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation“, International Organization for Standardization, Genf, CH, August 2008.

[10] M. Esche und F. Thiel, „Incorporating a Measure for Attacker Motivation into Software Risk Assessment for Measuring Instruments in Legal Metrology“, in *18. GMA/ITG-Fachtagung Sensoren und Messsysteme*, Nürnberg, Deutschland, 2016.

Anhang A Checkliste

Siehe separate Excel-Datei „Anhang A_Risikoanalyse (Version 4).xlsx“

Anhang B Tabellen und Beispiele

Tabelle 0-1 bis **Tabelle 0-5** liefern die Punktwerte, die den verschiedenen Eigenschaften eines Angriffs zuzuweisen sind. Erklärungen, welcher Wert in besonderen Fällen zu wählen ist, können in der Spalte „Anmerkungen“ gefunden werden.

Abgelaufene Zeit	Punkte	Anmerkungen
weniger als 1 Tag	0	Eine Person, die über das Fachwissen, das Wissen über das Messsystem und die Ausrüstung verfügt und Zugang zu dem Messgerät hat, kann den betrachteten Angriffsvektor in weniger als einem Tag implementieren.
weniger als 1 Woche	1	Eine Person, die über das Fachwissen, das Wissen über das Messsystem und die Ausrüstung verfügt und Zugang zu dem Messgerät hat, kann den betrachteten Angriffsvektor in weniger als einer Woche implementieren, da sie ein einfaches Script zur Durchführung des Angriffs vorbereiten oder eine Suche nach einem einfachen Passwort durchführen muss.
weniger als 2 Wochen	2	Eine Person, die über das Fachwissen, das Wissen über das Messsystem und die Ausrüstung verfügt und Zugang zu dem Messgerät hat, kann den betrachteten Angriffsvektor in weniger als zwei Wochen implementieren, da sie ein einfaches Programm zur Durchführung des Angriffs vorbereiten oder eine Suche nach einem einfachen Passwort durchführen muss.
weniger als 1 Monat	4	Einer Person mangelt es an Fachwissen, Wissen über das Messsystem oder an Ausrüstung, oder sie hat keinen Zugriff auf das Gerät und kann den betrachteten Angriffsvektor in weniger als einem Monat implementieren, da sie ein mittelmäßig komplexes Script zur Durchführung des Angriffs vorbereiten oder eine Suche nach einem mittelstarken Passwort durchführen muss.
weniger als 2 Monate	7	Einer Person mangelt es an Fachwissen, Wissen über das Messsystem oder an Ausrüstung, oder sie hat keinen Zugriff auf das Gerät und kann den betrachteten Angriffsvektor in weniger als zwei Monaten implementieren, da sie ein mittelmäßig komplexes Programm zur Durchführung des Angriffs vorbereiten oder eine Suche nach einem mittelstarken Passwort durchführen muss.
weniger als 3 Monate	10	Einer Person mangelt es an Fachwissen, Wissen über das Messsystem oder an Ausrüstung, oder sie hat keinen Zugriff auf das Gerät und kann den betrachteten Angriffsvektor in weniger als drei Monaten implementieren, da sie ein mittelmäßig komplexes Programm zur Durchführung des Angriffs vorbereiten oder eine Suche nach einem mittelstarken Passwort durchführen muss.
weniger als 4 Monate	13	Einer Person mangelt es an Fachwissen, Wissen über das Messsystem oder an Ausrüstung, oder sie hat keinen Zugriff auf das Gerät und kann den betrachteten Angriffsvektor in weniger als vier Monaten implementieren, da sie ein komplexes Programm zur Durchführung des Angriffs vorbereiten oder eine Suche nach einem starken Passwort durchführen muss.
weniger als 5 Monate	15	Einer Person mangelt es an Fachwissen, Wissen über

		das Messsystem oder an Ausrüstung, oder sie hat keinen Zugriff auf das Gerät und kann den betrachteten Angriffsvektor in weniger als fünf Monaten implementieren, da sie ein komplexes Programm sowie eine Infrastruktur zur Durchführung des Angriffs vorbereiten oder eine Suche nach einem starken Passwort oder einem einfachen kryptografischen Schlüssel durchführen muss.
weniger als 6 Monate	17	Einer Person mangelt es an Fachwissen, Wissen über das Messsystem oder an Ausrüstung, oder sie hat keinen Zugriff auf das Gerät und kann den betrachteten Angriffsvektor in weniger als sechs Monaten implementieren, da sie ein komplexes Programm sowie eine Infrastruktur zur Durchführung des Angriffs vorbereiten oder eine Suche nach einem starken Passwort oder einem mittelstarken kryptografischen Schlüssel durchführen muss.
mehr als 6 Monate	19	Eine Person wird mehr als ein halbes Jahr benötigen, um den Angriff zu implementieren. Dies schließt sowohl die direkt am Gerät vorgenommenen Schritte als auch die vorbereitende Arbeit andernorts ein, da der Angreifer/die Angreiferin ein komplexes Programm sowie eine Infrastruktur zur Durchführung des Angriffs vorbereiten oder eine Suche nach einem starken Passwort oder einem starken kryptografischen Schlüssel durchführen muss.

Tabelle 0-1: Punktwerte für abgelaufene Zeit

Fachwissen	Punkte	Anmerkungen
Laie	0	Bezogen auf IT-Fähigkeiten ist ein Laie jede Person, die mit einem PC auf Webseiten browsen kann.
Kompetent	3	Kompetent ist jede Person, die in der Lage ist, spezialisierte Software zu finden, zu installieren und zu nutzen (z.B. einen Netzwerksniffer).
Experte	6	Jede Person, die in der Lage ist, spezifische Software zur Durchführung einer bestimmten Aufgabe zu schreiben, zu bauen und zu nutzen, gilt als Experte.
Mehrfach-Experten	8	Die Fachwissen-Stufe „Mehrfach-Experten“ sollte nur gewählt werden, wenn Fachkenntnis auf mehr als einem Gebiet (Softwareentwicklung, Kryptografie, Hardwareentwicklung) erforderlich ist, um einen Angriff zu implementieren.

Tabelle 0-2: Punktwerte für Fachwissen

Wissen über das Messsystem	Punkte	Anmerkungen
Öffentlich	0	Die benötigten Kenntnisse, um einen Angriff zu implementieren, sind öffentlich verfügbar. Sämtliche Informationen, die durch eine Suche im Internet gefunden werden können, fallen in diese Kategorie.
Eingeschränkt	3	Beispiele für eingeschränkte Kenntnisse sind Bedienungsanleitungen, die nur zusammen mit einem Gerät versandt werden. Solche Informationen stehen nur einer eingeschränkten Gruppe zur Verfügung und sind nicht öffentlich einsehbar.
Sensibel	7	Kenntnisse, die nur dem Hersteller und autorisierten Personen

		zur Verfügung stehen. Ein Beispiel für sensible Kenntnisse wären Verbindungseinstellungen, die nur zwischen dem Hersteller und dem Nutzer/der Nutzerin geteilt werden.
Kritisch	11	Informationen, die nur einer begrenzten Anzahl an Angestellten des Herstellers und möglicherweise der Konformitätsbewertungsstelle bekannt sind, werden als „kritisch“ eingestuft. Ein Passwort, das von einem Eichbeamten/einer Eichbeamtin gesetzt wurde, würde ebenfalls in diese Kategorie fallen.

Tabelle 0-3: Punktwerte für Wissen über das Messsystem

Zugriffsgelegenheiten	Punkte	Anmerkungen
Unnötiger/unbeschränkter Zugriff	0	Nicht notwendiger/unbegrenzter Zugriff bedeutet, dass der Angreifer/die Angreiferin keinen Zugriff auf das Gerät haben muss, um einen Angriff zu implementieren, oder dass kein Risiko besteht, während des Zugriffs entdeckt zu werden.
Einfach	1	Zugriff gilt als leicht, wenn der Zugang zum Gerät ohne Schwierigkeiten erlangt werden kann und nicht länger als einen Tag dauern muss.
Moderat	4	Wenn ein Angreifer/eine Angreiferin nicht länger als einen Monat Zugriff auf das Gerät haben muss und wenn der Angriff wahrscheinlich entdeckt wird, gilt das Zugriffszeitfenster als moderat.
Schwierig	10	Schwieriger Zugriff bedeutet, dass eine Person länger als einen Monat direkten Zugriff auf das Gerät haben muss und dass eine Entdeckung höchstwahrscheinlich ist.
Kein Zugriff	**	Sollte Zugriff auf das Gerät aufgrund von zeitlichen Beschränkungen unmöglich sein, muss das damit verbundene Angriffsszenario nicht evaluiert werden.

Tabelle 0-4: Punktwerte für Zugriffsgelegenheiten

Ausrüstung	Punkte	Anmerkungen
Standard	0	Standardausrüstung ist sämtliche Ausrüstung, die leicht verfügbar ist, bspw. jedes übliche Werkzeug auf einem PC oder Software, die frei aus dem Internet heruntergeladen werden kann.
Speziell	4	Wenn ein Werkzeug gekauft oder ohne große Mühe geschrieben werden kann, fällt es in die Kategorie spezieller Ausrüstung.
Maßgeschneidert	7	Maßgeschneiderte Ausrüstung wäre hochentwickelte Software, die speziell für den Zweck eines Angriffs auf das Gerät entwickelt werden muss.
Mehrfach maßgeschneidert	9	Die Stufe „mehrfach maßgeschneidert“ sollte nur gewählt werden, wenn mehrere Spezialanfertigungen für verschiedene Zwecke (Kryptoanalyse, Softwareentwicklung etc.) notwendig sind.

Tabelle 0-5: Punktwerte für Ausrüstung

Summe der Punktwerte	Wahrscheinlichkeitswert	Anmerkungen
0-9	5	Das Gerät bietet keinen Widerstand gegen einen Angriff und das Auftreten eines Angriffs ist sehr

		wahrscheinlich.
10-13	4	Das Gerät verfügt nur über grundlegende Sicherheitsmerkmale; das Auftreten eines Angriffs ist wahrscheinlich.
14-19	3	Die Sicherheitsmerkmale des Geräts bieten erweiterten grundlegenden Schutz. Das Auftreten eines Angriffs ist nicht sehr wahrscheinlich.
20-24	2	Das Gerät bietet moderaten Widerstand gegen Angriffe und das Auftreten eines Angriffs ist unwahrscheinlich.
>24	1	Die Sicherheitsmerkmale des Geräts bieten hohen Schutz gegen Angriffe; ein Angriff ist sehr unwahrscheinlich.

Tabelle 0-6: Zuordnung von Punktwerten zu Wahrscheinlichkeitswerten

Eine Auswahl an beispielhaften vollständig evaluierten Angriffsvektoren ist in **Tabelle 0-7** gegeben.

Angriffs-ID	Angriffsvektor	Abgelaufene Zeit	Fachwissen	Wissen über das Messsystem	Zugriffsgelegenheiten	Ausrüstung	Begründung
Bsp. 1	Der Angreifer errät ein Administratorpasswort mit vier Ziffern, indem er willkürliche Zahlenkombinationen eingibt.	1	0	0	0	0	Mutmaßlicher Angreifer: Nutzer des Geräts. Die Passworteingabe dauert maximal 10 Sekunden, alle 10.000 Kombinationen können in 100.000 Sekunden = 1,15 Tagen getestet werden. Jeder Laie, der einen PC bedienen kann, kann diesen Angriff ausführen. Da der Nutzer der Angreifer ist, ist die Zugriffsgelegenheit unbeschränkt. Besondere Ausrüstung wird nicht benötigt.
Bsp. 2	Die Angreiferin erstellt ein gefälschtes Messergebnis aus Messdatensätzen, die von einem CRC32 geschützt sind und mit einem geheimen Startwert berechnet werden.	0	3	3	0	0	Mutmaßliche Angreiferin: Kundin. Da CRC eine lineare logische Operation auf binären Vektoren ist, erzeugt eine XOR-Verbindung von zwei Datensätzen automatisch einen dritten Datensatz mit einer korrekten CRC. Die XOR-Verbindung kann mit Standardsoftware von jeder fähigen Nutzerin berechnet werden. Um zwei oder mehr Datensätze zu erlangen, ist für die Kundin keine Zugriffsgelegenheit nötig. Die Art der Prüfsumme (CRC32) ist in der Bedienungsanleitung beschrieben.
Bsp. 3	Der Angreifer berechnet den geheimen CRC32-Startwert aus den erlangten Messdatensätzen, die jeweils durch Nutzung des geheimen Startwertes erzeugt worden sind.	1	6	3	4	4	Mutmaßlicher Angreifer: Kunde. Ein CRC32-Startwert hat eine Länge von 32 Bits. Daraus folgt, dass 2^32 = 4.3*10^9 mögliche Startwerte existieren. Jeder Angreifer mit Programmierfähigkeiten (Experte) könnte ein Programm schreiben (spezielle Ausrüstung), um den korrekten Startwert durch Brute-Force-Suche innerhalb weniger Stunden zu finden. Zur Überprüfung, ob der kor-

							rekte Startwert gefunden wurde, sind mehrere tausend Datensätze inklusive Prüfsummen nötig. Diese zu erlangen, erfordert eine moderate Zugriffsgelegenheit. Die Art der Prüfsumme (CRC32) ist in der Bedienungsanleitung beschrieben.

Tabelle 0-7: Beispielhaft evaluierte Angriffsvektoren

Anhang C Berichtsformat

1) Kurzbeschreibung der bewerteten [Messgerätebauart] [Name].

ID	Komponententyp	Beschreibung
C1	Kommunikationsschnittstelle	
U1	Nutzerschnittstelle	
S1	Speicherung von Messdaten	
X1	Übertragung von Messdaten	
P1	Speicherung von rechtlich relevanter Software	

Tabelle 1: Liste von Datenübertragungen, Speichergeräten, Nutzer- und Kommunikationsschnittstellen.

2) Checkliste für High-Level-Bedrohungen

Hier muss die ausgefüllte Checkliste aus Anhang A eingefügt werden.
0

3) Zusätzliche gerätespezifische Angriffsvektoren

Hier muss eine geprüfte Erklärung darüber abgegeben werden, weshalb gerätespezifische Angriffsvektoren betrachtet werden müssen oder nicht. In Fällen, in denen zusätzliche gerätespezifische Bedrohungen betrachtet werden müssen (siehe 3.3.4), müssen die folgenden Tabellen ausgefüllt werden.

a) Liste zusätzlicher Bedrohungen, die durch gerätespezifische Angriffsvektoren ermöglicht werden

ID	Ziel der Bedrohung	Beschreibung
T1		
T2		
T3		

Tabelle 2: Liste betrachteter Bedrohungen.

Anmerkung: Ziele (Tx.x)) aus Anhang A können als Bedrohungen für Risikoklasse C und niedriger genutzt werden.

b) Liste bewerteter Angriffsvektoren (AVxy), die eine Bedrohung Tx ermöglichen.

Angriffs-ID	Beschreibung des Angriffsvektors	Abgelaufene Zeit	Fachwissen	Wissen über das Messsystem	Zugriffsgelegenheiten	Ausstattung	Gesamt	Auswirkung	Begründung
AVx1									
AVx2									
AVx3									

Tabelle 3: Bewertung der elementaren Angriffsvektoren.

Wenn Angriffsvektoren mithilfe eines Angriffswahrscheinlichkeitsbaums kombiniert werden müssen, um eine zusätzliche Bedrohung zu realisieren, müssen diese Bäume hier zur Verfügung gestellt werden.

c) Liste des Wahrscheinlichkeitswerts, der zugewiesenen Auswirkung und des endgültigen Risikowertes für jeden Angriffsvektor (AVxy)

Angriffs-ID	Gesamt	Wahrschein-lichkeitswert	Auswirkung	Risiko
AVx1				
AVx2				
AVx3				

Tabelle 4: Jedem Angriffsvektor zugewiesener Risikowert.

Anmerkung: Die Regeln der Zuweisung von Gesamt-, Auswirkungs- Wahrscheinlichkeitswert und Risiko sind in Kapitel 4 beschrieben.

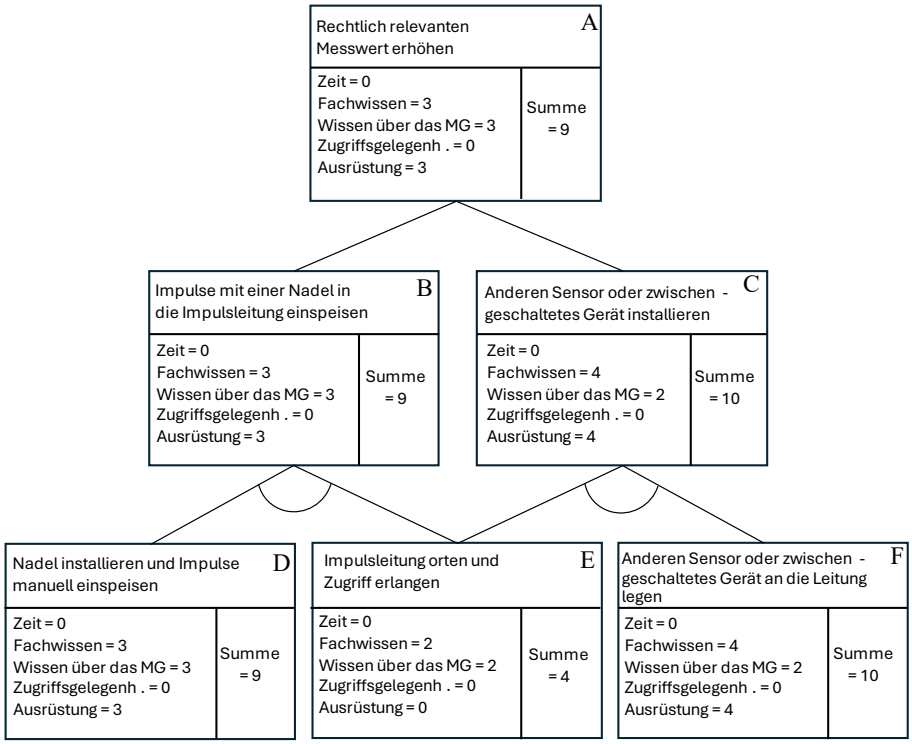
4) Schlussfolgerung

Hier muss eine Stellungnahme dazu geschrieben werden, ob die identifizierten Risiken für das Messgerät im akzeptablen Rahmen liegen oder ob Gegenmaßnahmen implementiert werden müssen.

Anhang D Bewertung von Angriffswahrscheinlichkeits-bäumen

Die grundlegendsten Eigenschaften eines jeden Angriffsbaums können folgendermaßen zusammengefasst werden: Während der Wurzelknoten eines solchen Baumes das Hauptziel eines Angreifers darstellt, können die untergeordneten Knoten als unterteilte Ziele angesehen werden, die erreicht werden müssen, um besagtes Hauptziel zu erreichen. Dieser Interpretation folgend, stehen die Blattknoten eines Angriffsbaums für Elementarangriffe, die nicht weiter unterteilt werden können. Ein beispielhafter Baum, der nur aus sechs Knoten besteht, ist in zu sehen.

Abbildung 0-1: Beispielhafter Angriffswahrscheinlichkeitsbaum für ein Taxameter,



das über eine Impulsleitung an einen Wegstreckensignalgeber am Rad eines Taxis verbunden ist.

In dem Beispiel sind die möglichen Strategien für einen Angriff dargestellt,
der die Fahrtkosten, die vom Taxameter berechnet werden, manipulieren soll. Bevor auf die Bedeutung des gezeigten Baums eingegangen wird, müssen die Besonderheiten der grafischen Repräsentation erläutert werden:

Untergeordnete Knoten sind immer logisch entweder als UND- oder ODER-Ausdruck verbunden. Die UND-Aussage ist durch einen Bogen illustriert, der die entsprechenden untergeordneten Knoten verbindet und anzeigt, dass alle Teilangriffe implementiert werden müssen, um den Angriff ausführen zu können, der mit dem übergeordneten Knoten assoziiert ist. Wenn andererseits untergeordnete Knoten alternative Wege anzeigen, um das übergeordnete Ziel zu erreichen, sind sie durch eine ODER-Aussage verbunden. In diesem Fall wird kein Bogen gezeichnet.

Es gibt keine Garantie dafür, dass ein Angriffsbaum ein binärer Baum sein wird. Werden jedoch mehr als zwei untergeordnete Knoten identifiziert, können sie immer in eine binäre Struktur umgeformt werden, indem sie so lange paarweise in unterge-

ordnete Ziele zusammengeführt werden, bis nur noch zwei untergeordnete Knoten übrigbleiben. Der beispielhafte Angriffsbaum in stellt Angriffe auf den analogen Signalpfad zwischen Wegstreckensignalgeber am Rad des Taxis und Taxameter dar.

In diesem Szenario existieren zwei bekannte Angriffsvektoren:

- das manuelle Einspeisen zusätzlicher Impulse in die Impulsleitung mithilfe einer Nadel (Knoten (B) in) und
- die Installation eines anderen Wegstreckensignalgebers oder eines anderen zwischengeschalteten Geräts in den Signalpfad (Knoten (C) in).

Da diese beiden Angriffsvektoren Alternativen zueinander sind, werden sie mit dem übergeordneten Knoten (A) durch eine ODER-Verbindung, dargestellt durch zwei einfache Linien, verbunden. Ein Bogen zwischen zwei oder mehr Linien würde eine UND-Verbindung repräsentieren. Solche UND-Aussagen können auf der nächsten Stufe des Angriffsbaums gefunden werden. Das manuelle Einspeisen zusätzlicher Impulse in die Impulsleitung mithilfe einer Nadel (Knoten (B)) bedarf sowohl des Zugangs zur Impulsleitung (Knoten (E)) als auch des manuellen Einspeisens der Impulse selbst (Knoten (D)). Wird ein anderer Sensor installiert (Knoten (C)), ist wieder der Zugang zur Impulsleitung notwendig (Knoten (E)). Zusätzlich muss die Installation selbst realisiert werden (Knoten (F)). Auch hier sind die Knoten (E) und (F) durch eine UND-Aussage verbunden. Interessanterweise spielt Knoten (E) in beiden Angriffen eine Rolle und bietet sich somit als möglicher Einstiegspunkt für eine Gegenmaßnahme an. Um den Wahrscheinlichkeitswert der ursprünglichen Bedrohung (A) zu berechnen, werden den Blattknoten (D), (E) und (F) jeweils Punktwerte in den obengenannten fünf Kategorien zugewiesen. Man kann sehen, dass das Zusammenführen von zwei Knoten zu einem Knoten keinen Einfluss auf die mathematischen Eigenschaften des lokalen Teilbaums hat, beispielsweise auf die Eintrittswahrscheinlichkeit. Daher liegt es im Ermessen der Prüferin bzw. des Prüfers, die Anzahl der Verfeinerungen eines Angriffs zu beschränken.

In der Praxis braucht ein Knoten keine weitere Verfeinerung, wenn der entsprechende Angriff aus einer einfachen technischen Aufgabe mit bekanntem Umfang und mit leicht zu bestimmenden Eigenschaften besteht. Jedem Knoten kann ein Satz vordefinierter Charakteristiken als Maßstab für die Eintrittswahrscheinlichkeit zugewiesen werden, z.B. abgelaufene Zeit, Fachwissen und Wissen über das Messsystem, Zugriffsgelegenheiten und Ausrüstung. Die Attribute jedes übergeordneten Knotens können bestimmt werden, indem die Informationen über die entsprechenden untergeordneten Knoten kombiniert werden. Es ist wichtig zu wissen, dass Knoten auch mehrmals innerhalb eines Baumes auftauchen dürfen. Es kann mehrere Kopien eines Knotens geben, deren Attribute verbunden sind; dadurch kann es vorkommen, dass eine Änderung in einem Teil des Angriffsbaums eine Änderung an einem ganz anderen Teil bewirken kann. Die entstandenen Angriffswahrscheinlichkeitsbäume stellen sowohl die Angriffslogik als auch die Eintrittswahrscheinlichkeit (und letztlich das Risiko) eines zugeordneten Angriffs dar. Dies bedeutet, dass ein solcher Angriffsvektor nicht länger individuell bewertet wird, sondern dass nur die elementaren Angriffe an den Blattknoten geprüft werden. Dadurch wird die Möglichkeit einer falschen Bewertung eines Angriffs reduziert und es wird ermöglicht, Elementarangriffe für verschiedene Bedrohungen erneut zu nutzen.

Die Attribute der übergeordneten Knoten und schließlich des Wurzelknotens können von unten nach oben berechnet werden, indem folgende Regeln beachtet werden.

Um die Attribute den Baum aufwärts zu vergeben, werden Regeln vorgestellt, die speziell auf die Charakteristiken jedes einzelnen Attributs zugeschnitten sind:

- Abgelaufene Zeit
    - UND: Darstellung der Zeit in Punktwerten ist logarithmisch (1 für mehr als ein Tag, 2 für eine oder zwei Wochen, 19 für ein halbes Jahr). Die abgelaufene Zeit für zwei Angriffe zusammen kann abgeschätzt werden, indem das Maximum beider Zeiten gewählt wird.
    - ODER: Der Zeitwert, der mit dem kleineren Summenwert verbunden ist, wird gewählt.
- Fachwissen
    - UND: Normalerweise wird das Maximum beider Werte gewählt. Sollte Fachkenntnis von sowohl Hardware als auch Software (HW und SW) nötig sein, so werden die Werte mit einem Maximalwert von 8 addiert, siehe ISO/IEC 18045 [9].
    - ODER: Der Fachwissen-Wert, der mit dem kleineren Summenwert verbunden ist, wird gewählt.
- Wissen über das Messsystem
    - UND: Das Maximum beider Werte wird gewählt.
    - ODER: Der Wert, der mit dem kleineren Summenwert verbunden ist, wird gewählt.
- Zugriffsgelegenheiten
    - UND: Eine geringere Zugriffsgelegenheit (höherer Wert) für einen Knoten ist das relevante Limit. Daher wird das Maximum gewählt.
    - ODER: Der Zugriffsgelegenheitswert, der mit dem kleineren Summenwert verbunden ist, wird gewählt.
- Ausrüstung
    - UND: Der Maximalwert beider Ausrüstung-Scores wird gewählt, es sei denn, es wird Ausrüstung aus verschiedenen Bereichen (HW oder SW) benötigt. In diesem Fall werden die Scores laut ISO/IEC 18045 [9] addiert mit einem Maximum von 9.
    - ODER: Der Ausrüstung-Wert, der mit dem kleineren Summenwert verbunden ist, wird gewählt.