Physikalisch-Technische Bundesanstalt
Nationales Metrologieinstitut

Arbeitsgruppe 8.51 „Metrologische Software“ Stand: 23. Juni 2022

Merkblatt:
Risikoanalyse für Software – Handlungshilfe für Hersteller

1 Einleitung

Ziel dieses Merkblatts ist es, eine Handlungsempfehlung für Hersteller von Messgeräten bereitzustellen, die der Konformitätsbewertungsstelle der PTB ihre Messgeräte entweder zur Baumusterprüfung nach Modul B gemäß der europäischen Messgeräterichtlinie (MID) [1] oder nach Mess- und Eichgesetz (MessEG) [2] vorlegen. In beiden Rechtsrahmen wird vom Hersteller gefordert, zusätzlich zur Dokumentation des Messgeräts und der Software eine geeignete Risikobewertung des Geräts hinsichtlich der wesentlichen Anforderungen vorzulegen (Anhang I der MID [1] bzw. Anlage 2 zur Mess- und Eichverordnung (MessEV) [3]). Dieses Merkblatt erläutert ausführlich, wie das im WELMEC Leitfaden 7.6 [4] harmonisierte Risikobewertungsverfahren anzuwenden ist. Weitere Details zum Verfahren finden sich in der Originalpublikation [5].

Die Risikoanalyse wird in der MID [1] in den Modulen A, A2, B, D1, E1, F1, G, H und H1 explizit gefordert. Diese Regelung ist im § 10 MessEV [3] in Verbindung mit §§ 7 und 8 MessEV [3] in nationales Recht umgesetzt worden.

WELMEC Leitfaden 7.6 [4] bietet einen auf schützenswerten Gütern basierenden Ansatz zur Risikoanalyse. Schützenswerte Güter werden zunächst formalisiert aus den wortgleichen Anforderungen von MID [1] und MessEV [3] abgeleitet (siehe Abschnitt 2).

Für Messgeräte alle Risikoklassen (siehe WELMEC 7.2, Softwareleitfaden [6]) fordert der WELMEC Leitfaden 7.6 [4], dass der Hersteller (anhand einer ausführlichen Tabelle) nachweist, wie allgemeine Bedrohungen für schützenswerte Güter adressiert werden. Weitere Einzelheiten zu den allgemeinen Bedrohungen und der Tabelle finden sich in Abschnitt 3. Für Messgeräte der Risikoklassen D bis F fordert der WELMEC Leitfaden 7.6 [4] die Hersteller außerdem auf, zusätzliche bauartspezifische Bedrohungen zu identifizieren, die in einer separaten Risikoanalyse behandelt werden müssen. Das Verfahren zur Identifizierung und Bewertung dieser zusätzlichen Bedrohungen ist in Abschnitt 4 beschrieben.

2 Schützenswerte Güter

Jedes im Rahmen einer Konformitätsbewertung auf Grundlage der MID [1] bzw. des MessEG [2] geprüfte Messgerät muss die in Spalte 1 von Tabelle 1 aufgelisteten wesentlichen Anforderungen mit Bezug auf die Software erfüllen. Diese werden hier in Form von **schützenswerten Gütern** (Spalte 2) interpretiert, denen generische **Sicherheitseigenschaften** (Spalte 3) zugeschrieben werden, siehe [4].

Tabelle 1: Bezug zwischen den softwarebezogenen wesentlichen Anforderungen, den daraus abgeleiteten schützenswerten Gütern und diesen zugeschriebenen Sicherheitseigenschaften

Softwarebezogene wesentliche Anforderung im Anhang I der MID bzw. in Anlage 2 zur MessEV	Schützenswertes Gut	Sicherheitseigenschaft
7.6 Wenn ein Messgerät über zugehörige zusätzliche Software verfügt, die neben der Messfunktion weitere Funktionen erfüllt, muss die für die messtechnischen Merkmale entscheidende Software identifizierbar sein; sie darf durch die zugehörige zusätzliche Software nicht in unzulässiger Weise beeinflusst werden.	Identifikation der rechtlich relevanten Software	Verfügbarkeit, Integrität
	unzulässige Beeinflussung der rechtlich relevanten Software durch andere Software	Nichtverfügbarkeit[1]
8.1 Die messtechnischen Merkmale eines Messgeräts dürfen durch das Anschließen eines anderen Geräts, durch die Merkmale des angeschlossenen Geräts oder die Merkmale eines abgetrennten Geräts, das mit dem Messgerät in Kommunikationsverbindung steht, nicht in unzulässiger Weise beeinflusst werden.	unzulässige Beeinflussung der rechtlich relevanten Software über Kommunikations-schnittstellen	Nichtverfügbarkeit
8.3 Software, die für die messtechnischen Merkmale entscheidend ist, ist entsprechend zu kennzeichnen und zu sichern. Die Identifikation der Software muss auf einfache Weise vom Messgerät zur Verfügung gestellt werden. Eventuelle Eingriffe müssen über einen angemessenen Zeitraum nachweisbar sein.	Anzeige der Softwareidentifikation	Verfügbarkeit
	Nachweis eines Eingriffes	Verfügbarkeit, Integrität
8.2 Eine für die messtechnischen Merkmale entscheidende Baueinheit ist so auszulegen, dass sie gesichert werden kann. Die vorgesehenen Sicherungsmaßnahmen müssen den Nachweis eventueller Eingriffe ermöglichen. 8.4 Messdaten, Software, die für die messtechnischen Merkmale entscheidend ist, und messtechnisch wichtige Parameter, die gespeichert oder übertragen werden, sind angemessen gegen versehentliche oder vorsätzliche Verfälschung zu schützen.	Messergebnisse	Integrität, Authentizität
	rechtlich relevante Software, die für den Messzweck entscheidend ist	Integrität, Authentizität
	messtechnisch wichtige Parameter	Integrität, Authentizität
10.1 Die Anzeige des Ergebnisses erfolgt in Form einer Sichtanzeige oder eines Papierausdrucks.	Anzeige des Messergebnisses	Verfügbarkeit, Integrität
10.2 Die Anzeige des Ergebnisses muss klar und eindeutig sowie mit den nötigen Markierungen und Aufschriften versehen sein, um dem Benutzer die Bedeutung des Ergebnisses zu verdeutlichen. Unter normalen Einsatzbedingungen muss ein problemloses Ablesen des dargestellten Ergebnisses gewährleistet sein.	Klare und eindeutige Anzeige des Ergebnisses, Markierungen und Aufschriften, die ein Messergebnis begleiten	Verfügbarkeit, Integrität
11.1 Ein Messgerät, das nicht der Messung von Versorgungsleistungen dient, muss das Messergebnis und die zur Bestimmung eines bestimmten Geschäftsvorgangs erforderlichen Angaben dauerhaft aufzeichnen, wenn a) die Messung nicht wiederholbar ist und b) das Messgerät normalerweise dazu bestimmt ist, in Abwesenheit einer der Parteien benutzt zu werden. 11.2 Darüber hinaus muss bei Abschluss der Messung auf Anfrage ein dauerhafter Nachweis des Messergebnisses und der zur Bestimmung eines bestimmten Geschäftsvorgangs erforderlichen Angaben zur Verfügung stehen.	dauerhaft gespeichertes Messergebnis und zusätzlich erforderliche Angaben	Verfügbarkeit

[1] Der Begriff „Nichtverfügbarkeit“ muss hier wie folgt verstanden werden: „Es darf keine unzulässige Beeinflussung der rechtlich relevanten Software vorhanden sein.“

3 Allgemeine Bedrohungen schützenswerter Güter mit Angriffsvektoren auf hoher Ebene

WELMEC Leitfaden 7.6 [4] enthält für jedes schützenswerte Gut eine Liste generischer Bedrohungen mit zugehörigen Angriffsvektoren auf hoher Ebene, denen das Messgerät entgegenwirken muss, um die Einhaltung der grundlegenden Anforderungen nach MID [1] nachzuweisen. Der Leitfaden fasst diese wie folgt zusammen:

> *"An attacker attacks the software, parameters, measurement result, stored result or indication through*
> - *Other software*
> - *User Interface*
> - *Communication interface*
>   - *Direct influence by connecting a device to the measurement instrument*
>   - *Through transmission (including software downloads)*
> - *Connecting a device to the instrument*
> - *Replacing hardware.*
>   - *Replacing complete parts*
>   - *Replacing components*
> - *Replacing software (for Type U instruments*)"*

Um Herstellern dabei zu helfen, jeden Angriffsvektor auf hoher Ebene für jede generisch Bedrohung anzugeben, wurde eine ausführliche Tabelle in Form eines Anhangs zu WELMEC Leitfaden 7.6 [4] veröffentlicht:
https://www.welmec.org/welmec/documents/guides/7.6/2021/WELMEC_Guide_7.6_v2021_Annex_1_Riskanalysis.xlsx

Es kann davon ausgegangen werden, dass für Messgeräte bis Risikoklasse C eine vollständig ausgefüllte Tabelle als ausreichende Risikoanalyse dient. Ein Auszug aus der Tabelle ist in *Abbildung **1*** unten dargestellt.

1.1.1 Through other software

Threat nr.	Asset nr.	Asset	Countermeasure	Break down threat	Passed / Failed	Remarks
T.1	1	**Legally relevant software**				
T.1.1	**Extension S**	Inadmissible influence **Through other software**				
T.1.1.1	**P2, U2**	**Identification**				
T.1.1.1.1		Availability				
T.1.1.1.2		Integrity				
T.1.1.1.3		Authenticity				
T.1.1.2		**Evidence of an intervention**				
T.1.1.2.1		Availability				
T.1.1.2.2		Integrity				
T.1.1.2.3		Authenticity				
T.1.1.3		**Adequate protection with respect to**				
T.1.1.3.1		Availability				
T.1.1.4		**Combined evaluation (T.1.1.1-T.1.1.3)**				

Abbildung 1: Liste generischer Bedrohungen für Software mit Angriffsvektoren auf hoher Ebene aus Anhang I in **[4]**

Spalte 1 in der Tabelle listet einfach eine Bedrohungs-ID auf. Verweise auf die Anforderungen aus dem WELMEC 7.2 Softwareleitfaden [6] sind in Spalte 2 angegeben. Der Name des schützenswerten Guts und die zugehörige Sicherheitseigenschaften sind in Spalte 3 angegeben. Die Hersteller müssen die gesamte Tabelle ausfüllen, indem sie die Gegenmaßnahmen für jede aufgelistete Bedrohung (4. Spalte der Tabelle) angeben und in Spalte 5 Einzelheiten darüber angeben, wie die Bedrohung umgesetzt werden könnte. Spalte 6 ist für die Konformitätsbewertungsstelle vorgesehen, Spalte 7 kann für zusätzliche Anmerkungen verwendet werden.

4 Identifikation zusätzlicher Bedrohungen und möglicher Angriffsszenarien

4.1 Grundkonzept der Risikoanalyse

Die Norm ISO/IEC 27005 [7] definiert den Risikobegriff als eine Kombination des Schadens, der aus einem unerwünschten Ereignis (Bedrohung) resultiert, und der Eintrittswahrscheinlichkeit der Bedrohung. Das mit einer Bedrohung verbundene Risiko lässt sich somit auch mit Hilfe der folgenden Formel abbilden:

$$\text{Risiko} = \text{Schaden} \times \text{Eintrittswahrscheinlichkeit}$$

Im Rahmen des gesetzlichen Messwesens besteht ein Schaden in einer Verletzung der wesentlichen Anforderungen. Die wesentlichen Anforderungen sind als Ausprägung der Schutzziele der MID [1] zu sehen (unter Berücksichtigung von [8]).

Es wird hier hinsichtlich der **Schwere des Schadens** nur zwischen zwei Kategorien unterschieden:

a. Der aus einer Bedrohung resultierende Schaden soll nur dann als gering angesehen werden (Faktor $\frac{1}{3}$), wenn eine Bedrohung nur einmalig und kurzzeitig eine grundlegende Anforderung verletzt.
b. In allen anderen Fällen wird ein Schadensfaktor von 1 angenommen.

4.2 Identifizierung von Bedrohungen und Angriffsvektoren

Jede Verletzung der Sicherheitseigenschaft eines schützenswerten Guts stellt im Kontext dieses Merkblatts eine relevante Bedrohung dar. Es ist anhand des zur Konformitätsbewertung vorgelegten Messgeräts bzw. der dazugehörigen Dokumentation anzugeben, welche Bedrohungen (Verletzung der Sicherheitseigenschaften der schützenswerten Güter) ggf. durch gezielte technische Schritte realisierbar sind. Der Hersteller wird gebeten, für jede Sicherheitseigenschaft eines schützenswerten Guts anzugeben, welche Schritte/Handlungen theoretisch notwendig wären, damit die geforderte Eigenschaft verletzt wird. Gegebenenfalls ist zu begründen, inwiefern eine Verletzung einer Sicherheitseigenschaft grundsätzlich ausgeschlossen werden kann. Quellen aktueller Angriffsszenarien z.B. für netzangebundene Messgeräte finden sich bspw. unter *https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment* oder unter *https://cve.mitre.org/*.

4.3 Bestimmung der Eintrittswahrscheinlichkeit

Der Hersteller muss für jedes realisierbare identifizierte Angriffsszenario abschätzen, welche Voraussetzungen ein möglicher Angreifer für einen erfolgreichen Angriff besitzen muss. Empfehlenswert ist dabei eine Abschätzung nach den folgenden fünf Kriterien:

1. benötigte Zeit (0-19 Punkte)
2. erforderliche Expertise (0-8 Punkte)
3. Detailkenntnisse des Messsystems (0-11 Punkte)
4. erforderliches Zugriffszeitfenster (0-10 Punkte)
5. benötigtes Equipment (0-9 Punkte)

Dabei soll für jedes Kriterium eine Punktzahl vergeben werden, die sich nach den in Anhang B beigefügten Tabellen richtet. Basierend auf der Summe der Punkte wird jedem Angriff dann anhand der folgenden Tabelle ein Wahrscheinlichkeitsscore als Maß für die Eintrittswahrscheinlichkeit zugeordnet. Details zu dem Bewertungsschema finden sich in der Norm ISO/IEC 18045 "Information technology – Security techniques - Methodology for IT security evaluation" [9], Teil 2, B.4.2.2 ff. Ein Beispiel findet sich in Anhang A.

Tabelle 2: Punktebewertung des Angriffsszenarios nach **[9]**

Summe der Punkte	Widerstandsfähigkeit des Geräts	Wahrscheinlichkeitsscore
0-9	Ohne Bewertung	5
10-13	Grundschutz	4
14-19	Erweitert	3
20-24	Moderat	2
>24	Hoch	1

4.4 Bestimmung des Schadens

Sollte eine Bedrohung sich auf unbegrenzt viele zukünftige oder vergangene Messungen auswirken, so ist ein Schaden von 1 anzusetzen. Sollten nur einzelne Messungen betroffen sein, so ist ein Schaden von $\frac{1}{3}$ anzunehmen.

4.5 Bestimmung des Risikos

Abschließend wird der ermittelte Wahrscheinlichkeitsscore unter Berücksichtigung des ermittelten Schadens in ein Risiko überführt. Dazu werden Schaden und Eintrittswahrscheinlichkeit miteinander multipliziert. Abschließend wird ggf. auf den nächsten ganzzahligen Wert gerundet. Eine detaillierte Beschreibung des gesamten Verfahrens mit weiteren Beispielen findet sich in [5].

4.6 Konsequenzen

Im Regelfall müssen alle Bedrohungen mit einem Risiko von 4 oder 5 durch technische oder organisatorische Maßnahmen abgemildert werden, bis nach einer neuerlichen Bewertung das Risiko im Bereich 1 bis 3 liegt.

5 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 96/149,* 29. März 2014.

[2] „Gesetz über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen (Mess- und Eichgesetz – MessEG),“ *Bundesgesetzblatt, Jahrgang 2013 Teil 1 Nr. 43,* Juli 2013, zuletzt geändert am 11. April 2016.

[3] „Verordnung über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt sowie über ihre Verwendung und Eichung (Mess- und Eichverordnung – MessEV),“ *Bundesgesetzblatt, Jahrgang 2014 Teil 1 Nr. 58,* Dezember 2014, zuletzt geändert am 11. August 2017.

[4] WELMEC, *WELMEC Guide 7.6: Software Risk Assessment for Measuring Instruments,* 2021.

[5] M. Esche und F. Thiel, „Software Risk Assessment for Measuring Instruments in Legal Metrology,“ in *Proceedings of the Federated Conference on Computer Science and Information Systems, Volume 5*, Lodz, Polen, September 2015, DOI: *http://dx.doi.org/10.15439/978-83-60810-66-8*, ISSN 2300-5963, (2015).

[6] WELMEC, *WELMEC 7.2, Softwareleitfaden (Europäische Messgeräterichtlinie 2014/32/EU),* 2020.

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

[8] „The 'Blue Guide' on the implementation of EU product rules,“ Council of the European Union, Version 1.1, Juli 2015.

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

Anhang A: Beispielhafte Risikoanalyse einer gerätespezifischen Bedrohung

Betrachtet werde ein Beispielgerät auf Basis eines Universalcomputers (PC), das über einen eichpflichtigen Messwertspeicher verfügt. Dieser Speicher sei in Form einer Textdatei realisiert, auf die nur die rechtlich relevante Applikation sowohl lesend als auch schreibend zugreifen darf. Die Zugriffskontrolle werde mit Betriebssystemmitteln realisiert und sei über ein geheimes Administratorpasswort (hier: 4 Ziffern) gesichert. Ein möglicher Angriff auf die Verfügbarkeit der gespeicherten Messergebnisse besteht folglich darin, dass ein Angreifer durch Ausprobieren das richtige Passwort errät und dann die entsprechende Textdatei löscht. Das Messgerät sei für den Verwender uneingeschränkt verfügbar. In diesem Beispiel ist das schützenswerte Gut ein gespeichertes Messergebnis. Die dazugehörige Sicherheitseigenschaft ist Verfügbarkeit.

Bedrohung

Der Verwender mit gewöhnlichen Nutzerrechten verletzt die Verfügbarkeit der gespeicherten Messergebnisse.

Angriffsszenario

Der Verwender errät das Administratorpasswort durch Ausprobieren beliebiger vierstelliger Zahlenkombinationen und löscht anschließend die Textdatei.

Bewertung

- **Benötigte Zeit:** Es gibt 10^4 = 10.000 verschiedene mögliche vierziffrige Passwörter. Wenn angenommen wird, dass man zur Eingabe eines vierziffrigen Passworts inklusive Passwortüberprüfung durch das Gerät maximal 10 Sekunden benötigt, lassen sich alle 10.000 Kombinationen in 100.000 Sekunden = 27,78 Stunden = 1,15 Tage ausprobieren. Selbst wenn der Angreifer täglich nur 4 Stunden lang nach der richtigen Kombination sucht, benötigt er dafür maximal 1,15×24/4 = 6,9 Tage. Im statistischen Mittel wird die richtige Kombination schon nach der Hälfte der durchprobierten Passwörter, also nach 3,5 Tagen, gefunden werden. In jedem Fall dauert die Suche nicht länger als eine Woche. Die zu vergebende Punktzahl ist also 1.
- **Benötigte Expertise:** Zum Erraten einer Ziffernkombination und zum Löschen einer Datei sind keinerlei Spezialkenntnisse notwendig. Dementsprechend kommt ein Laie als potenzieller Angreifer in Frage und es werden 0 Punkte für Expertise vergeben.
- **Benötigte Detailkenntnisse des Messsystems:** Zunächst muss der Angreifer in Erfahrung bringen, wo auf dem System die Messwerte gespeichert werden und feststellen, dass Sie nur unter Eingabe des Administratorpassworts verändert werden können. Bei den meisten Betriebssystemen, genügt allerdings das Auffinden der Datei, da dann beim Öffnen der Datei automatisch das Administratorpasswort abgefragt werden würde. Es sind also allenfalls eingeschränkt verfügbare Detailkenntnisse notwendig. Die zu vergebende Punktzahl ist also 3.
- **Erforderliches Zugriffszeitfenster:** Da der Verwender bei diesem Gerät als Angreifer in Frage kommt, hat er unbegrenzt Zugriff auf das System und läuft dabei nicht Gefahr entdeckt zu werden. Entsprechend sind hierfür 0 Punkte zu vergeben.
- **Benötigtes Equipment:** Es wird kein Equipment benötigt (0 Punkte).

Tabelle 3: Auswertung des Beispiels

Bedrohung	Angriffsszenario	Benötigte Zeit	Expertise	Detailkenntnisse des Messsystems	Erforderliches Zugriffszeitfenster	Equipment	Summe	Wahrscheinlich-keitsscore	Schaden	Risiko
Der Verwender mit gewöhnlichen Nutzerrechten verletzt die Verfügbarkeit der gespeicherten Messergebnisse.	Der Verwender errät das Administratorpassworts durch Ausprobieren beliebiger vierstelliger Zahlenkombinationen und löscht anschließend die Textdatei.	1	0	3	0	0	4	5	1	5

Da die beschriebene Bedrohung Konsequenzen für alle vergangenen Messungen haben kann und der Schaden somit 1 ist, ist hier nach der Multiplikation von Wahrscheinlichkeitsscore und Schaden das ermittelte Risiko identisch mit dem berechneten Wahrscheinlichkeitsscore.

Konsequenzen

Im Regelfall müssen alle Bedrohungen mit einem Risiko von 4 oder 5 durch technische oder organisatorische Maßnahmen abgemildert werden, bis nach einer neuerlichen Bewertung das Risiko im Bereich 1 bis 3 liegt. Im genannten Beispiel würde eine Anpassung der Passwortlänge auf 6 Zeichen (100 mal mehr Kombinationen als für 4 Zeichen) dafür sorgen, dass für die benötigte Zeit (3,5 Tage * 100 = 350 Tage) 19 Punkte vergeben werden müssten. Damit ließe sich die Bedrohung mittels Erraten der richtigen Passwortkombination nahezu ausschließen.

Anhang B: Tabellen

Benötigte Zeit	Punkte
weniger als 1 Tag	0
weniger als 1 Woche	1
weniger als 2 Wochen	2
weniger als 1 Monat	4
weniger als 2 Monate	7
weniger als 3 Monate	10
weniger als 4 Monate	13
weniger als 5 Monate	15
weniger als 6 Monate	17
mehr als 6 Monate	19

Erforderliches Zugriffszeitfenster	Punkte
nicht notwendig/unbegrenzt	0
leicht	1
moderat	4
schwierig	10
unmöglich	**

**Wenn der Zugriff zeitlich ausgeschlossen werden kann, muss das entsprechende Angriffsszenario nicht weiter bewertet werden.

Erforderliche Expertise	Punkte
Laie	0
Sachkundiger	3
Experte	6
Experte auf mehreren Gebieten	8

Equipment	Punkte
Standard	0
spezialisiert	4
Spezialanfertigung	7
mehrere Spezialanfertigungen	9

Detailkenntnisse des Messsystems	Punkte
öffentlich	0
eingeschränkt	3
sensibel	7
kritisch	11