

WELMEC

European cooperation in legal metrology

Softwareleitfaden

(Europäische Messgeräte Richtlinie 2014/32/EU¹)



WELMEC

European cooperation in legal metrology

WELMEC steht für die Zusammenarbeit zwischen den Behörden des gesetzlichen Messwesens der Mitgliedstaaten der Europäischen Union und der EFTA. Das vorliegende Dokument ist einer von zahlreichen Leitfäden, die die WELMEC 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 als die aus Sicht der WELMEC beste Vorgehensweise, die verfolgt werden kann.

This document is a translation of WELMEC Guide 7.2: Software Guide (Measuring Instruments 2014/32/EU) also Applicable to 2004/22/EU (Version 2020).

The translation has been prepared by members of the WELMEC Working Group 7.

In case of any inconsistency between the terms of the translation and the terms of the original document the original document shall prevail.

Herausgeber:
WELMEC Sekretariat

E-Mail: secretary@welmec.org

Website: www.welmec.org

Softwareleitfaden

(Europäische Messgeräte-richtlinie 2014/32/EU)

Inhaltsverzeichnis

Vorwort	5
Einleitung	6
1 Begriffe	7
2 Verwendung des Leitfadens	11
2.1 Gesamtstruktur des Leitfadens	11
2.2 Auswahl der geeigneten Teile des Leitfadens	13
2.3 Arbeit mit einem Anforderungsblock	14
2.4 Arbeiten mit Checklisten	15
3 Definition von Risikoklassen	16
3.1 Allgemeiner Grundsatz	16
3.2 Beschreibung der Stufen von Gegenmaßnahmen für die Risikofaktoren	16
3.3 Ableitung von Risikoklassen	17
3.4 Interpretation der Risikoklassen	17
4 Basisanforderungen an die eingebettete Software in einem Messgerät mit zweckgebundener Hard- und Software (Typ P)	19
4.1 Technische Beschreibung	19
4.2 Spezifische Anforderungen an Typ P	20
5 Basisanforderungen an Software von Messgeräten mit Universalrechner (Typ U)	29
5.1 Technische Beschreibung	29
5.2 Spezifische Softwareanforderungen an Typ U	30
6 Anhang L: Langzeitspeicherung von Messdaten	40
6.1 Technische Beschreibung	40
6.2 Spezifische Softwareanforderungen an die Langzeitspeicherung	41
7 Anhang T: Messdatenübertragung über Kommunikationsnetze	51
7.1 Technische Beschreibung	51
7.2 Spezifische Softwareanforderungen an die Datenübertragung	52
8 Anhang S: Softwaretrennung	60
8.1 Technische Beschreibung	60
8.2 Spezifische Softwareanforderungen an die Softwaretrennung	61
9 Anhang D: Download von rechtlich relevanter Software	65
9.1 Technische Beschreibung	65
9.2 Spezifische Softwareanforderungen	65

10	Anhang I: Gerätespezifische Softwareanforderungen	70
10.1	Wasserzähler	72
10.2	Gaszähler und Mengenumwerter	84
10.3	Elektrizitätszähler für Wirkverbrauch	97
10.4	Wärmezähler.....	108
10.5	Messsysteme zur kontinuierlichen und dynamischen Mengenmessung von Flüssigkeiten außer Wasser	118
10.6	Waagen	120
10.7	Taxameter.....	126
10.8	Maßverkörperungen	131
10.9	Längenmessgeräte	132
10.10	Abgasanalysatoren	132
11	Muster eines Prüfberichts (einschließlich Checklisten)	133
11.1	In die Baumusterprüfbescheinigung einzubeziehende Informationen	133
11.2	Muster für den allgemeinen Teil des Prüfberichts.....	135
11.3	Anhang 1 des Prüfberichts: Checklisten zur Unterstützung der Wahl der geeigneten Anforderungssätze.....	138
11.4	Anhang 2 des Prüfberichts: Spezielle Checklisten für die entsprechenden technischen Teile	139
12	Querverweise zwischen den MID-Softwareanforderungen und MID-Artikeln bzw. -Anhängen.....	141
12.1	Softwareanforderungen und ihr Bezug zur MID.....	142
12.2	Auslegung von MID-Artikeln und -Anhängen durch MID- Softwareanforderungen	144
13	Verweise und Literatur	148
14	Revisionshistorie	149

Vorwort

Der vorliegende Leitfaden basiert auf dem “Software Requirements and Validation Guide”, Version 1.00, 29. Oktober 2004, der im Netzwerk “*MID-Software*” [1] des Europäischen Growth Programms entwickelt und als Ergebnis bereitgestellt worden ist. Das Netzwerk wurde von Januar 2002 bis Dezember 2004 von der EU-Kommission unter der Vorhabensnummer G7RT-CT-2001-05064 unterstützt.

Der Leitfaden hat rein empfehlenden Charakter und legt keine Beschränkungen oder zusätzliche technische Anforderungen fest, die über diejenigen in der europäischen Messgeräte Richtlinie (MID) hinausgehen. Alternative Ansätze können akzeptabel sein, jedoch stellt die in diesem Dokument bereitgestellte Anleitung nach Ansicht der WELMEC eine gute Praxis dar, der gefolgt werden sollte.

Obwohl sich der Leitfaden an die in die MID-Vorschriften aufgenommenen Messgeräten richtet, sind die Ergebnisse allgemeiner Natur und lassen sich darüber hinaus anwenden.

Die neueste Ausgabe 6 berücksichtigt die jüngsten Erfahrungen aus den Anwendungen des Leitfadens.

¹**Hinweis:** Die vorliegende Ausgabe des Leitfadens bleibt ebenfalls für die Richtlinie 2004/22/EC [3] gültig.

Einleitung

Dieses Dokument bietet all jenen eine technische Anleitung, die die Messgeräte Richtlinie (Measuring Instruments Directive, MID) [2] für mit Software ausgestattete Messgeräte anwenden. Es wendet sich an all jene, die am technischen Verständnis softwarebezogener Anforderungen der MID interessiert sind, insbesondere der wesentlichen Anforderungen in der MID, Anhang 1. Der Grad an Detailliertheit orientiert sich an den Bedürfnissen der Messgerätehersteller und der Benannten Stellen, die Konformitätsbewertungen von Messgeräten gemäß Modul B durchführen.

Wird nach diesem Leitfaden verfahren, ist davon auszugehen, dass die softwarebezogenen Anforderungen der MID eingehalten werden. Des Weiteren ist davon auszugehen, dass alle Benannten Stellen diesen Leitfaden als MID-konforme Auslegung hinsichtlich der Software akzeptieren. Um den Zusammenhang zwischen den in diesem Leitfaden aufgestellten Anforderungen und den entsprechenden MID-Anforderungen aufzuzeigen, wurde dem Leitfaden eine Querverweisliste als Anhang beigelegt (Kapitel 12).

Aktuelle Informationen zu den Leitfäden und zur Arbeit der WELMEC Arbeitsgruppe 7 sind auf folgender Webseite verfügbar: www.welmec.org.

1 Begriffe

In diesem Abschnitt werden die im Leitfaden benutzten Begriffe erläutert. Verweise auf einen Standard oder andere Quellen sind angegeben, wenn die Definition vollständig oder in wesentlichen Teilen daraus entnommen ist.

Akzeptable Lösung: Gestaltung oder Prinzip eines Softwaremoduls, einer Hardwareeinheit oder einer Funktionseinheit, bei der oder dem die zutreffende Anforderung als erfüllt angesehen wird. Eine akzeptable Lösung liefert ein Beispiel dafür, wie eine zutreffende Anforderung erfüllt werden kann. Sie schließt keine andere Lösungsmöglichkeit aus, die ebenfalls die Anforderung erfüllt.

Authentifizierung: Verifizierung der erklärten oder vorgeblichen Identität eines Benutzers, Prozesses oder Gerätes.

Authentizität: Die Eigenschaft echt, verifizierbar und vertrauenswürdig zu sein [4].

Basiskonfiguration: Aufbau des Messgerätes in Bezug auf die grundlegende Architektur. Es gibt zwei unterschiedliche Basiskonfigurationen: Messgeräte mit zweckgebundener Hard- und Software und Messgeräte mit Universalcomputer. Die Begriffe sind entsprechend auf *Teilgeräte* anwendbar.

Messgerät mit zweckgebundener Hard- und Software (Typ P): Ein *Messgerät*, das speziell für die anstehende Aufgabe entwickelt und gebaut wurde. Entsprechend ist die gesamte Anwendungssoftware für den Messzweck konstruiert. Für eine ausführlichere Definition siehe Unterkapitel 4.1.

Geschlossenes Netz: Ein Netz mit einer festen Anzahl von Teilnehmern mit bekannter Identität, Funktionalität und bekanntem Standort (siehe auch *Offenes Netz*).

Kommunikationsschnittstelle: Eine elektronische, optische, Funk- oder andere technische Schnittstelle, die es ermöglicht, Informationen automatisch zwischen Teilen von *Messgeräten*, *Teilgeräten* oder externen Geräten auszutauschen.

Gerätespezifischer Parameter: *Rechtlich relevanter* Parameter, dessen Wert vom einzelnen Gerät abhängt. Gerätespezifische Parameter umfassen Kalibrierparameter (z.B. Anpassung des Messbereichsumfangs oder andere Justierungen oder Korrekturen) und Konfigurationsparameter (z.B. Maximalwert, Minimalwert, Maßeinheiten usw.). Sie sind nur in einem speziellen Betriebsmodus des Gerätes justierbar oder auswählbar. Gerätespezifische Parameter können als solche eingestuft werden, die gesichert werden müssen (unveränderbar), und als solche, die zugänglich sind, während das Gerät in Gebrauch ist (setzbare Parameter).

Ereigniszähler: Ein Ereigniszähler registriert jede Änderung eines Parameterwertes. Es dient als Mittel zur Überwachung von Änderungen.

Ereignislogbuch: Ein Ereignislogbuch registriert jede Änderung der Software oder der Parameter. Es dient als Mittel zur Überwachung von Änderungen. Es registriert mindestens den Identifikator des geänderten Elementes sowie zusätzliche Informationen.

Integrierter Speicher: Nicht entfernbare Speicher, der Teil des Messgerätes ist, wie z.B. RAM, EEPROM oder Festplatte.

Integrität von Daten und von Software: Gewissheit, dass die Daten und die Software während ihrer Nutzung, Übertragung oder Speicherung nicht geändert wurden.

IT-Konfiguration: Aufbau des *Messgerätes* hinsichtlich der IT-Funktionen und Eigenschaften. In diesem Leitfaden werden vier IT-Konfigurationen betrachtet:

Langzeitspeicherung von Messdaten, Messdatenübertragung, Softwaredownload und Softwaretrennung (siehe auch *Basiskonfiguration*). Die Begriffe sind entsprechend auf *Teilgeräte* anwendbar.

Rechtlich relevanter Parameter: Parameter eines *Messgeräts* oder eines *Teilgeräts*, welcher der gesetzlichen Kontrolle unterliegt. Die folgenden rechtlich relevanten Parameter werden unterschieden: bauartspezifische Parameter und gerätespezifische Parameter.

Rechtlich relevante Software: Teil der Software, einschließlich der bauartspezifischen *Parameter*, der Funktionen ausführt, die der gesetzlichen Kontrolle unterliegen. Die übrige Software wird als rechtlich nicht relevant bezeichnet. Die vom Gerät erzeugten oder von rechtlich relevanter Software verarbeiteten Messdaten werden separat behandelt und gelten nicht als Teil der rechtlich relevanten Software.

Rechtlich relevanter Software-Identifikator: Die Identifikatoren der rechtlich relevanten Software werden als *rechtlich relevante Software-Identifikatoren* bezeichnet.

Langzeitspeicherung von Messdaten: Speicherung von Messdaten, um diese nach Abschluss der Messung für spätere, rechtlich relevante Zwecke bereitzuhalten

Messdaten: Rechtlich relevante Messwerte, die von Messgeräten erzeugt oder verarbeitet werden und mit physikalischen Einheiten oder anderen regelmäßig mit ihnen verbundenen Informationen, z.B. Zeitstempeln, begleitet werden, die sie metrologisch charakterisieren.

Messgerät: Jedes Gerät oder System mit einer Messfunktion. Der Vorsatz "Mess-" wird weggelassen, wenn Missverständnisse ausgeschlossen werden können. [2]

Messgeräte mit Universalcomputer (Typ U): *Messgerät*, das einen Allzweckrechner, gewöhnlich ein PC-basiertes System, enthält, um rechtlich relevante Funktionen auszuführen. Ein Typ-U-System ist anzunehmen, wenn die Bedingungen eines *Messgerätes mit zweckgebundener Hard- und Software (Typ P)* nicht erfüllt sind.

Offenes Netz: Ein Netzwerk mit beliebigen Teilnehmern (Geräten mit beliebigen Funktionen). Anzahl, Identität und Aufenthaltsort eines Teilnehmers können dynamisch und den anderen Teilnehmern unbekannt sein (siehe auch *Geschlossenes Netz*).

Betriebssystem: Eine Sammlung von Software und Firmware-Elementen, die die Ausführung von Computerprogrammen steuert und Dienste wie z.B. Betriebsmittelzuweisung, Auftragssteuerung, Eingabe-/Ausgabesteuerung und Dateiverwaltung in einem Computersystem zur Verfügung stellt [5].

Schnittstelle für die Software: Schnittstelle zwischen der rechtlich relevanten und der rechtlich nicht relevanten Software; Schutzbedingungen siehe Abschnitt S3.

Risikoklasse: Klasse von *Messgerätebauarten* mit fast identischen Risikobewertungen.

Softwaredownload: Der Prozess der automatischen Übertragung von Software unter Nutzung beliebiger technischer Mittel zu einem Ziel-Messgerät oder zu einer Hardware-Einheit von einer lokalen oder entfernten Quelle (z.B. austauschbare Speichermedien, tragbarer Computer, entfernte Computer) über beliebige Verbindungen (z.B. direkte Verbindungen, Netzwerke).

Software-Identifikator: Eine Folge von Zeichen, die die Software identifizieren. Der Identifikator wird logisch als Teil der Software angesehen.

Softwaretrennung: Die eindeutige Trennung von Software in *rechtlich relevante Software* und rechtlich nicht relevante Software. Wenn keine Softwaretrennung vorhanden ist, muss die gesamte Software als rechtlich relevant angesehen werden.

Teilgerät: Ein Hardwaregerät (Hardware-Einheit), das selbständig funktioniert und zusammen mit anderen Teilgeräten (oder einem *Messgerät*), mit denen es kompatibel ist, ein Messgerät bildet [MID, Artikel 4].

Messdatenübertragung: Übertragung von Messdaten zu einem entfernten Gerät über Kommunikationsnetze oder andere Medien, wo diese weiter verarbeitet und/oder für gesetzlich geregelte Zwecke verwendet werden.

TEC: Baumusterprüfbescheinigung.

Bauartspezifischer Parameter: *Rechtlich relevanter Parameter* mit einem Wert, der für alle Geräte dieses Typs gleich ist. Ein bauartspezifischer Parameter gilt als Teil der rechtlich relevanten Software.

Benutzerschnittstelle: Schnittstelle, die den Teil des Gerätes oder Messsystems bildet, der es ermöglicht, Informationen zwischen einem Menschen und dem Messgerät oder seinen Hardware- oder Softwareteilen auszutauschen, wie z.B. Schalter, Tastatur, Maus, Display, Monitor, Drucker, Touch-Screen.

Validierung: Bestätigung durch Prüfung und Beibringung von objektiven Belegen (d.h. von als richtig nachweisbaren Informationen, die auf Fakten aus Beobachtungen, Messungen, Tests usw. beruhen), dass die speziellen Anforderungen für die vorgesehene Nutzung erfüllt sind. Im vorliegenden Fall sind die Anforderungen, auf die Bezug genommen wird, jene der MID [2].

Die folgenden Definitionen sind sehr spezifisch. Sie werden nur in einigen Anhängen und für Risikoklasse D oder höher verwendet.

Hashalgorithmus: Algorithmus, der den Inhalt eines Datenblocks zu einer hexadezimalen Zahl definierter Länge (Hashcode) komprimiert, so dass die Änderung jedes Bits des Datenblocks in der Praxis zu einem anderen Hashcode führt. Hashalgorithmen werden so gewählt, dass theoretisch eine sehr geringe Wahrscheinlichkeit besteht, dass zwei verschiedene Datenblöcke denselben Hashcode haben.

Signaturalgorithmus: Ein kryptografischer Algorithmus, der unter Nutzung eines Signaturschlüssels einen Hashcode verschlüsselt und der es ermöglicht, diesen mit dem entsprechenden Entschlüsselungs-Signaturschlüssel wieder zu entschlüsseln.

Schlüssel: Eine passende Zahl oder Zeichenfolge, die zum Verschlüsseln und/oder Entschlüsseln von Informationen verwendet wird.

Public-Key-System: Ein Paar unterschiedlicher Schlüssel: Der eine wird als geheimer *Schlüssel* und der andere als öffentlicher Schlüssel bezeichnet. Um *Integrität* und *Authentizität* der Informationen zu überprüfen, wird der durch einen *Hashalgorithmus* erzeugte Hashwert der Informationen mit dem geheimen Schlüssel des Senders verschlüsselt, um die Signatur zu erzeugen; später entschlüsselt der Empfänger die Signatur mit Hilfe des öffentlichen Schlüssels des Senders.

Public-Key-Infrastruktur (PKI): Organisation zur Gewährleistung der Vertrauenswürdigkeit eines *Public-Key-Systems*. Dies schließt die Gewährung und Verteilung von digitalen Zertifikaten an alle Mitglieder ein, die am Informationsaustausch teilnehmen.

Zertifizierung von Schlüsseln: Prozess der Zuordnung eines Public-Key-Paares an eine Person, Organisation oder andere Instanzen.

Elektronische Signatur: Ein Kurzcode (die Signatur), der eindeutig einem Text, Datenblock oder Binärsoftwarefile zugeordnet ist, um die *Integrität* und *Authentizität* der gespeicherten oder übertragenen Daten nachzuweisen. Die Signatur wird mit Hilfe eines

Signaturalgorithmus und eines geheimen *Signaturschlüssels* erzeugt. Gewöhnlich besteht die Erzeugung einer elektronischen Signatur aus zwei Schritten: (1) zuerst komprimiert ein Hashalgorithmus den Inhalt der zu signierenden Informationen zu einem kurzen Wert, und (2) dann verarbeitet ein Signaturalgorithmus diese Zahl zur Erzeugung der Signatur mit dem geheimen Schlüssel.

Trust Centre: Eine Organisation, die Informationen über die Authentizität der öffentlichen Schlüssel von Personen oder anderen Instanzen, wie z.B. Messgeräten, vertrauenswürdig erzeugt, aufbewahrt und ausgibt.

2 Verwendung des Leitfadens

Dieses Kapitel beschreibt den Aufbau des Leitfadens und erläutert seine Verwendung.

2.1 Gesamtstruktur des Leitfadens

Der Leitfaden besteht aus einem strukturierten Satz von Anforderungsblöcken. Die Gesamtstruktur des Leitfadens berücksichtigt die Einteilung von Messinstrumenten in Basiskonfigurationen sowie die Einteilung in sogenannte IT-Konfigurationen. Dieser Anforderungssatz wird durch gerätespezifische Anforderungen ergänzt.

Demnach gibt es drei Arten von Anforderungssätzen:

1. Anforderungen für zwei Basiskonfigurationen von Messgeräten (als Typ P und U bezeichnet),
2. Anforderungen für vier IT-Konfigurationen (als Anhänge L, T, S und D bezeichnet),
3. Gerätespezifische Anforderungen (als Anhänge I.1, I.2, ... bezeichnet).

Der erste Anforderungstyp ist auf alle Geräte anwendbar. Der zweite Anforderungstyp betrifft die folgenden IT-Funktionen: Langzeitspeicherung von Messdaten (L), Messdatenübertragung (T), Softwaredownload (D) sowie Softwaretrennung (S). Jeder Satz dieser Anforderungen ist nur dann anwendbar, wenn die dazugehörige Funktion vorhanden ist. Der letzte Anforderungstyp bietet eine Sammlung weiterer, gerätespezifischer Anforderungen. Die Nummerierung ist an die Nummerierung der gerätespezifischen Anhänge der MID angelehnt. Der Satz von Anforderungsblöcken, der für ein bestimmtes Messgerät verwendet werden kann, ist schematisch in **Abbildung 2-1** dargestellt.

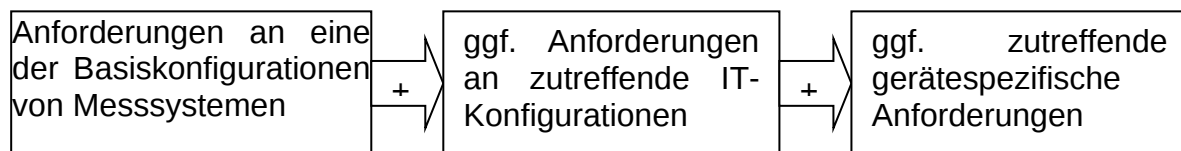


Abbildung 2-1: Arten von Anforderungssätzen, die auf ein Gerät angewandt werden sollten

Die Übersichten in der folgenden **Abbildung 2-2** zeigen, welche Anforderungssätze vorhanden sind.

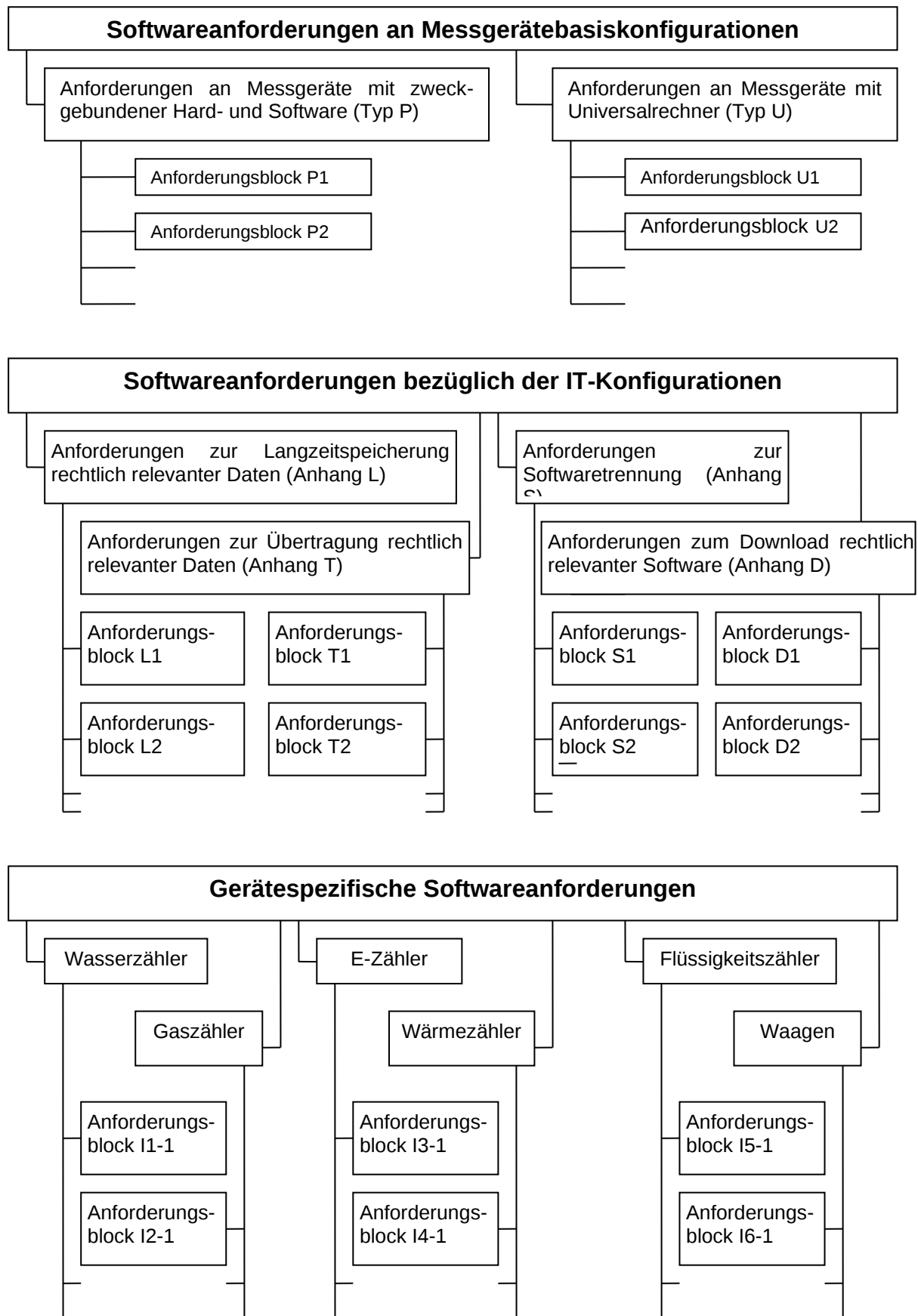


Abbildung 2-2: Übersicht über die Anforderungssätze

Neben der beschriebenen Struktur werden die Anforderungen des vorliegenden Leitfadens in Risikoklassen unterteilt. Sechs Risikoklassen mit steigender Gefährdungsvermutung, durchnummeriert von A bis F, werden eingeführt. Die niedrigste Risikoklasse A und die höchsten Risikoklassen E und F werden gegenwärtig nicht für Geräte verwendet, die unter die Bestimmungen der MID fallen. Sie sind Platzhalter für den Fall, dass sie in Zukunft notwendig werden. Die verbleibenden Risikoklassen B bis D decken alle Geräteklassen ab, die unter die Bestimmungen der MID fallen. Darüber hinaus bieten die Risikoklassen A bis F genügend Spielraum für den Fall geänderter Risikobewertungen. Die Klassen werden in Kapitel 3 des Leitfadens definiert, das jedoch nur informativen Charakter besitzt.

Jedes Messgerät muss in eine bestimmte Risikoklasse eingestuft werden, da die anzuwendenden besonderen Softwareanforderungen davon abhängen, zu welcher Risikoklasse das Gerät gehört.

2.2 Auswahl der geeigneten Teile des Leitfadens

Der vorliegende umfassende Softwareleitfaden ist auf eine Vielzahl von Geräten anwendbar. Der Leitfaden ist modular aufgebaut. Die entsprechenden Anforderungssätze lassen sich durch Beachtung folgenden Verfahrens leicht auswählen:

Schritt 1: Auswahl der Basiskonfiguration (P oder U)

Es braucht nur einer der beiden Anforderungssätze für Basiskonfigurationen angewendet zu werden. Dabei ist zu entscheiden, mit welcher Basiskonfiguration das Gerät übereinstimmt: als Messgerät mit zweckgebundener Hard- und Software (Typ P, siehe Unterkapitel 4.1) oder als Messgerät mit Universalcomputer (Typ U, siehe Unterkapitel 5.1). Falls nicht das gesamte Gerät, sondern nur ein Teilgerät des Geräts untersucht wird, entscheide man sich entsprechend für das jeweilige Teilgerät. Anzuwenden ist der vollständige Anforderungssatz, der zur jeweiligen Basiskonfiguration gehört.

Schritt 2: Auswahl der geeigneten IT-Konfigurationen (Anhänge L, T, S und D)

Die IT-Konfigurationen umfassen: Langzeitspeicherung von Messdaten (L), Übertragung von Messdaten (T), Softwaretrennung (S) und Download rechtlich relevanter Software (D). Die entsprechenden Anforderungssätze – die modularen Anhänge – sind voneinander unabhängig. Die ausgewählten Sätze hängen nur von der IT-Konfiguration ab. Wird ein Anforderungssatz ausgewählt, so muss er vollständig angewendet werden. Es ist zu entscheiden, welche modularen Anhänge gegebenenfalls anzuwenden sind (Abbildung 2-2).

Schritt 3: Auswahl von gerätespezifischen Anforderungen (Anhang I)

Mit Hilfe des jeweiligen gerätespezifischen Anhangs I.x ist auszuwählen, welche gerätespezifischen Anforderungen gegebenenfalls anzuwenden sind (Abbildung 2-2).

Schritt 4: Auswahl der geeigneten Risikoklasse (Anhang I)

Die Risikoklasse ist entsprechend der Definition in dem jeweiligen gerätespezifischen Anhang I.x, Unterkapitel I.x.6 auszuwählen. Dort kann die Risikoklasse einheitlich für

eine Messgeräteart definiert oder weiter in Kategorien, Anwendungsfelder usw. unterteilt werden. Sobald die entsprechende Risikoklasse identifiziert wurde, brauchen nur noch die jeweiligen Anforderungen und die Validierungsanleitung berücksichtigt zu werden.

2.3 Arbeit mit einem Anforderungsblock

Jeder Anforderungsblock enthält eine eindeutige Anforderung. Er besteht aus einem definierenden Text, Detaillierenden Anmerkungen, der bereitzustellenden Dokumentation, der Validierungsanleitung sowie Beispielen akzeptabler Lösungen (falls vorhanden). Der Inhalt eines Anforderungsblocks kann nach Risikoklassen unterteilt sein. Daraus ergibt sich die schematische Darstellung eines Anforderungsblocks in **Abbildung 2-3**.

Titel der Anforderung		
Hauptaussage der Anforderung		
Detaillierende Anmerkungen (Anwendungsbereich, zusätzliche Erklärungen, Ausnahmen usw.)		
Erforderliche Dokumentation (eventuell nach Risikoklassen unterteilt)		
Validierungsanleitung für eine Risikoklasse	Validierungsanleitung für eine andere Risikoklasse	...
Beispiel einer akzeptablen Lösung für eine Risikoklasse	Beispiel einer akzeptablen Lösung für eine andere Risikoklasse	...

Abbildung 3-3: Aufbau eines Anforderungsblocks

Der Anforderungsblock enthält den technischen Inhalt der Anforderung einschließlich der Validierungsanleitung. Er richtet sich in zwei Richtungen sowohl an den Hersteller als auch an die Benannte Stelle: (1) die Berücksichtigung der Anforderung als Mindestbedingung, und (2) kein Aufstellen von Forderungen über diese Anforderung hinaus.

Hinweise für den Hersteller:

- Erfüllen der Hauptaussage sowie der zusätzlichen Detaillierenden Anmerkungen.
- Bereitstellen der Dokumentation wie gefordert.
- Akzeptable Lösungen sind Beispiele, die die Anforderung erfüllen. Es besteht keine Verpflichtung, sie zu befolgen.
- Die Validierungsanleitung hat informativen Charakter.

Hinweise für Benannte Stellen:

- Erfüllen der Hauptaussage sowie der zusätzlichen Detaillierenden Anmerkungen.
- Befolgen der Validierungsanleitung.

- Bestätigen der Vollständigkeit der bereitgestellten Dokumentation.

2.4 Arbeiten mit Checklisten

Checklisten sind ein Mittel, um sicherzustellen, dass alle Anforderungen innerhalb eines Kapitels durch den Hersteller oder Prüfer abgedeckt wurden. Sie sind Teil des Baumusterprüfberichtes. Es ist zu beachten, dass die Checklisten nur zusammenfassenden Charakter haben und nicht zwischen Risikoklassen unterscheiden. Die Checklisten ersetzen nicht die Anforderungsdefinitionen. Die vollständigen Beschreibungen sind den Anforderungsblocks zu entnehmen.

Durchführung:

- Die Checklisten, die gemäß der in Schritt 1, 2 und 3 in Unterkapitel 2.2 beschriebenen Auswahl notwendig sind, sind zu sammeln.
- Die Checklisten sind durchzugehen und es ist zu prüfen, ob alle Anforderungen erfüllt wurden.
- Die Checklisten sind wie vorgegeben auszufüllen.

3 Definition von Risikoklassen

3.1 Allgemeiner Grundsatz

Die Anforderungen des vorliegenden Leitfadens werden nach (Software-) Risikoklassen unterschieden. In diesem Leitfaden beziehen sich die Risiken auf die Software des Messgeräts und nicht auf eine sonstige Komponente. Der Einfachheit halber wird der kürzere Begriff "Risikoklasse" verwendet. Jedes Messgerät muss in eine bestimmte Risikoklasse eingestuft werden, da die anzuwendenden spezifischen Softwareanforderungen auf die Risikoklasse zugeschnitten sind, zu welcher das Gerät gehört.

Die in diesem Leitfaden behandelten Software-Risiken bei Messgeräten werden hauptsächlich durch drei Risikofaktoren verursacht: unangemessener Softwareschutz, unangemessene Softwareprüfung und Abweichung vom Gerätetyp. Eine Risikoklasse ist eine Kombination von Stufen dieser drei Risikofaktoren, bei der sich die Definition der Risikofaktorstufen indirekt von der Definition der Stufen für die entsprechend notwendigen Gegenmaßnahmen ableitet. Für jeden dieser Risikofaktoren werden drei Stufen von Gegenmaßnahmen eingeführt – niedrig, mittel und hoch. Je höher das angenommene Risiko, desto höher die Stufe der zu ergreifenden Gegenmaßnahme.

3.2 Beschreibung der Stufen von Gegenmaßnahmen für die Risikofaktoren

Für die jeweiligen Stufen werden die folgenden Festlegungen benutzt:

Stufen für den Softwareschutz

- Niedrig:** Es sind keine besonderen Schutzmaßnahmen gegen vorsätzliche Veränderungen erforderlich.
- Mittel:** Die Software ist gegen vorsätzliche Veränderungen geschützt, die mit Hilfe von leicht verfügbaren und einfachen, gängigen Softwaretools (z.B. Texteditoren) vorgenommen werden können.
- Hoch:** Die Software ist gegen vorsätzliche Veränderungen geschützt, die mit Hilfe von anspruchsvollen Softwaretools (z.B. Debuggern oder Festplattenditoren, Softwareentwicklungstools usw.) vorgenommen werden können.

Stufen für die Softwareprüfung

- Niedrig:** Mit dem Gerät wird eine Standard-Baumusterfunktionsprüfung durchgeführt. Eine zusätzliche Softwareprüfung ist nicht erforderlich.
- Mittel:** Zusätzlich zu der Prüfung der Stufe "Niedrig" wird die Software auf Basis ihrer Dokumentation geprüft. Die Dokumentation beinhaltet die Beschreibung der Softwarefunktionen, die Parameterbeschreibung usw. Praktische Tests der softwaregestützten Funktionen (Stichproben) können ausgeführt werden, um die Plausibilität der Dokumentation und die Wirksamkeit der Schutzmaßnahmen zu überprüfen.
- Hoch:** Zusätzlich zu den Prüfungen der Stufe "Mittel" wird ein Tiefentest der Software ausgeführt, normalerweise auf Basis des Quellcodes.

Software-Konformitätsebene

- Niedrig:** Die rechtlich relevante Software einzelner Geräte gilt als konform mit der rechtlich relevanten Software des in der Prüfung befindlichen Gerätetyps, falls die Funktionalität der Software der technischen Dokumentation des Gerätetyps entspricht. Der Binärcode der Software selbst muss nicht unbedingt identisch mit der Software des Gerätetyps sein.
- Mittel:** Zusätzlich zur Konformitätsebene "niedrig" ist der Binärcode der rechtlich relevanten Software einzelner Geräte identisch mit der Software des in der Prüfung (oder Nachprüfung) befindlichen Gerätetyps. Software-Trennung ist erlaubt, wenn die Einschränkungen in Teil S des vorliegenden Leitfadens (Kapitel 8) erfüllt sind.
- Hoch:** Der Binärcode der vollständigen Software, die in den einzelnen Geräten implementiert ist, ist identisch mit der Software des in der Prüfung befindlichen Gerätetyps. Eine Softwaretrennung ist nicht mehr relevant.

3.3 Ableitung von Risikoklassen

Von den 27 theoretisch möglichen Stufenkombinationen sind nur 3 oder höchstens 6 von praktischem Interesse (Risikoklassen B, C, D, eventuell A, E und F). Sie decken alle Messgeräteklassen ab, die unter die Bestimmungen der MID fallen. Darüber hinaus bieten sie genügend Spielraum für den Fall geänderter Risikobewertungen. Die Klassen werden in der nachstehenden Tabelle definiert. Die Tabelle muss so interpretiert werden, dass eine bestimmte Risikoklasse mit Hilfe der entsprechenden Stufenkombination der notwendigen Gegenmaßnahmen definiert wird.

Risikoklasse	Softwareschutz	Softwareprüfung	Softwarekonformität
A	<i>niedrig</i>	<i>niedrig</i>	<i>niedrig</i>
B	<i>mittel</i>	<i>mittel</i>	<i>niedrig</i>
C	<i>mittel</i>	<i>mittel</i>	<i>mittel</i>
D	<i>hoch</i>	<i>mittel</i>	<i>mittel</i>
E	<i>hoch</i>	<i>hoch</i>	<i>mittel</i>
F	<i>hoch</i>	<i>hoch</i>	<i>hoch</i>

Tabelle 3-1: Definition der Risikoklassen

3.4 Interpretation der Risikoklassen

Risikoklasse A: Dies ist die niedrigste Risikoklasse überhaupt. Es sind keine besonderen Maßnahmen gegen vorsätzliche Softwareänderungen erforderlich. Die Softwareprüfung ist Teil der Funktionsprüfung des Geräts. Konformität mit der Dokumentation wird gefordert. Es wird nicht erwartet, dass irgendein Gerät als Gerät der Risikoklasse A

eingestuft wird. Durch Einführen dieser Klasse wird jedoch die entsprechende Möglichkeit offen gehalten

Risikoklasse B: Im Vergleich mit Risikoklasse A wird der Softwareschutz auf mittlerer Stufe gefordert. Dementsprechend wird die Prüfstufe auf die mittlere Stufe angehoben. Die Konformität bleibt gegenüber Risikoklasse A unverändert.

Die Softwareprüfung wird auf der Basis der Dokumentation ausgeführt. Folglich ermöglicht die Baumusterprüfbescheinigung verschiedene Umsetzungen der gleichen Dokumentation, wenn die Messgeräte auf den Markt gebracht werden¹.

Risikoklasse C: Im Vergleich mit Risikoklasse B wird die Konformitätsebene auf "mittel" angehoben. Dies bedeutet, dass der Binärcode der rechtlich relevanten Software einzelner Geräte identisch mit der Software des in der Prüfung befindlichen Gerätetyps ist. Die Schutz- und Prüfstufen bleiben gegenüber Risikoklasse B unverändert.

Risikoklasse D: Der wichtigste Unterschied zu Risikoklasse C ist das Anheben der Schutzstufe auf "hoch". Da die Prüfstufe unverändert bei "mittel" bleibt, muss eine ausreichend informative Dokumentation bereitgestellt werden, um die Eignung der ergriffenen Schutzmaßnahmen zu zeigen. Die Konformitätsebene bleibt gegenüber Risikoklasse C unverändert.

Risikoklasse E: Im Vergleich mit Risikoklasse D wird die Prüfstufe auf "hoch" angehoben. Die Schutz- und Konformitätsebenen bleiben unverändert.

Risikoklasse F: Die Stufen werden in jeder Hinsicht (Schutz, Prüfung und Konformität) auf "hoch" gesetzt. Der Unterschied zur Risikoklasse E ist, dass es keine rechtlich nicht relevante Software mehr gibt.

¹ Nachdem das Messgerät auf den Markt gebracht wurde, hängt die Erlaubnis für die Änderung von Software von nationalen Regelungen ab.

4 Basisanforderungen an die eingebettete Software in einem Messgerät mit zweckgebundener Hard- und Software (Typ P)

Der Satz spezifischer Anforderungen des vorliegenden Kapitels ist gültig für Messgeräte mit zweckgebundener Hard- und Software sowie für Teilgeräte und Teile gemäß WELMEC Leitfaden 8.8 (Modulare Bewertung von Messgeräten) mit zweckgebundener Hard- und Software. Die Gültigkeit erstreckt sich auf Teilgeräte und Baueinheiten, auch wenn sie im folgenden Text nicht fortwährend erwähnt wird. Die Bedingungen, unter denen Teilgeräte und Baueinheiten separat geprüft und die dazugehörigen Zertifikate akzeptiert werden können, sind jedoch nicht Bestandteil des vorliegenden Leitfadens. Wenn das Messgerät einen Universalcomputer (All-Zweck-PC) benutzt, gelten die spezifischen Anforderungen in Kapitel 5 (Typ-U-Gerät). Die spezifischen Anforderungen für Typ-U-Geräte müssen immer dann verwendet werden, wenn mindestens eins der folgenden technischen Merkmale der Messgeräte mit zweckgebundener Hard- und Software nicht vollständig zutrifft.

4.1 Technische Beschreibung

Ein Typ-P-Gerät ist ein Messgerät mit einem eingebetteten IT-System (z.B. ist es ein Mikroprozessor- oder Mikrocontroller-basiertes System). *Sämtliche Komponenten des IT-Systems können bewertet werden.*

Das eingebettete IT-System wird insbesondere wie folgt charakterisiert:

- Die Software ist ausschließlich für den Messzweck konstruiert. Zusätzliche Funktionen für die Sicherung von Software und Daten, für die Übertragung von Daten und den Download von Software gelten als für den Messzweck konstruiert.
- Die Benutzerschnittstelle ist für den Messzweck ausgelegt, d.h. sie wird normalerweise in einem Betriebsmodus verwendet, der der gesetzlichen Kontrolle unterliegt. Das Umschalten in einen Betriebsmodus, der nicht der gesetzlichen Kontrolle unterliegt, ist möglich.
- Ein Betriebssystem oder Subsysteme davon können vorhanden sein, wenn
 - die gesamte Kommunikation von der rechtlich relevanten Software gesteuert wird,
 - das Laden oder Ändern von Programmen, Parametern oder Daten oder sie das Laden oder Ändern von Programmen, Parametern oder Daten oder das Ausführen von Programmen nicht erlauben,
 - sie die Änderung der Umgebung der rechtlich relevanten Anwendung usw. nicht erlauben.

Dies beinhaltet, dass der Zugangsschutz voreingestellt sein muss und nicht Ergebnis einer entsprechenden nachfolgenden Konfiguration dieser Komponenten ist.

- Die Softwareumgebung ist unveränderlich; es gibt keine internen oder externen Mittel für die Programmierung oder Änderung der Software in ihrem eingebetteten Status. Softwaredownload ist erlaubt, wenn die spezifischen Anforderungen von Anhang D (Kapitel 9) beachtet werden.

4.2 Spezifische Anforderungen an Typ P

Risikoklassen B bis E		
P1: Dokumentation <i>Zusätzlich zur spezifischen Dokumentation, die für jede der folgenden Anforderungen erforderlich ist, muss die Dokumentation grundsätzlich Folgendes umfassen:</i> - Eine Beschreibung der rechtlich relevanten Software. - Eine Beschreibung der Genauigkeit der Messalgorithmen (z.B. Preisberechnungs- und Rundungsalgorithmen). - Eine Beschreibung der Benutzerschnittstelle, der Menüs und der Dialoge. - Der Software-Identifikator bzw. die Software-Identifikatoren der rechtlich relevanten Software. - Einen Überblick über die Systemhardware, z.B. Block-Schaltbild, Computerart(en), Netzwerkarten, usw. - Das Betriebshandbuch.		
Risikoklasse B	Risikoklasse C	Risikoklasse D
P2: Softwareidentifikation <i>Die rechtlich relevante Software muss eindeutig gekennzeichnet sein. Der bzw. die Identifikatoren müssen dauerhaft durch Gerät angezeigt oder auf Befehl oder während des Arbeitsablaufs angezeigt werden.</i>		
Detaillierende Anmerkungen: - Rechtlich relevante Software-Identifikatoren können unabhängig oder Teil gut strukturierter Identifikatoren sein. Im zweiten Fall müssen rechtlich relevante Software-Identifikatoren klar erkennbar sein. - Wenn verschiedene Softwareversionen gültige Umsetzungen desselben Baumusters sind (z.B. für Geräte in Risikoklasse B), dann müssen die rechtlich relevanten Software-Identifikatoren für jede Version eindeutig sein. - Die rechtlich relevanten Software-Identifikatoren werden als bauartspezifische Parameter betrachtet. - Die rechtlich relevanten Software-Identifikatoren müssen ohne ein zusätzliches Tool problemlos darstellbar sein. - Der bzw. die Identifikator(en) werden dauerhaft auf einem gesicherten Schild, auf Befehl oder beim Anlaufvorgang dargestellt.		
Erforderliche Dokumentation: Die Dokumentation muss Software-Identifikatoren auflisten und beschreiben, wie sie erzeugt, gesichert und dargestellt werden können und wie sie strukturiert sind, um sowohl zwischen rechtlich relevanten Software-Identifikatoren und anderen unterscheiden als auch ihre Eindeutigkeit bewerten zu können.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - ob in der Dokumentation rechtlich relevante Software-Identifikatoren angegeben sind - ob die Software, die rechtlich relevante Aufgaben ausführt, klar beschrieben ist, so dass nachvollziehbar ist, welcher rechtlich relevante Softwareteil von welchem Software-Identifikator abgedeckt wird - die Beschreibung der Visualisierung der rechtlich relevanten Software-Identifikatoren - ob alle rechtlich relevanten Software-Identifikatoren eindeutig sind (besonders bei Nachprüfungen). Funktionsprüfungen: - ob die rechtlich relevanten Software-Identifikatoren wie in der Dokumentation beschrieben sichtbar gemacht werden können - Es ist nachzuprüfen, ob die dargestellten rechtlich relevanten Software-Identifikatoren mit den in der Dokumentation angegebenen Identifikatoren identisch sind. - Die rechtlich relevanten Software-Identifikatoren sind von anderen Identifikatoren unterscheidbar		

Beispiel einer akzeptablen Lösung:

- a) eine Prüfsumme über den Code.
- b) jede beliebige Zeichenreihe, die evtl. von einer Versionsnummer ergänzt wird,
- c) jede beliebige Zahlen-, Buchstaben- oder andere Zeichenreihe,
- Wählt der Hersteller einen gemischten Identifikator für die rechtlich relevante und die rechtlich nicht relevante Software, ist eine einfache Lösung zur Unterscheidung der Identifikatoren die Verwendung von Platzhaltern in der Baumusterprüfbescheinigung, z.B. "abc1.xx", wobei "abc1" für die rechtlich relevante Software und "xx" als Platzhalter für rechtlich nicht relevante Software steht.

Zusätze für Risikoklasse E**Erforderliche Dokumentation**

Identisch mit den Risikoklassen B bis D

Validierungsanleitung

Identisch mit den Risikoklassen B bis D

Risikoklasse B**Risikoklasse C****Risikoklasse D****P3: Beeinflussung über Nutzerschnittstellen**

Die über die Benutzerschnittstelle eingegebenen Befehle dürfen die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten nicht unzulässig beeinflussen.

Detaillierende Anmerkungen:

1. Jeder Befehl muss eindeutig einer eingeleiteten Funktion oder Datenänderung zugeordnet werden können.
2. Befehle, die nicht dokumentiert sind, dürfen keine Wirkung auf die rechtlich relevanten Funktionen, gerätespezifischen Parameter und Messdaten haben.
3. Die jeweiligen Softwareteile, die die Befehle interpretieren, müssen als rechtlich relevante Software betrachtet werden.

Erforderliche Dokumentation:

Wenn das Gerät die Fähigkeit zum Befehlsempfang hat, muss die Dokumentation Folgendes enthalten:

- Beschreibung von Befehlen und ihrer Wirkung auf die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten.
- Eine Beschreibung, wie die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten vor dem Einfluss anderer Eingaben geschützt werden.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu überprüfen:

- ob alle dokumentierten Befehle zulässig sind, d.h. ob sie eine erlaubte Auswirkung auf rechtlich relevante Software, gerätespezifische Parameter und Messdaten haben.
- Prüfen der Schutzmaßnahmen gegen Einflüsse von anderen Eingaben.

Funktionsprüfungen:

- Durchführung praktischer Tests (Stichproben) mit dokumentierten Befehlen.
- Prüfen, ob es nicht dokumentierte Befehle gibt.

Beispiel einer akzeptablen Lösung:

Ein Softwaremodul empfängt und interpretiert Daten von der Schnittstelle. Dieses Modul ist Teil der rechtlich relevanten Software. Es leitet nur erlaubte Befehle zu den anderen rechtlich relevanten Softwaremodulen weiter. Alle unbekannten oder nicht erlaubten Abfolgen von Schalter- oder Tastenbetätigungen werden zurückgewiesen und haben keine Auswirkung auf die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (zusätzlich zur für Risikoklasse B bis D geforderten Dokumentation):

Quellcode der rechtlich relevanten Software.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D):

Auf Basis des Quellcodes ist zu überprüfen:

- ob die Software so aufgebaut ist, dass der Datenfluss bezüglich der Befehle eindeutig definiert ist und nur in der rechtlich relevanten Software realisiert wird.
- dass kein unzulässiger Datenfluss von der Benutzerschnittstelle zu den zu schützenden Bereichen erfolgt.
- ob die Befehle richtig entschlüsselt werden. Das Überprüfen kann mit Tools oder manuell erfolgen. den.

Risikoklasse B	Risikoklasse C	Risikoklasse D
P4: Einflussnahme über die Kommunikationsschnittstellen <i>Die über Kommunikationsschnittstellen des Geräts eingegebenen Befehle dürfen die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten nicht unzulässig beeinflussen.</i>		
Detaillierende Anmerkungen: 1. Jeder Befehl muss eindeutig einer eingeleiteten Funktion oder Datenänderung zugeordnet werden können. 2. Befehle, die nicht dokumentiert sind, dürfen keine Wirkung auf die rechtlich relevanten Funktionen, gerätespezifischen Parameter und Messdaten haben. 3. Die jeweiligen Softwareteile, die die Befehle interpretieren, müssen als rechtlich relevante Software betrachtet werden. 4. Schnittstellen, die Befehle mit unzulässigen Auswirkungen auf die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten zulassen, müssen versiegelt oder auf sonstige angemessene Weise geschützt werden. Dies gilt auch für Schnittstellen, die nicht vollständig bewertet werden können. 5. Diese besondere Anforderung gilt nicht, wenn ein Softwaredownload entsprechend Anhang D durchgeführt wird.		
Erforderliche Dokumentation: Verfügt das Gerät über eine Schnittstelle, muss die Dokumentation umfassen: • Beschreibung von Befehlen und ihrer Wirkung auf die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten. • Eine Beschreibung, wie die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten vor dem Einfluss anderer Eingaben geschützt werden.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob alle dokumentierten Befehle zulässig sind, d.h. ob sie eine erlaubte Auswirkung auf rechtlich relevante Software, gerätespezifische Parameter und Messdaten haben. • Prüfen der Schutzmaßnahmen gegen Einflüsse von anderen Eingaben. <i>Funktionsprüfungen:</i> Ausführen praktischer Tests (Stichproben) mit Peripherieausstattung.		
Beispiel einer akzeptablen Lösung: Ein Softwaremodul empfängt und interpretiert die Daten von der Schnittstelle. Dieses Modul ist Teil der rechtlich relevanten Software. Es leitet nur erlaubte Befehle zu den anderen rechtlich relevanten Softwaremodulen weiter. Alle unbekannten oder nicht erlaubten Signal- oder Codefolgen werden zurückgewiesen und haben keine Auswirkung auf die rechtlich relevante Software, gerätespezifischen Parameter oder Messdaten.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die Software so aufgebaut ist, dass der Datenfluss bezüglich der Befehle eindeutig in der rechtlich relevanten Software definiert ist und nachvollzogen werden kann. • ob kein unzulässiger Datenfluss von der Benutzerschnittstelle zu den zu schützenden Bereichen erfolgt. • ob die Befehle richtig entschlüsselt werden. Das Überprüfen kann mit Tools oder manuell erfolgen. den.

Risikoklasse B	Risikoklasse C	Risikoklasse D
P5: Schutz vor zufälligen oder unbeabsichtigten Änderungen <i>Rechtlich relevante Software und gerätespezifische Parameter müssen vor zufälligen oder unbeabsichtigten Veränderungen geschützt werden.</i>		
Detaillierende Anmerkungen: 1. Die Software muss in der Lage sein, mögliche Änderungen infolge physikalischer Effekte (elektromagnetische Störung, Temperatur, Vibration usw.) zu erfassen. 2. Es sind Maßnahmen zu ergreifen, um die Benutzerschnittstellen vor unbeabsichtigter Fehlbedienung zu schützen.		
Erforderliche Dokumentation: Die Dokumentation sollte die Maßnahmen aufzeigen, die zur Erkennung und zum Schutz der rechtlich relevanten Software und gerätespezifischen Parameter gegen unbeabsichtigte Änderungen getroffen wurden.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob Maßnahmen gegen unbeabsichtigte Änderungen beschrieben werden und angemessen sind. <i>Funktionsprüfungen:</i> • Durch geeignete Stichproben überprüfen, ob vor dem Löschen von Messdaten eine Warnung erfolgt, sofern Löschen überhaupt möglich ist.		
Beispiel einer akzeptablen Lösung: • Die versehentliche Änderung von rechtlich relevanter Software und gerätespezifischen Parametern wird dadurch überprüft, dass periodisch Prüfsummen berechnet und automatisch mit den hinterlegten Sollwerten verglichen werden. Stimmt der Vergleich nicht überein, sind zum Gerät passende Reaktionen erforderlich (z.B. Anhalten der Messung, entsprechende Anzeige der Messdaten, siehe Kapitel 10 für eventuelle Empfehlungen). • Alternativmethoden sind möglich, wenn sich der Änderungsstatus der Software mit ihrer Hilfe identifizieren lässt. • Zum Thema Fehlererkennung siehe Anhang I (Kapitel 10).		
Zusätze für Risikoklasse E		
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen C und D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.		
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen C und D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die getroffenen Maßnahmen zum Erkennen von Veränderungen geeignet sind. • ob alle Teile der rechtlich relevanten Software von der Prüfsumme abgedeckt sind.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
P6: Schutz vor vorsätzlichen Änderungen <i>Rechtlich relevante Software und Messdaten müssen vor unzulässigen Veränderungen, Laden oder Austausch von Hardwarespeichern geschützt werden.</i>		
Detaillierende Anmerkungen: 1. Zum Thema Schutz gegen Manipulation mit Hilfe der Benutzerschnittstelle, siehe P3. 2. Zum Thema Schutz gegen Manipulation mit Hilfe der Kommunikationsschnittstelle, siehe P4. 3. Messdaten gelten bereits als ausreichend gesichert, wenn sie lediglich von rechtlich relevanter Software verarbeitet werden (z.B. im Speicher oder in Registern).		
	Detaillierende Anmerkungen: 4. Eine Prüfsumme oder eine Alternativmethode mit derselben Anforderungsstufe ist zur Verfügung zu stellen, um den Nachweis von Softwareänderungen zu unterstützen. 5. Die berechnete Prüfsumme oder eine Alternativanzeige der Softwareänderung ist auf Befehl für Kontrollzwecke sichtbar zu machen. 6. Die Prüfsumme oder Alternativanzeige wird über die rechtlich relevante Software berechnet. Die Software, mit Hilfe derer die Prüfsummen oder Alternativanzeigen erzeugt werden, ist Bestandteil der rechtlich relevanten Software. 7. Wird eine Prüfsumme verwendet, muss der Algorithmus eine Schlüssellänge von mindestens 4 Byte besitzen (siehe auch Anhänge L und T).	
Erforderliche Dokumentation: In der Dokumentation sollten die Schutzmethoden beschrieben sein: Beschreibung von Maßnahmen, die ergriffen wurden, um die Software und gerätespezifischen Parameter zu schützen, insbesondere die Beschreibung der Berechnungsmethode für Prüfsummen sowie die Sollprüfsummen oder Alternativmethoden mit der entsprechenden Sollanzeige.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - ob die dokumentierten Maßnahmen zur Sicherung des Softwarespeichers gegen unbefugten Austausch ausreichend sind. - ob die Prüfsumme(n) oder Alternativanzeige(n) die rechtlich relevante Software abdecken. <i>Funktionsprüfungen:</i> - Praktisches Testen des Programmiermodus und Prüfen, ob das Abschalten funktioniert. - Vergleich berechneter Prüfsummen oder alternativer Anzeigen mit den Sollwerten.		
Beispiel einer akzeptablen Lösung: a) Um zu verhindern, dass der physische Speicher entfernt und ausgetauscht wird, sollte entweder das Gerätegehäuse oder der physische Speicher selbst gegen unbefugte Entnahme gesichert sein. b) Das Gerät ist versiegelt und die Schnittstellen genügen den Anforderungen P3 und P4.	Beispiel einer akzeptablen Lösung: (zusätzlich zu a) und b)) c) Der Programmcode wird mittels Prüfsummen geschützt. Das Programm berechnet seine eigene Prüfsumme und vergleicht sie mit einem Sollwert, der im ausführbaren Code verborgen ist. Wenn der Selbsttest fehlschlägt, wird das Programm gesperrt. Es wird eine CRC-32-Prüfsumme mit einem geheimen Anfangsvektor (versteckt im ausführbaren Code) verwendet.	

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D):

Auf Basis des Quellcodes ist zu überprüfen:

- ob die zur Erfassung von vorsätzlichen Änderungen getroffenen Maßnahmen angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
P7: Sicherung der Parameter <i>Gerätespezifische Parameter müssen nach dem Einstellen gegen unzulässige Änderung gesichert werden.</i>		
Detaillierende Anmerkungen: 1. Im normalen gesicherten Betriebsmodus dürfen gerätespezifische Parameter nicht mehr änderbar sein. Sie dürfen nur in einem speziellen Betriebsmodus des Gerätes justierbar sein. 2. Einige gerätespezifische Parameter dürfen ungesichert bleiben. Zu gerätespezifischen Parametern siehe Anhang I.		
Erforderliche Dokumentation: Die Dokumentation muss die gerätespezifischen Parameter beschreiben, ob sie eingestellt werden dürfen, wie sie eingestellt werden und wie sie gesichert werden.		
Validierungsanleitung: Auf Basis der Dokumentation ist zu überprüfen: • ob Änderung oder Justierung zu sichernder gerätespezifischer Parameter nach der Sicherung unmöglich ist. • ob alle relevanten Parameter (falls vorhanden, in Anhang I angegebenen) gesichert sind. Funktionsprüfungen: • Überprüfen des Justierungs-/ (Konfigurations-) Modus und Prüfen, ob die Sperrung nach der Sicherung funktioniert. • Prüfen der Klassifizierung und des Zustands der Parameter (gesichert/setzbar) am Display des Messgerätes, wenn ein entsprechender Menüpunkt zur Verfügung steht.		
Beispiel einer akzeptablen Lösung: a) Die Parameter sind durch Versiegelung des Geräts oder Speichergehäuses und Sperren des Schaltkreiseingangs, der Schreiben aktiviert/sperrt, durch einen dazugehörigen, versiegelten Jumper oder Schalter gesichert.		
b) Ereigniszähler / Ereignislogbuch: • Ein Ereigniszähler registriert jede Änderung eines Parameterwertes. Der aktuelle Zählerstand kann angezeigt und mit dem ursprünglichen Zählerstand verglichen werden, der vor der Inbetriebnahme des Messinstruments oder bei der letzten Eichung aufgezeichnet wurde und unlöschar auf dem Gerät registriert ist. • Änderungen der Parameter werden in einem Ereignislogbuch registriert, d.h. es erfolgt eine Informationsaufzeichnung in einem nicht löschbaren Speicher. Jeder Eintrag wird automatisch von der rechtlich relevanten Software erzeugt und enthält: ○ den Identifikatoren des Parameters (z.B. den Namen), ○ den Parameterwert (den aktuellen oder den vorherigen Wert), ○ den Zeitstempel der Änderung • Das Ereignislogbuch kann nicht ohne Zerstörung eines Siegels gelöscht oder geändert werden. Der Inhalt des Ereignislogbuchs ist dann auf der Anzeige sichtbar oder wird auf Befehl gedruckt.		

Zusätze für Risikoklasse E

Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation):
--

Quellcode der rechtlich relevanten Software, der die Art und Weise der Sicherung und Anzeige der rechtlich relevanten Parameter aufzeigt.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D):

Auf Basis des Quellcodes ist zu überprüfen:

- ob die Maßnahmen für den Schutz der Parameter angemessen sind (z.B. Justiermodus nach dem Sichern gesperrt).

Risikoklasse C	Risikoklasse D
P8: Authentifizierung der dargestellten Messdaten <i>Die Authentizität der dargestellten Messdaten muss garantiert sein.</i>	

Detaillierende Anmerkungen:

1. Dargestellte Messdaten können als authentisch angesehen werden, wenn die Darstellung von der rechtlich relevanten Software generiert wird.
2. Es darf nicht möglich sein, zugelassene rechtlich relevante Software zur Darstellung von Messdaten mit Hilfe leicht verfügbarer und handhabbarer Werkzeuge betrügerisch nachzuahmen (vorzutäuschen).
3. Dargestellte Messdaten müssen verständlich und klar unterscheidbar von anderen rechtlich nicht relevanten Informationen sein. Gegebenenfalls muss eine zusätzliche Erläuterung gegeben werden.
4. Wenn die Quelle der dargestellten Messdaten (z.B. ein Sensor) nicht implizit identifiziert oder nachgewiesen werden kann (z.B., wenn mehr als ein Sensor vorhanden ist oder wenn der Sensor aus der Ferne angeschlossen ist), muss das Gerät die jeweilige Quelle identifizieren. Der einzelne Identifikator der zugelassenen Quelle ist ein rechtlich relevanter Parameter, der von P6/U6 oder P7/U7 abgedeckt ist. Abhängig vom Daten Verbindungstyp muss gegebenenfalls Anhang T angewendet werden.

Erforderliche Dokumentation:

In der Dokumentation sollte beschrieben sein, wie die Authentizität der Messdaten garantiert wird.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu überprüfen,

- ob die rechtlich relevante Software die dargestellten Messdaten erzeugt
- ob die Darstellung der Messdaten nur durch rechtlich relevante Software ausgeführt werden kann.
- Wenn die Quelle der dargestellten Messdaten nicht implizit identifizierbar oder nachweisbar ist, ist zu prüfen, ob die Quelle dieser Daten von der rechtlich relevanten identifiziert und nachgewiesen werden kann.

Funktionsprüfungen:

- Überprüfen durch Sichtkontrolle, ob die Darstellung der Messdaten leicht unterscheidbar von anderen möglicherweise auch dargestellten Informationen ist.
- Gegebenenfalls ist durch visuelle Kontrollen zu prüfen, ob die dargestellten Messdaten korrekt der jeweiligen Quelle beigeordnet werden.

Beispiel einer akzeptablen Lösung:

1. Eine Messanwendung wird von der rechtlich relevanten Software erzeugt. Die für die Anwendung nötigen technischen Maßnahmen sind:
 - Die rechtlich nicht relevanten Programme erhalten keinen Zugriff auf die Messdaten, bis die Messdaten angezeigt wurden.
 - Die Anwendung wird periodisch aktualisiert. Das zugehörige Programm überprüft, ob die Anwendung sichtbar ist, solange die Messung nicht abgeschlossen ist. Die Messwertverarbeitung hält an, wenn diese Anwendung geschlossen wird oder nicht vollständig sichtbar ist.
- 2a Die Sensoreinheit verschlüsselt die Messwerte mit einem Schlüssel, der auf dem Universalcomputer nur der zugelassenen Software bekannt ist (z.B. ihre Versionsnummer). Nur die zugelassene Software kann die Messwerte entschlüsseln und benutzen, nicht zugelassene Programme auf dem Universalcomputer können es nicht, da sie den Schlüssel nicht kennen. Zur Schlüsselhandhabung siehe Anhang T.
- 2b Vor dem Senden von Messwerten stößt der Sensor eine Handshake-Sequenz mit der rechtlich relevanten Software auf dem Universalcomputer an, die auf geheimen Schlüsseln basiert. Nur wenn das Programm auf dem Messgerät mit zweckgebundener Hard- und Software korrekt kommuniziert, sendet die Sensoreinheit ihre Messwerte. Zur Schlüsselhandhabung siehe Anhang T.
3. Der in 2a / 2b verwendete Schlüssel wird gewählt sowie der Sensoreinheit und der Software auf dem Universalcomputer ohne Zerstörung eines Siegels übergeben.
3. Der in 2a / 2b verwendete Schlüssel ist der Hashcode des Programms auf dem Messgerät mit zweckgebundener Hard- und

	Software. Jedes Mal, wenn die Software auf dem Universalcomputer geändert wird, wird der neue Schlüssel in die Sensoreinheit eingegeben und so gesichert, dass ein Siegel aufgebrochen werden muss, um ihn zu ändern.
4 Wenn die dargestellten Messdaten nicht explizit mit einem Sensor verbunden sind, überträgt der ursprüngliche Sensor seine Daten zusammen mit einer eindeutigen Kennzeichnung des Sensors selbst. Alle dargestellten Messdaten werden mit der Kennzeichnung des einzelnen Sensors versehen. Die Kennzeichnung jedes Sensors ist ein rechtlich relevanter Parameter, der am Sensorgehäuse angezeigt wird.	

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen C bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen C bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die rechtlich relevante Software die dargestellten Messergebnisse erzeugt. • ob alle getroffenen Maßnahmen angemessen und richtig sind, um die Darstellung der Messergebnisse durch rechtlich relevante Software zu gewährleisten.

5 Basisanforderungen an Software von Messgeräten mit Universalrechner (Typ U)

Der Satz spezifischer Anforderungen des vorliegenden Kapitels ist gültig für Messgeräte, die auf einem Universalrechner gestützt sind, sowie für Teilgeräte und Teile gemäß WELMEC Leitfaden 8.8, die Universalrechner verwenden. Die Gültigkeit erstreckt sich auf Teilgeräte und Baueinheiten, auch wenn sie im folgenden Text nicht fortwährend erwähnt wird. Die Bedingungen, unter denen Teilgeräte und Baueinheiten separat geprüft und die dazugehörigen Zertifikate akzeptiert werden können, sind jedoch nicht Bestandteil des vorliegenden Leitfadens.

5.1 Technische Beschreibung

Ein Messgerät vom Typ U wird typischerweise durch die folgenden Konfigurationen charakterisiert.

Hardwarekonfiguration

- a) Ein modulares auf einen Universalcomputer gestütztes System. Das Computersystem kann ein Stand-alone-System, Teil eines geschlossenen Netzes (z.B. Ethernet, Token-Ring-LAN) oder Teil eines offenen Netzes (z.B. Internet) sein.
- b) Da das System für universelle Zwecke ausgelegt ist, befindet sich der Messsensor normalerweise außerhalb des Computersystems und ist über eine Kommunikationsverbindung angekoppelt.
- c) Die Benutzerschnittstelle bietet neben dem Betriebsmodus für die Messaufgabe weitere Funktionen, die nicht unter rechtlicher Kontrolle stehen.
- d) Speichermedien können fest installiert (z.B. Festplatte), entfernbar (z.B. USB) oder entfernt vorhanden (remote) sein.

Softwarekonfiguration

- e) Üblicherweise wird ein Betriebssystem verwendet.
- f) Neben der Anwendung des Messgeräts können sich gleichzeitig auch andere Softwareanwendungen auf dem System befinden.

Zusätzlich zu den oben beschriebenen Konfigurationen ist von einem System vom Typ U auch dann auszugehen, wenn die Eigenschaften eines Geräts vom Typ P (siehe Unterkapitel 4.1) nicht vollständig erfüllt sind.

Ein serienmäßig gefertigtes Betriebssystem und mit ihm gelieferte Low-Level-Treiber (z.B. Video-Treiber, Druckertreiber, Disk-Treiber usw.) werden als rechtlich nicht relevant angesehen, soweit Teile nicht durch Alternativteile ersetzt sind oder speziell für eine bestimmte Messaufgabe programmiert worden sind.

Folgen für die Risikoklassifikation

Die Software von Geräten vom Typ U ist sehr viel leichter zugänglich als die Software von Geräten vom Typ P. Der Schutz der Softwareintegrität muss im Vergleich zu Geräten vom Typ P erhöht werden. Insbesondere wird eine Prüfsumme oder ein gleichwertiges Mittel erwartet, um die Integritätsprüfungen des Softwarecodes zu unterstützen. Die Folge ist, dass die Software-Konformitätsebene "niedrig" (nur

funktionelle Übereinstimmung der Software mit der technischen Dokumentation des in der Prüfung befindlichen Gerätetyps) kein adäquates Mittel ist, um die Softwareintegrität zu sichern. Dies bedeutet, dass die Risikoklasse C die niedrigste Risikoklasse ist, in die Geräte vom Typ U eingestuft werden können

5.2 Spezifische Softwareanforderungen an Typ U

Risikoklassen C bis E
U1: Dokumentation <i>Zusätzlich zur spezifischen Dokumentation, die in jeder der folgenden Anforderungen erforderlich ist, muss die Dokumentation grundsätzlich Folgendes umfassen:</i> <i>Eine Beschreibung der rechtlich relevanten Software, der Bedeutung der Daten usw..</i> <i>Eine Beschreibung der Genauigkeit der Messalgorithmen (z.B. Preisberechnungs- und Rundungsalgorithmen).</i> <i>Eine Beschreibung der Benutzerschnittstelle, der Menüs und der Dialoge.</i> <i>Der bzw. die Software-Identifikator(en) der rechtlich relevanten Software.</i> <i>Einen Überblick über die Systemhardware, z.B. Block-Schaltbild, Computerart(en), Netzwerktypen, usw.</i> <i>Einen Überblick über die Konfiguration des verwendeten Betriebssystems, Sicherheitsaspekte des verwendeten Betriebssystems (z.B. Schutz, Benutzerkonten, Zugriffsrechte) usw.</i> <i>Das Betriebshandbuch.</i>
Risikoklasse C und D
U2: Softwareidentifikation <i>Die rechtlich relevante Software muss eindeutig gekennzeichnet sein. Der bzw. die Identifikator(en) müssen vom Gerät auf Befehl oder laufend während des Betriebs dargestellt werden.</i>
Detaillierende Anmerkungen: - Rechtlich relevante Software-Identifikatoren können unabhängig oder Teil eines gut strukturierten Identifikators sein. - Für den Fall, dass ein rechtlich relevanter Software-Identifikator in einen Gesamtidentifikator eingebettet ist, muss er deutlich unterscheidbar sein. - Die rechtlich relevanten Identifikatoren müssen für jede rechtlich relevante Software, mit der das Gerät ausgestattet ist, eindeutig sein. - Die rechtlich relevanten Identifikatoren müssen ohne zusätzliches Werkzeug problemlos darstellbar sein. - Die Identifizierung soll Treiber und Komponenten des Betriebssystems umfassen, die geändert oder speziell für eine rechtlich relevante Aufgabe programmiert wurden. Standardkomponenten, die unverändert verwendet werden, können von der Identifikation ausgenommen werden. - Wenn die rechtlich relevanten Funktionen und der Account des Messprozesses durch eine spezielle Betriebssystemkonfiguration geschützt sind, müssen die relevanten Konfigurationsdateien einen eigenen Identifikator besitzen. - Die rechtlich relevanten Software-Identifikatoren werden als bauartspezifische Parameter betrachtet und müssen als solche geschützt werden (siehe U5 und U6). Wenn die Identifikatoren nicht untrennbar mit der Software selbst verbunden sind, sind andere Sicherheitsmaßnahmen erforderlich. - Die Identifikatoren werden auf Befehl oder beim Einschalten dargestellt.
Erforderliche Dokumentation: Die Dokumentation muss die Software-Identifikatoren auflisten und beschreiben, wie diese erzeugt werden, wie sie gesichert werden, wie sie dargestellt werden können und, gegebenenfalls, wie sie strukturiert sind, um zwischen rechtlich relevanten Software-Identifikatoren und anderen unterscheiden zu können.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu überprüfen:

- ob in der Dokumentation die rechtlich relevanten Software-Identifikatoren angegeben sind.
- ob die Software, die die rechtlich relevanten Aufgaben ausführt, klar beschrieben ist, so dass nachvollziehbar ist, welcher rechtlich relevante Softwareteil von welchem Software-Identifikator abgedeckt wird.
- Beschreibung der Erzeugung und Visualisierung der Identifikatoren.
- ob es geänderte oder selbst entwickelte Komponenten eines Betriebssystems gibt und, wenn ja, ob sie in der Identifikation inbegriffen sind.
- ob relevante Konfigurationsdateien einen eigenen Identifikator besitzen, wenn die Software für Messfunktionen über eine spezielle Betriebssystemkonfiguration geschützt ist.
- ob alle rechtlich relevanten Software-Identifikatoren eindeutig sind.

Funktionsprüfungen:

- Die Software-Identifikatoren können so dargestellt werden, wie in der Dokumentation beschrieben.
- Die dargestellten Identifikatoren stimmen mit den in der Dokumentation angegebenen Identifikatoren überein.
- Die rechtlich relevanten Software-Identifikatoren sind von anderen Identifikatoren unterscheidbar.

Beispiel einer akzeptablen Lösung:

- a) eine Prüfsumme über den Code.
- b) eine Zeichenreihe, die von einer Versionsnummer ergänzt wird,
- c) jede beliebige Zahlen-, Buchstaben- oder andere Zeichenreihe,
- d) .
- Wählt der Hersteller einen gemischten Identifikator für die rechtlich relevante und die rechtlich nicht relevante Software, ist eine einfache Lösung zur Unterscheidung der Identifikatoren die Verwendung von Platzhaltern in der Baumusterprüfbescheinigung, z.B. "abc1.xx", wobei "abc1" für die rechtlich relevante Software und "xx" als Platzhalter für rechtlich nicht relevante Software steht.
-

Zusätze für Risikoklasse E
Erforderliche Dokumentation Identisch mit den Risikoklassen C und D.
Validierungsanleitung Identisch mit den Risikoklassen C und D.

Risikoklasse C	Risikoklasse D
U3: Einflussnahme über die Benutzerschnittstelle Die über die Benutzerschnittstelle eingegebenen Befehle dürfen die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten nicht unzulässig beeinflussen.	
Detaillierende Anmerkungen:	
1. Jeder Befehl muss eindeutig einer eingeleiteten Funktion oder Datenänderung zugeordnet werden können. 2. Befehle, die nicht dokumentiert sind, dürfen keine Wirkung auf die rechtlich relevanten Funktionen, gerätespezifischen Parameter und Messdaten haben. 3. Die jeweiligen Softwareteile, die die Befehle interpretieren, müssen als rechtlich relevante Software betrachtet werden. 4. Insbesondere dürfen die über die Benutzerschnittstelle verfügbaren Betriebssystemfunktionen die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten einschließlich der Konfiguration des Betriebssystems oder andere Mittel für ihren Schutz nicht beeinflussen.	5. Die Benutzeranwendung muss geschlossen sein, d.h. der Nutzer darf nicht in der Lage sein, Programme zu laden, Programme zu schreiben oder Befehle an das Betriebssystem auszuführen.

÷

Erforderliche Dokumentation: Wenn das Gerät die Fähigkeit zum Befehlsempfang hat, muss die Dokumentation Folgendes enthalten: • Beschreibung von Befehlen und ihrer Wirkung auf die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten. • Eine Beschreibung, wie die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten vor dem Einfluss anderer Eingaben geschützt werden. • Insbesondere eine Beschreibung, wie die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten vor Funktionen des Betriebssystems geschützt werden, die für den Nutzer verfügbar sind.	Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklasse C erforderlich ist): • Eine Beschreibung der Schutzmittel gegen andere Eingaben, einschließlich der Funktionen des Betriebssystems, die für den Nutzer verfügbar sind.
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob alle dokumentierten Befehle zulässig sind, d.h. ob sie eine erlaubte Auswirkung auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten haben. • Die Schutzmaßnahmen gegen Einflüsse von anderen Befehlen. • Insbesondere die Schutzmaßnahmen gegen Einflüsse von Funktionen des Betriebssystems, die für den Nutzer verfügbar sind. <i>Funktionsprüfungen:</i> • Durchführung praktischer Tests (Stichproben) mit dokumentierten Befehlen. • Prüfen, ob es nicht dokumentierte Befehle gibt.	Validierungsanleitung (zusätzlich zur Anleitung für die Risikoklasse C): <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die getroffenen Maßnahmen und die Testprotokolle dem hohen Schutzniveau entsprechen
Beispiel einer akzeptablen Lösung: • Ein Modul in der rechtlich relevanten Software filtert unzulässige Befehle heraus. Nur dieses Modul empfängt die Befehle, und es kann nicht umgangen werden. Jede falsche Eingabe ist gesperrt.	Beispiel einer akzeptablen Lösung: • Für den Einsatz des Messsystems ist ein Konto mit nur eingeschränkten Berechtigungen eingerichtet. Der Zugriff auf das Administratorkonto ist entsprechend U6 gesperrt.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (zusätzlich zur für Risikoklasse D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für die Risikoklasse D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die Software so aufgebaut ist, dass der Datenfluss bezüglich der Befehle eindeutig in der rechtlich relevanten Software definiert ist und nachvollzogen werden kann. • dass kein unzulässiger Datenfluss von der Benutzerschnittstelle zu den zu schützenden Bereichen erfolgt. • ob die Befehle richtig entschlüsselt werden. Das Überprüfen kann mit Tools oder manuell erfolgen.

Risikoklasse C	Risikoklasse D
U4: Einflussnahme über die Kommunikationsschnittstelle <i>Die über die Kommunikationsschnittstellen des Geräts eingegebenen Befehle dürfen keinen unzulässigen Einfluss auf die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten haben.</i>	
Detaillierende Anmerkungen: 1. Jeder Befehl muss eindeutig einer eingeleiteten Funktion oder Datenänderung zugeordnet werden können. 2. Befehle, die nicht dokumentiert sind, dürfen die rechtlich relevanten Funktionen, die gerätespezifischen Parameter und die Messdaten nicht beeinflussen. 3. Die jeweiligen Softwareteile, die die Befehle interpretieren, müssen als rechtlich relevante Software betrachtet werden. 4. Schnittstellen, die Befehle mit unzulässigen Auswirkungen auf die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten zulassen, müssen versiegelt oder auf sonstige angemessene Weise geschützt werden. Dies gilt auch für Schnittstellen, die nicht vollständig bewertet werden können. 5. Diese besondere Anforderung gilt nicht, wenn ein Softwaredownload entsprechend Anhang D durchgeführt wird. <i>Hinweis:</i> Wenn das Betriebssystem Fernsteuerung oder –zugriff gestattet, bezieht sich die Anforderung U3 auf die Kommunikationsschnittstelle bzw. die angeschlossenen Fernzugriffsterminals.	
Erforderliche Dokumentation: Verfügt das Gerät über eine Schnittstelle, muss die Dokumentation umfassen: • Beschreibung von Befehlen und ihrer Wirkung auf die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten. • Eine Beschreibung, wie die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten vor dem Einfluss andere Eingaben geschützt werden.	
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob alle dokumentierten Befehle zulässig sind, d.h. ob sie eine erlaubte Auswirkung auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten haben. • Die Schutzmaßnahmen gegen Einflüsse von anderen Befehlen. <i>Funktionsprüfungen:</i> • Ausführen praktischer Tests (Stichproben) mit Peripherieausstattung.	
Beispiel einer akzeptablen Lösung: Ein Softwaremodul empfängt und interpretiert Befehle von der Schnittstelle. Dieses Modul ist Teil der rechtlich relevanten Software. Es leitet nur erlaubte Befehle zu den anderen rechtlich relevanten Softwaremodulen weiter. Alle unbekannten oder nicht erlaubten Befehle werden zurückgewiesen und haben keine Auswirkung auf die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten.	

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen C bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen C bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die Software so aufgebaut ist, dass der Datenfluss bezüglich der Befehle eindeutig in der rechtlich relevanten Software definiert ist und nachvollzogen werden kann. • ob kein unzulässiger Datenfluss von der Benutzerschnittstelle zu den zu schützenden Bereichen erfolgt. • ob die Befehle richtig entschlüsselt werden. Das Überprüfen kann mit Tools oder manuell erfolgen.

Risikoklasse C	Risikoklasse D
U5: Schutz vor zufälligen oder unbeabsichtigten Änderungen <i>Rechtlich relevante Software und gerätespezifische Parameter müssen vor zufälligen oder unbeabsichtigten Veränderungen geschützt werden.</i>	
Detaillierende Anmerkungen: 1. Die Software muss in der Lage sein, mögliche Änderungen infolge physikalischer Effekte (elektromagnetische Störung, Temperatur, Vibration usw.) zu erfassen. 2. Es sind Maßnahmen zu ergreifen, um die Benutzerschnittstellen vor unbeabsichtigter Fehlbedienung zu schützen. 3. Die zufällige Änderung der rechtlich relevanten Software und gerätespezifischen Parameter muss mittels periodischer Berechnung der Prüfsumme(n) und automatischem Vergleich mit hinterlegten Sollwerten geprüft werden. Stimmt der Vergleich nicht überein, sind Reaktionen erforderlich, die für das Gerät angemessen sind (z.B. Anhalten der Messung, Anzeige der Messdaten, siehe Kapitel 10 für eventuelle Empfehlungen). Alternativmethoden sind möglich, wenn sich der Änderungsstatus der Software mit ihrer Hilfe identifizieren lässt. 4. Falls das Betriebssystem es gestattet, ist es empfehlenswert, dass alle Nutzerrechte zum Löschen, Verschieben oder Ändern der rechtlich relevanten Software gelöscht werden und der Zugriff über Hilfsprogramme gesteuert wird. 5. Zugriffskontrolle auf rechtlich relevante Software durch die Verwendung von Passwörtern ist ebenso zu empfehlen, wie der Einsatz von Read-Only-Mechanismen. Der Systemsupervisor darf Rechte nur bei Bedarf wiederherstellen.	
Erforderliche Dokumentation: • Beschreibung der Maßnahmen, die zur Erkennung und zum Schutz der rechtlich relevanten Software und der gerätespezifischen Parameter gegen unbeabsichtigte Änderungen getroffen wurden. • Beschreibung der Prüfsummenmethode und der Reaktionen im Falle der Nichtübereinstimmung. • Beschreibung, wie und wo die Sollprüfsumme(n) oder die Alternativanzeigen des Änderungsstatus abgelegt werden.	
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob Maßnahmen gegen unbeabsichtigte Änderungen beschrieben werden und angemessen sind. • ob Prüfsummen die rechtlich relevante Software abdecken. • ob die Methoden zur Prüfsummenberechnung, der Vergleich und die Reaktionen im Falle der Nichtübereinstimmung korrekt sind.	
Beispiel einer akzeptablen Lösung: • Missbrauch des Betriebssystems, Überschreiben oder Löschen gespeicherter Daten und Programme: Die Schutz- und Vertraulichkeitsrechte, die durch das Betriebssystem oder die Programmiersprache zur Verfügung stehen, werden in vollem Umfang genutzt. • Die versehentliche Änderung von rechtlich relevanter Software wird dadurch geprüft werden, dass eine Prüfsumme über den entsprechenden Code berechnet wird, diese mit dem Sollwert verglichen wird und entsprechende Reaktionen eingeleitet werden, wenn der Code verändert wurde. •	
Zusätze für Risikoklasse E	
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen C bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.	
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen C bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die getroffenen Maßnahmen zum Erkennen von Veränderungen (Fehler) geeignet sind. • ob alle Teile der rechtlich relevanten Software von der Prüfsumme abgedeckt sind.	

Risikoklasse C	Risikoklasse D
U6: Schutz vor vorsätzlichen Änderungen <i>Rechtlich relevante Software und Messdaten müssen vor unzulässigen absichtlichen Veränderungen oder Austausch geschützt werden.</i> Detaillierende Anmerkungen: 1. Der Massenspeicher, in dem die rechtlich relevante Software, Konfigurationsdateien und gerätespezifischen Parameter aufbewahrt werden, muss vor Austausch geschützt sein. 2. Eine Prüfsumme oder eine Alternativmethode mit derselben Anforderungsstufe ist zur Verfügung zu stellen, um den Nachweis von Softwareänderungen zu unterstützen. Die berechnete Prüfsumme oder eine Alternativanzeige der Softwareänderung ist auf Befehl für Kontrollzwecke sichtbar zu machen. 3. Die Prüfsumme oder Alternativanzeige wird über die rechtlich relevante Software berechnet. Die Software, mit Hilfe derer die Prüfsummen oder Alternativanzeigen erzeugt werden, ist Bestandteil der rechtlich relevanten Software. 4. Es müssen Maßnahmen ergriffen werden, um rechtlich relevante Software vor Änderungen oder Austausch durch andere Software mit Hilfe der Schutzmaßnahmen des Betriebssystems zu schützen. 5. Die Teile und Merkmale des Betriebssystems, die den Schutz der rechtlich relevanten Software realisieren, müssen als rechtlich relevante Software betrachtet und als solche geschützt werden. Diese besondere Anforderung gilt nicht, wenn ein Softwaredownload entsprechend Anhang D durchgeführt wird. 6. Wird eine Prüfsumme verwendet, muss der Algorithmus eine Schlüssellänge von mindestens 4 Bytes haben;	
	7. Generell ist ein Universalcomputer nur dann geeignet, wenn zusätzliche Hardware zur Sicherung verwendet werden kann. 8. Was Algorithmen und minimale Schlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden.
Erforderliche Dokumentation: • Beschreibung von Maßnahmen, die ergriffen wurden, um die Software und gerätespezifischen Parameter zu schützen, insbesondere die Beschreibung der Berechnungsmethode für Prüfsummen sowie die Sollprüfsummen oder Alternativmethoden mit der entsprechenden Sollanzeige. • Beschreibung von Methoden, wie die Massenspeicher gegebenenfalls vor Austausch geschützt werden. • Beschreibung der verwendeten Sicherungsmerkmale des Betriebssystems. • Beschreibung, wie die Prüfsumme oder eine Alternativanzeige dargestellt werden.	
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen</i> • ob die Prüfsumme(n) oder Alternativanzeigen die rechtlich relevante Software umfassen. • ob die Maßnahmen, mit denen verhindert werden soll, dass rechtlich relevante Software mit Hilfe des Betriebssystems geändert oder ausgetauscht wird, angemessen sind • dass die Merkmale des Betriebssystems, die für den Schutz der rechtlich relevanten Software genutzt werden, Teil der rechtlich relevanten Software sind und als solche geschützt werden. • dass Massenspeichergeräte gegebenenfalls vor Austausch geschützt werden. Funktionsprüfungen • Vergleich berechneter Prüfsummen oder Alternativanzeigen mit den Sollwerten.	

	<i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die getroffenen Maßnahmen dem geforderten hohen Schutzniveau gemäß dem Stand der Technik entsprechen.
Beispiel einer akzeptablen Lösung: 1. Der Programmcode wird mittels Prüfsummen geschützt. Das Programm berechnet seine eigene Prüfsumme und vergleicht sie mit einem Sollwert, der im ausführbaren Code verborgen ist. Wenn der Selbsttest fehlschlägt, wird das Programm gesperrt. Eine CRC-32 Prüfsumme mit einem geheimen Initialvektor (im ausführbaren Code versteckt) wird verwendet. Der Zugang zum Administratorkonto wird mittels eines automatisch generierten Passworts gesperrt, das niemandem bekannt ist. Änderung der rechtlich relevanten Konfiguration nur möglich mittels Durchführung eines Betriebssystem-Setups. Ein Umgehen der Schutzmaßnahmen des Betriebssystems durch direktes Schreiben auf den Massenspeicher oder dessen Austausch wird durch Versiegelung verhindert. 2. Die unerlaubte Veränderung der rechtlich relevanten Software kann über die Zugriffskontrolle oder die Datenschutzattribute des Betriebssystems verhindert werden. Die Administrationsebene dieser Systeme muss durch Versiegelung oder ein gleichwertiges Mittel gesichert werden. • • •	Beispiel einer akzeptablen Lösung: • Programmcode wird durch die Speicherung der rechtlich relevanten Software in einer geeigneten Einsteckeinheit gesichert, die versiegelt ist. Die Einsteckeinheit kann z.B. einen Read-Only-Speicher oder einen Mikrocontroller enthalten. •

Zusätze für Risikoklasse E

Erforderliche Dokumentation (zusätzlich zur für Risikoklassen C bis D geforderten Dokumentation):
Quellcode der rechtlich relevanten Software.

Validierungsanleitung (zusätzlich zur Anleitung für die Risikoklasse D):

Auf Basis des Quellcodes ist zu überprüfen:

- die Kommunikation mit der zusätzlichen Sicherungshardware,
- ob Änderungen der rechtlich relevanten Software erkannt werden.

Risikoklasse C	Risikoklasse D
U7: Sicherung der Parameter <i>Gerätespezifische Parameter müssen nach dem Einstellen gegen unzulässige Änderung gesichert werden.</i>	
Detaillierende Anmerkungen: 1. Da einrichtungsabhängige Parameter durch den Gebrauch einfacher Tools auf Universalcomputern manipuliert werden könnten, dürfen sie nicht auf Standardspeichern eines Universalcomputers gespeichert werden.	

Erforderliche Dokumentation:

Die Dokumentation muss die gerätespezifischen Parameter beschreiben, ob sie eingestellt werden dürfen, wie sie eingestellt werden und wie sie gesichert werden.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu überprüfen:

- ob Änderung oder Justierung gerätespezifischer Parameter nach der Sicherung unmöglich ist.
- ob alle relevanten Parameter gesichert sind.

Beispiel einer akzeptablen Lösung:

- Zu schützende gerätespezifische Parameter werden auf einer Einsteckspeichereinheit aufbewahrt, die gegen das Entfernen versiegelt ist oder sich direkt auf der Sensoreinheit befindet. Das Schreiben von Parametern wird durch Versiegeln des Schreibschuttschalters im gesicherten Zustand unterbunden.
- Ungeschützte setzbare Parameter sind auf einem Standardspeicher des Universalcomputers gespeichert.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (zusätzlich zur für Risikoklassen C bis D geforderten Dokumentation):
Quellcode der rechtlich relevanten Software.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen C bis D):

Auf Basis des Quellcodes ist zu überprüfen:

- ob die zum Schutz von Parametern getroffenen Maßnahmen angemessen sind.

Risikoklasse C**Risikoklasse D****U8: Authentifizierung der dargestellten Messdaten**

Die Authentizität der dargestellten Messdaten muss garantiert sein.

Detaillierende Anmerkungen:

1. Dargestellte Messdaten können als authentisch angesehen werden, wenn die Darstellung von der rechtlich relevanten Software generiert wird.
2. Es darf nicht möglich sein, zugelassene rechtlich relevante Software zur Darstellung von Messdaten mit Hilfe der Funktionen des Betriebssystems oder anderer leicht verfügbarer und handhabbarer Werkzeuge betrügerisch nachzuahmen (vorzutäuschen).
3. Dargestellte Messdaten müssen verständlich und klar unterscheidbar von anderen rechtlich nicht relevanten Informationen sein. Gegebenenfalls muss eine zusätzliche Erläuterung gegeben werden.
4. Falls es nicht möglich ist, mit Hilfe der Betriebssystemmöglichkeiten einen vollständigen Schutz herzustellen, muss durch technische Mittel sichergestellt werden, dass auf dem Universalcomputer nur die rechtlich relevante Software rechtlich relevante Funktionen durchführen kann (z.B. darf ein Sensor nur mit dem rechtlich relevanten Anzeigeprogramm auf dem Universalcomputer zusammenarbeiten).
5. Wenn die Quelle der dargestellten Messdaten (z.B. ein Sensor) nicht implizit identifiziert oder nachgewiesen werden kann (z.B., wenn mehr als ein Sensor vorhanden ist oder wenn der Sensor aus der Ferne angeschlossen ist), muss das Gerät die jeweilige Quelle identifizieren. Der einzelne Identifikator der zugelassenen Quelle ist ein rechtlich relevanter Parameter, der von P6/U6 oder P7/U7 abgedeckt ist. Abhängig vom Datenverbindungstyp muss gegebenenfalls Anhang T angewendet werden.

Erforderliche Dokumentation:

In der Dokumentation sollte beschrieben sein, wie die Authentizität der Messdaten garantiert wird.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu überprüfen,

- ob die rechtlich relevante Software die dargestellten Messdaten erzeugt
- ob die Darstellung der Messdaten nur durch rechtlich relevante Software ausgeführt werden kann.
- Wenn die Quelle der dargestellten Messdaten nicht implizit identifizierbar oder nachweisbar ist, ist zu prüfen, ob die Quelle dieser Daten von der rechtlich relevanten identifiziert und nachgewiesen werden kann.

Funktionsprüfungen:

- Überprüfen durch Sichtkontrolle, ob die Darstellung der Messdaten leicht unterscheidbar von anderen möglicherweise auch dargestellten Informationen ist.
- Gegebenenfalls ist durch visuelle Kontrollen zu prüfen, ob die dargestellten Messdaten korrekt der jeweiligen Quelle beigeordnet werden.

Beispiel einer akzeptablen Lösung:

1. Die rechtlich relevante Software zeigt die Messdaten in einem Fenster an, welches immer oben ist. Die rechtlich nicht relevante Software hat keinen Zugriff auf die Messdaten, bis die Messdaten angezeigt werden
- 2a Die Sensoreinheit verschlüsselt die Messwerte mit einem Schlüssel, der auf dem Universalcomputer nur der zugelassenen Software bekannt ist (z.B. ihre Versionsnummer). Nur die zugelassene Software kann die Messwerte entschlüsseln und benutzen, nicht zugelassene Programme auf dem Universalcomputer können es nicht, da sie den Schlüssel nicht kennen. Zur Schlüsselhandhabung siehe Anhang T.
- 2b Vor dem Senden von Messwerten stößt der Sensor eine Handshake-Sequenz mit der rechtlich relevanten Software auf dem Universalcomputer an, die auf geheimen Schlüsseln basiert. Nur wenn das Programm auf dem Universalcomputer korrekt kommuniziert, sendet die Sensoreinheit ihre Messwerte. Zur Schlüsselhandhabung siehe Anhang T.

3. Der in 2a / 2b verwendete Schlüssel wird gewählt sowie der Sensoreinheit und der Software auf dem Universalcomputer ohne Zerstörung eines Siegels übergeben.

3. Der in 2a / 2b verwendete Schlüssel ist der Hashcode des Programms auf dem Universalcomputer. Jedes Mal, wenn die Software auf dem Universalcomputer geändert wird, wird der neue Schlüssel in die Sensoreinheit eingegeben und so gesichert, dass ein Siegel aufgebrochen werden muss, um ihn zu ändern.

4. Wenn die dargestellten Messdaten nicht explizit mit einem Sensor verbunden sind, überträgt der ursprüngliche Sensor seine Daten zusammen mit einer eindeutigen Kennzeichnung des Sensors selbst. Alle dargestellten Messdaten werden mit der Kennzeichnung des einzelnen Sensors versehen. Die Kennzeichnung jedes Sensors ist ein rechtlich relevanter Parameter, der am Sensorgehäuse angezeigt wird.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (zusätzlich zur für Risikoklassen C bis D geforderten Dokumentation):
Quellcode der rechtlich relevanten Software.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen C bis D):

Auf Basis des Quellcodes ist zu überprüfen:

- ob die rechtlich relevante Software die dargestellten Messergebnisse erzeugt.
- ob alle getroffenen Maßnahmen angemessen und richtig sind, um die Darstellung der Messergebnisse durch rechtlich relevante Software zu gewährleisten.

Risikoklassen C bis E**U9: Einfluss anderer Software**

Die rechtlich relevante Software muss so aufgebaut sein, dass andere Software sie nicht unzulässig beeinflusst.

Detaillierende Anmerkungen:

1. Die Softwaretrennung zwischen der rechtlich relevanten und der rechtlich nicht relevanten Software muss gemäß dem Stand des Software-Engineering für Modularisierung oder für objektorientierte Konzepte konstruiert sein. Anhang S muss beachtet werden. Dies ist für Universalcomputer der Normalfall.

Erforderliche Dokumentation:

Siehe Anhang S.

Validierungsanleitung:

Siehe Anhang S.

Beispiel einer akzeptablen Lösung:

Siehe Anhang S.

6 Anhang L: Langzeitspeicherung von Messdaten

Die spezifischen Anforderungen dieses Kapitels wird nur dann angewendet, wenn eine Langzeitspeicherung von Messdaten durchgeführt wird. Sie sind eine Ergänzung zu den spezifischen Anforderungen sowohl an die eingebettete Software eines Messgerätes mit zweckgebundener Hard- und Software (Typ-P-Anforderungen) als auch an die Software von Messgeräten mit Universalcomputer (Typ-U-Anforderungen).

Die Langzeitspeicherung umfasst den Zeitpunkt, ab dem eine Messung physisch abgeschlossen ist, bis zu dem Zeitpunkt, an dem alle durch die Software zu erledigenden Prozesse beendet sind. Die Anforderungen können ebenso auf die anschließende Langzeitspeicherung der Daten angewendet werden.

6.1 Technische Beschreibung

Drei unterschiedliche technische Konfigurationen für die Langzeitspeicherung sind in der folgenden Tabelle aufgeführt. Für ein Messgerät mit zweckgebundener Hard- und Software ist die Variante eines integrierten Speichers typisch: Hier ist die Speicherung Teil der messtechnisch notwendigen Hard- und Software. Für Geräte mit einem Universalcomputer ist eine weitere Variante typisch: Die Verwendung von bereits bestehenden Ressourcen, z.B. Festplatten. Die dritte Variante ist der Wechseldatenträger: Hier kann der Speicher aus dem Gerät, das sowohl ein Messgerät mit zweckgebundener Hard- und Software als auch ein Messgerät mit Universalcomputer sein kann, entfernt und mitgenommen werden. Wenn Daten von Wechseldatenträgern für rechtliche Zwecke, wie Visualisierung, Belegdruck usw., abgefragt werden, muss das abfragende Gerät der rechtlichen Kontrolle unterliegen.

A) Integrierte Speicher Einfaches Gerät, zweckgebunden, keine von außen anwendbaren Werkzeuge oder Mittel für Bearbeiten oder Ändern von Daten, integrierter Speicher für Messdaten oder Parameter (z.B. RAM, Flash-Speicher, Festplatte) verfügbar.
B) Speicher des Universalcomputers Universalcomputer, grafische Benutzeroberfläche, Multitasking-Betriebssystem, Aufgaben, die der rechtlichen Kontrolle unterliegen, und solche, die ihr nicht unterliegen, bestehen parallel; der Speicher kann aus dem Gerät entfernt werden oder Inhalte können überall innerhalb oder außerhalb des Computers kopiert werden.
C) Wechseldatenträger oder entfernte (externe) Speicherung Beliebiges Grundgerät (Gerät mit zweckgebundener Hard- und Software oder Gerät mit Universalcomputer); der Speicher kann aus dem Gerät genommen werden. Dies können beispielsweise USB-Stick, Flash-Karten oder entfernte, über das Netzwerk angeschlossene Datenbanken sein.

Tabelle 6-1: Technische Beschreibung der Langzeitspeicherung

Durch Entschluss der zuständigen WELMEC-Arbeitsgruppen kann die Einstufung für ausgewählte Arten von Messgeräten reduziert werden (siehe Kapitel 10).

6.2 Spezifische Softwareanforderungen an die Langzeitspeicherung

Risikoklasse B	Risikoklasse C	Risikoklasse D
L1: Vollständigkeit der gespeichert Messdaten <i>Die gespeicherten Messdaten müssen von sämtlichen relevanten Informationen begleitet werden, die für rechtlich relevante Zwecke nötig sind.</i>		
Detaillierende Anmerkungen: 1. Die gespeicherten Messdaten müssen auf die Messung rückführbar sein, die die Daten erzeugt hat. 2. Die gespeicherten Messdaten müssen für die Kontrolle von Rechnungen ausreichend sein. 3. Die Art der notwendigen Informationen kann von der Geräteart abhängen. 4. Eine Voraussetzung, um diese besondere Anforderung zu erfüllen, ist die Identifizierung jedes gespeicherten Datensatzes.		
Erforderliche Dokumentation: Beschreibung aller Datensatzfelder.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob alle für die rechtlich relevanten Zwecke notwendigen Informationen im Datensatz enthalten sind.		
Beispiel einer akzeptablen Lösung: • Ein rechtlich und messtechnisch vollständiger Datensatz besteht aus den folgenden Feldern: ◦ Messwert(e) mit der richtigen Auflösung ◦ Maßeinheit ◦ Preis je Einheit oder zu zahlender Preis (falls zutreffend) ◦ Datum und Uhrzeit der Messung (falls zutreffend) ◦ Identifikator des Messgeräts ◦ Ort der Messung (falls zutreffend) • Die Daten werden mit der gleichen Auflösung, den gleichen Werten, Einheiten usw. gespeichert, wie auf dem Lieferschein angegeben oder ausgedruckt.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software, der die Datensätze für die Speicherung erzeugt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die Datensätze korrekt aufgebaut sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
L2: Schutz vor zufälliger oder unbeabsichtigter Änderung <i>Die gespeicherten Messdaten müssen vor zufälliger oder unbeabsichtigter Änderung geschützt sein.</i>		
Detaillierende Anmerkungen: 1. Mit den gespeicherten Daten sollen zufällige Datenänderungen infolge physikalischer Effekte (elektromagnetische Störung, Temperatur, Vibration usw.) erkannt werden. 2. Es sind Maßnahmen zum Schutz vor unbeabsichtigtem Ändern oder Löschen von Messdaten zu ergreifen.		
Erforderliche Dokumentation: Beschreibung der Sicherungsmaßnahmen.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen,</i> • ob eine Methode zur Erkennung zufälliger Datenänderungen implementiert ist. • ob die Methode alle Daten erfasst. • ob die Daten nicht vor Ende des vorgesehenen Datenspeicherungszeitraumes überschrieben werden können. • ob eine Warnung an den Benutzer ausgegeben wird, wenn er im Begriff ist, Messdaten-Files zu ändern oder zu löschen. <i>Funktionsprüfungen:</i> • Überprüfen durch geeignete Stichproben, ob vor dem Ändern/Löschen von Messdaten – sofern das Ändern/Löschen überhaupt möglich ist – eine Warnung erfolgt		
Beispiel einer akzeptablen Lösung: • Die gespeicherten Messdaten werden von zusätzlichen redundanten Informationen begleitet, um der Software Abruf, Auswertung und Anzeige der Daten zu ermöglichen (siehe L6) • Zum Aufdecken von Datenänderungen aufgrund physikalischer Effekte wird mit dem CRC-16-Algorithmus eine Prüfsumme über den gesamten Datensatz berechnet und in den zu speichernden Datensatz eingefügt. <i>Hinweis:</i> Der Algorithmus ist nicht geheim, und im Gegensatz zu Anforderung L3 ist weder der Startvektor des CRC-Registers noch das Generatorpolynom, d.h. der Divisor im Algorithmus, geheim. Startvektor und Generatorpolynom sind gleichermaßen beiden Programmen bekannt, welche die Prüfsummen erzeugen und überprüfen. • Messdaten bzw. Rechnungsdateien werden durch das Anbringen eines automatischen Zeitstempels bei der Erzeugung und eines Kennzeichens, ob die Rechnung bezahlt oder unbezahlt ist, geschützt. Ein Dienstprogramm löscht oder verschiebt Dateien nur, wenn die Rechnungen bezahlt sind oder die Aufbewahrungsfrist abgelaufen ist. • Messdaten werden nicht ohne vorherige Genehmigung gelöscht, z.B. mittels Dialog oder Fenster, die eine Löschbestätigung einholen. • Messdaten dürfen automatisch überschrieben werden, wenn ein angemessener Schutz der aufzubewahrenden Datensätze vorhanden ist. Ein Parameter, der die Mindestaufbewahrungszeit festlegt, kann bei Inbetriebnahme gemäß Nutzungsbedingungen und Datenspeichergröße eingestellt und gesichert werden. Das Gerät muss anhalten, wenn der Speicher voll und kein Datensatz alt genug zum Überschreiben ist. In diesem Fall kann manuelles Löschen (mit vorheriger Genehmigung) durchgeführt werden.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software, der den Schutz der gespeicherten Daten umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die zum Schutz der gespeicherten Daten getroffenen Maßnahmen angemessen sind und korrekt umgesetzt wurden.

Risikoklasse B	Risikoklasse C	Risikoklasse D
L3: Datenintegrität <i>Die gespeicherten Messdaten müssen vor vorsätzlichen Änderungen geschützt sein.</i>		
Detaillierende Anmerkungen: 1. Gespeicherte Daten in integrierten Speichern werden im Allgemeinen durch Hardware geschützt. Ein zusätzlicher Softwareschutz ist nicht notwendig. 2. Die Sicherung muss gegen beabsichtigte Änderungen wirksam sein, die von leicht verfügbaren und handhabbaren Softwaretools vorgenommen werden. 3. Die gespeicherten Messdaten müssen von zusätzlichen redundanten Informationen begleitet werden, um der Software Abruf, Auswertung und Anzeige der Daten oder anderweitige Verarbeitung zu ermöglichen, um die Datenintegrität zu verifizieren.		
	4. Der Schutz muss gegen vorsätzliche Änderungen wirksam sein, die durch spezielle, anspruchsvolle Softwaretools ausgeführt werden. 5. Was Algorithmen und minimale Schlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden. 6. Auch wenn Algorithmus und Schlüssel das hohe Niveau erfüllen, setzt eine technische Lösung mit einem Standard-PC dieses Schutzniveau nicht um, sofern es nicht geeignete Schutzmaßnahmen für die Programme gibt, die den Datensatz signieren oder überprüfen (siehe Basisleitfaden U für Universalcomputer, Kommentar auf Anforderung U6-Risikoklasse D).	
Erforderliche Dokumentation: Die Methode zur Umsetzung der Schutzmaßnahmen und zur Kennzeichnung der korrupten Daten muss dokumentiert sein.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - wenn eine Prüfsumme oder Signatur verwendet wird: ob die Prüfsumme oder Signatur über den gesamten Datensatz erzeugt wird und ob die rechtlich relevante Software, welche die Daten liest und eine Prüfsumme berechnet oder eine Signatur entschlüsselt, wirklich die berechneten Werte mit den Sollwerten vergleicht. - ob geheime Daten (z.B. Schlüsselinitialwert, falls verwendet) gegen das Ausspähen mit einfachen Werkzeugen geheim gehalten werden.	Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): <i>Auf Basis der Dokumentation ist zu überprüfen:</i> ob die getroffenen Maßnahmen dem geforderten hohen Schutzniveau gemäß dem Stand der Technik entsprechen.	

Beispiel für eine akzeptable Lösung: Gespeicherte Daten werden durch einen CRC-16-Algorithmus gesichert.	Beispiel einer akzeptablen Lösung: Gespeicherte Daten werden von einer kryptographischen Signatur gesichert.
Zusätze für Risikoklasse E	
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software, der die Integrität der gespeicherten Daten umsetzt.	
Validierungsanleitung (zusätzlich zur Anleitung für die Risikoklasse D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die zur Integritätssicherung getroffenen Maßnahmen angemessen und korrekt implementiert sind.	

Risikoklasse B	Risikoklasse C	Risikoklasse D
L4: Messtechnische Rückführung der gespeicherten Messdaten <i>Die gespeicherten Messdaten müssen authentisch auf die Messung rückführbar sein, bei der sie erzeugt wurden.</i>		
Detaillierende Anmerkungen: 1. Authentizität erfordert die korrekte Zuordnung (Verknüpfung) von Messdaten zu der Messung, bei der die Daten erzeugt wurden. 2. Rückführbarkeit erfordert die korrekte Zuordnung (Verknüpfung) von Messdaten zum Messgerät, das die Messdaten erzeugt hat. 3. Rückführbarkeit auf Messungen erfordert eine Identifizierung der Messungen. 4. Die Rückführbarkeit auf ein Messgerät setzt eine Identifizierung der Messgeräte voraus.		
Erforderliche Dokumentation: Beschreibung der Methode für die Gewährleistung der Authentizität.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob es eine korrekte Verknüpfung zwischen den einzelnen Messwerten und der zugehörigen Messung gibt. • bei Verwendung von Prüfsumme oder Signatur, ob die Prüfsumme oder Signatur über den gesamten Datensatz erzeugt wird. • ob geheime Daten (z.B. Schlüsselinitialwert, falls verwendet) gegen das Ausspähen mit einfachen Werkzeugen geheim gehalten werden. Funktionsprüfungen: • Überprüfen, ob die entsprechenden gespeicherten Daten und die auf den Beleg oder die Rechnung gedruckten Daten identisch sind. • Überprüfen, ob aus dem Beleg hervorgeht, dass die Messwerte mit den Referenzdaten auf einem Speichermedium, das der gesetzlichen Kontrolle unterliegt, verglichen werden können.		Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die getroffenen Maßnahmen dem geforderten hohen Schutzniveau gemäß dem Stand der Technik entsprechen.
Beispiel einer akzeptablen Lösung: Die gespeicherten Messdaten enthalten folgende Datenfelder: • Eine eindeutige (fortlaufende) Identifikationsnummer und eine Identifikation des Messgerätes, das den Wert erzeugt hat. Eine Signatur, die für die Gewährleistung der Datenintegrität verwendet wird, kann gleichzeitig für die Gewährleistung der Rückverfolgbarkeit verwendet werden. • Zeitpunkt, zu dem die Messung durchgeführt wurde (Zeitstempel) und das Messgerät identifiziert wurde, das den Wert erzeugt hat. <i>Hinweis:</i> Auf dem Beleg kann angegeben werden, dass die Messwerte mit den Referenzdaten auf einem Speichermedium, das der gesetzlichen Kontrolle unterliegt, verglichen werden können. Die Zuordnung wird durch Vergleich der Identifikationsnummer oder des Zeitstempels auf dem Lieferschein mit denjenigen, die sich im gespeicherten Datensatz befinden, nachgewiesen.		Beispiel einer akzeptablen Lösung: Zusätzlich zu der akzeptablen Lösung für die Risikoklassen B und C wird die Herkunft von Zertifikaten für die Signierung von Messdaten wird mit Hilfe einer PKI verifiziert.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode, der die Speicherdatensätze erzeugt und die Authentifizierung umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für die Risikoklasse D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die Datensätze korrekt aufgebaut sind und zuverlässig authentifiziert werden.

Risikoklasse B	Risikoklasse C	Risikoklasse D
L5: Geheimhaltung der Schlüssel <i>Schlüssel und zugehörige Informationen müssen wie Messdaten behandelt, geheim gehalten und vor Kompromittierung geschützt werden.</i>		
Detaillierende Anmerkungen: 1. Diese Anforderung gilt nur, wenn überhaupt ein geheimer Schlüssel verwendet wird. 2. Diese Anforderung gilt nur für die Messdatenspeicher, die sich außerhalb des Messgerätes befinden oder auf Universalcomputern umgesetzt sind. 3. Wenn der Zugang zu den geheimen Schlüsseln durch Hardware verhindert wird, so sind keine zusätzlichen Softwareschutzmaßnahmen erforderlich. 4. Die Sicherung muss gegen beabsichtigte Änderungen wirksam sein, die von leicht verfügbaren und handhabbaren Softwaretools vorgenommen werden. 5. Wenn eine Prüfsumme an Stelle eines Signaturalgorithmus verwendet wird, spielen der Startvektor oder das Generatorpolynom die Rolle eines Schlüssels.		
		6. Der Schutz muss gegen vorsätzliche Änderungen wirksam sein, die durch spezielle, anspruchsvolle Softwaretools ausgeführt werden. 7. Was Algorithmen und minimale Schlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden. 8. Eine technische Lösung mit einem Standard-PC reicht nicht aus, um das hohe Schutzniveau sicherzustellen, wenn es keine entsprechenden Hardwareschutzmaßnahmen für den Schlüssel und andere geheime Daten gibt (siehe Basisleitfaden für den Universalcomputer U6).
Erforderliche Dokumentation: Beschreibung des Schlüsselmanagements und der Maßnahmen zur Geheimhaltung der Schlüssel und der zugehörigen Informationen.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die geheimen Informationen nicht kompromittiert werden können.		Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die getroffenen Maßnahmen dem geforderten hohen Schutzniveau gemäß dem Stand der Technik entsprechen.

Beispiel einer akzeptablen Lösung: Der geheime Schlüssel und zugehörige Informationen sind in Binärformat im ausführbaren Code der rechtlich relevanten Software gespeichert. Die Systemsoftware bietet keine Funktionen zur Anzeige und zum Bearbeiten dieser Informationen.	Beispiel einer akzeptablen Lösung: Der geheime Schlüssel befindet sich in einem Hardwareteil, der versiegelt werden kann. Die Software bietet keine Funktionen zur Anzeige und zum Bearbeiten dieser Daten. • Der öffentliche Schlüssel der unter gesetzlicher Kontrolle stehenden Speicherung wurde von einem akkreditierten Trust Center zertifiziert. • Es ist möglich, den öffentlichen Schlüssel des Messgerätes direkt an dem gesetzlich geregelten Gerät abzulesen, das den betreffenden Datensatz erzeugt.
--	--

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode, der das Schlüsselmanagement umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für die Risikoklasse D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die für das Schlüsselmanagement getroffenen Maßnahmen angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
L6: Abrufen, Verifizieren und Anzeigen von gespeicherten Messdaten <i>Es muss rechtlich relevante Software für die Ablesung, Verifizierung und Anzeige gespeicherter Messdaten geben.</i>		
Detaillierende Anmerkungen: 1. Die Software muss in der Lage sein, die zusammen mit den relevanten Information (siehe L1) gespeicherten Messdaten anzuzeigen. 2. Die abgerufenen Daten sollten verifiziert sein. 3. Die angezeigten oder gedruckten Messdaten müssen einen möglichen Verstoß gegen die Rückführung und Integrität melden.		
Erforderliche Dokumentation: • Beschreibung der Funktionen der Abrufsoftware. • Beschreibung wie beschädigte Daten angezeigt werden.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die Abrufsoftware die erforderlichen Fähigkeiten hat <i>Funktionsprüfungen:</i> • Durchführung von Stichprobenüberprüfungen, um zu prüfen, ob der Abruf alle erforderlichen Informationen liefert.		
Beispiel einer akzeptablen Lösung: Die Integrität und Rückführung der gespeicherten Messdaten werden von einer Signatur über alle Datenfelder gesichert. Misslingt die Verifizierung der Signatur, werden die Messdaten als ungültig angezeigt oder ansonsten ausgedruckt.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der Abrufsoftware.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob getroffene Maßnahmen für Abfrage, Signaturüberprüfung usw. angemessen und richtig umgesetzt sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
L7: Automatisches Speichern <i>Die Messdaten müssen automatisch gespeichert werden, wenn die Messung abgeschlossen ist.</i>		
Detaillierende Anmerkungen: 1. Die Speicherfunktion darf nicht von der Entscheidung des Bedieners abhängen. 2. In Fällen, in denen der Bediener eine Entscheidung treffen muss, ob er ein Messergebnis akzeptiert oder nicht, müssen die Messdaten automatisch gespeichert werden, nachdem die Entscheidung getroffen wurde.		
Erforderliche Dokumentation: Beschreibung der automatischen Speicherung. Beschreibung der grafischen Benutzeroberfläche im Falle von bedienerabhängigen Speicherentscheidungen.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob der Speicherprozess automatisch abläuft. <i>Funktionsprüfungen:</i> • Stichprobenkontrollen, ob die Messwerte nach der Messung oder nach Abschluss der Messungsannahme automatisch gespeichert werden. Überprüfen, ob es keine Schaltflächen oder Menüpunkte zum Unterbrechen oder Deaktivieren der automatischen Speicherung gibt.		
Beispiel einer akzeptablen Lösung: In der grafischen Benutzeroberfläche (GUI) gibt es keinen Menüpunkt (oder Schaltfläche), der ein manuelles Anstoßen des Speicherns von Messergebnissen unterstützt. Die Messwerte werden zusammen mit zusätzlichen Informationen wie Zeitstempel und Signatur in einen Datensatz gepackt und sofort nach der Messung bzw. nach Annahme der Messung gespeichert.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die für die automatische Speicherung getroffenen Maßnahmen angemessen und korrekt umgesetzt sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
L8: Speicherkapazität und -dauer <i>Der Langzeitspeicher muss eine Kapazität besitzen, die für den beabsichtigten Zweck ausreichend ist.</i>		
Detaillierende Anmerkungen: 1. Wenn ein Speicher voll ist oder entfernt oder vom Gerät getrennt wird, muss eine Warnung an den Bediener gegeben werden. 2. Es muss sichergestellt sein, dass nur abgelaufene Daten überschrieben werden können. 3. Die Regelungen hinsichtlich des Mindestzeitraumes für die Speicherung von Messdaten und der geforderten Kennzeichnungen sind nationalen Regelungen überlassen und liegen daher außerhalb des Anwendungsbereiches dieses Leitfadens. 4. Die Informationen über die Speicherkapazität müssen verfügbar sein.		
Erforderliche Dokumentation: Speicherkapazität, Beschreibung der Managements der Messdatenspeicherung.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die Speicherkapazität oder eine Berechnungsformel dafür vom Hersteller angegeben wird. • ob das Überschreiben von Daten nicht vor Ende des Datenspeicherungszeitraumes eintreten kann, der durch den Hersteller vorgesehen und dokumentiert ist. <i>Funktionsprüfungen:</i> • Überprüfen, ob gegebenenfalls eine Warnung erfolgt, wenn der Speicher voll ist oder entfernt wurde.		
Beispiel einer akzeptablen Lösung: • Für unterbrechbare Messungen, wenn der Speicher nicht mehr verfügbar ist, bevor die Messung abgeschlossen ist: Das Messgerät hat einen Puffer, der groß genug für die Speicherung der aktuellen Messung ist. Es wird kein neuer Messvorgang begonnen und die gepufferten Werte werden zur späteren Übertragung in einen neuen Speicher aufbewahrt. • Nicht unterbrechbare Messungen: Das kumulative Register wird zu einem späteren Zeitpunkt, wenn der Speicher wieder verfügbar ist, ausgelesen und übertragen. • Messdaten werden automatisch von einem Tool überschrieben, das prüft, ob die Messdaten veraltet sind (den jeweiligen Zeitraum regeln nationale Bestimmungen). Das Dienstprogramm fordert die Löscherlaubnis vom Benutzer, und die Daten werden in der Reihenfolge „älteste zuerst“ gelöscht.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software, der die Datenspeicherung umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die für die automatische Speicherung getroffenen Maßnahmen angemessen und korrekt umgesetzt sind.

7 Anhang T: Messdatenübertragung über Kommunikationsnetze

Die spezifischen Anforderungen dieses Kapitels gelten nur, wenn Messdaten über Kommunikationsnetze zu einem entfernten Gerät übertragen werden, wo sie am Empfänger für rechtlich relevante Zwecke verwendet werden. Sie bilden einen Anhang zu den spezifischen Anforderungen sowohl an die Software eines Messgerätes mit zweckgebundener Hard- und Software (Typ-P-Anforderungen) als auch an die Software von Messgeräten mit Universalcomputer (Typ-U-Anforderungen).

Dieser Anhang gilt nicht, wenn es keine nachträgliche Messdaten-Verarbeitung gibt. Wenn Software auf ein Gerät heruntergeladen wird, das der gesetzlichen Kontrolle unterliegt, gelten die Anforderungen des Anhangs D.

7.1 Technische Beschreibung

In der folgenden Tabelle sind zwei Netzwerkkonfigurationen aufgezeigt.

Beschreibung von Konfigurationen	
A) Geschlossenes Netzwerk	Nur eine feste Anzahl von Teilnehmern mit eindeutiger Identität, Funktionsweise und Standort sind verbunden. Alle Geräte unterliegen der gesetzlichen Kontrolle.
B) Offenes Netz	Beliebige Teilnehmer (Geräte mit beliebiger Funktionsweise) können im Netz verbunden sein. Die Identität und Funktionsweise eines teilnehmenden Geräts und sein Standort kann den anderen Teilnehmern unbekannt sein. Jedes Netz, das gesetzlich kontrollierte Geräte mit Infrarot- oder Drahtlosnetzwerkkommunikationsschnittstellen enthält, gilt als offenes Netz.

Tabelle 7-1: Technische Beschreibung der Kommunikationsnetze.

7.2 Spezifische Softwareanforderungen an die Datenübertragung

Risikoklasse B	Risikoklasse C	Risikoklasse D
T1: Vollständigkeit der übertragenen Daten <i>Die übertragenen Daten müssen alle relevanten Informationen enthalten, die zur Darstellung oder Weiterverarbeitung der Messergebnisse in der Empfangseinheit nötig sind.</i>		
Detaillierende Anmerkungen: Die Vollständigkeit hängt individuell vom Typ der Messung ab.		
Erforderliche Dokumentation: Beschreibung aller Felder des Datensatzes.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob alle Informationen für die weitere Messwertverarbeitung in der Empfangseinheit im Datensatz enthalten sind.		
Beispiel einer akzeptablen Lösung: Der Datensatz umfasst die folgenden Felder: • Messwert(e) mit der richtigen Auflösung • rechtlich korrekte Maßeinheit • Preis je Einheit oder zu zahlender Preis (falls zutreffend) • Datum und Uhrzeit der Messung (falls zutreffend) • Identifikation des Geräts falls zutreffend (Datenübertragung) • Ort der Messung (falls zutreffend)		
Zusätze für Risikoklasse E		
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode, der die Datensätze zur Übertragung erzeugt.		
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die Datensätze korrekt aufgebaut sind.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
T2: Schutz vor zufälligen oder unbeabsichtigten Änderungen <i>Die übertragenen Daten müssen vor zufälliger oder unbeabsichtigter Änderung geschützt sein.</i>		
Detaillierende Anmerkungen: 1. Es sind Maßnahmen zum Schutz vor unbeabsichtigtem Ändern oder Löschen von Messdaten zu ergreifen.		
Erforderliche Dokumentation: Beschreibung der verwendeten Methoden zum Erkennen von Übertragungsfehlern.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen,</i> • ob eine Methode zum Erkennen von Übertragungsfehlern umgesetzt ist		
Beispiel einer akzeptablen Lösung: • Die übertragenen Messdaten müssen von zusätzlichen redundanten Informationen begleitet werden, damit die Software des Empfängers zufällige Datenübertragungsfehler entdecken kann. • Zum Aufdecken von Datenänderungen wird mit dem CRC-16-Algorithmus eine Prüfsumme für sämtliche Bytes den gesamten Datensatz berechnet und in den zu übertragenden Datensatz eingefügt. Vor der Wiederverwendung der Daten wird der Wert der Prüfsumme vom Empfänger neu berechnet und mit dem beigefügten Sollwert verglichen. Wenn die Werte übereinstimmen, ist der Datensatz gültig und kann verwendet werden, andernfalls muss er gelöscht oder als ungültig markiert werden. <i>Hinweis:</i> Der Algorithmus ist nicht geheim, und im Gegensatz zu Anforderung T3, sind es weder der Startvektor des CRC-Registers noch das Generatorpolynom, d.h. der Divisor im Algorithmus. Startvektor und Generatorpolynom sind gleichermaßen beiden Programmen bekannt, welche die Prüfsummen erzeugen und überprüfen. • Nutzung von Mitteln, die von den Übertragungsprotokollen, z.B. TCP/IP, IFSF, bereitgestellt werden.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software, der den Schutz der übertragenen Daten umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die zum Schutz der übertragenen Daten getroffenen Maßnahmen angemessen sind und korrekt umgesetzt wurden.

Risikoklasse B	Risikoklasse C	Risikoklasse D
T3: Datenintegrität <i>Die gespeicherten Messdaten müssen vor vorsätzlichen Änderungen geschützt sein.</i>		
Detaillierende Anmerkungen: 1. Diese Anforderung bezieht sich nur auf offene Netze, nicht auf geschlossene Netze. 2. Die Sicherung muss gegen beabsichtigte Änderungen wirksam sein, die von leicht verfügbaren und handhabbaren Softwaretools vorgenommen werden.		
		3. Der Schutz muss gegen vorsätzliche Änderungen wirksam sein, die durch spezielle, anspruchsvolle Softwaretools ausgeführt werden. 4. Was Algorithmen und minimale Schlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden. 5. Um die hohe Schutzstufe zu erfüllen, sind geeignete Schutzmittel für die Software (z.B. Hardwareunterstützung), die einen Datensatz signiert oder verifiziert, notwendig (siehe auch Kapitel 5 für Software auf Universalcomputern, spezielle Anforderung U6, Detaillierende Anmerkung 6 für Risikoklasse D).
Erforderliche Dokumentation: Beschreibung der Schutzmethode.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> ob eine angemessene Methode ausgewählt wurde.		
Beispiel einer akzeptablen Lösung: • Die übertragenen Messdaten müssen von zusätzlichen redundanten Informationen begleitet werden, damit die Software des Empfängers zufällige Datenübertragungsfehler entdecken kann. • Eine Prüfsumme von dem zu übertragenden Datensatz wird erzeugt. Vor Wiederverwendung der Daten wird die Prüfsumme neu berechnet und mit dem Sollwert verglichen, der im empfangenen Datensatz enthalten ist. Wenn die Werte übereinstimmen, ist der Datensatz gültig und kann verwendet werden, andernfalls muss er gelöscht oder als ungültig markiert werden. • Eine akzeptable Lösung ist der CRC-16-Algorithmus. <i>Hinweis:</i> Der Algorithmus ist nicht geheim, aber im Gegensatz zu Anforderung T2 muss der Startvektor des CRC-Registers oder das Generatorpolynom (d.h. der Divisor im Algorithmus) geheim sein. Der Startvektor und das Generatorpolynom sind nur den Programmen bekannt, welche die Prüfsummen erzeugen und überprüfen. Sie müssen wie Schlüssel behandelt werden (siehe T5).		Beispiel einer akzeptablen Lösung: • Die übertragenen Messdaten müssen von zusätzlichen redundanten Informationen begleitet werden, damit die Software des Empfängers zufällige Datenübertragungsfehler entdecken kann. • Anstelle des CRC wird eine Signatur berechnet. • Schutz ist durch einige Übertragungsprotokolle wie z.B. HTTPS, TLS gegeben.
Zusätze für Risikoklasse E		
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software, der die Integrität der übertragenen Daten umsetzt.		

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D):

Auf Basis des Quellcodes ist zu überprüfen:

- ob die Maßnahmen angemessen sind, die zur Integritätsgarantie der übertragenen Daten getroffen wurden.

Risikoklasse B	Risikoklasse C	Risikoklasse D
T4: Rückführbarkeit der übertragenen Messdaten <i>Die gespeicherten Messdaten müssen auf die Messung und das Messgerät rückführbar sein, die die Daten erzeugt hat.</i>		
Detaillierende Anmerkungen: 1. Diese Anforderung bezieht sich nur auf offene Netze, nicht auf geschlossene Netze. 2. Die Rückführbarkeit erfordert die korrekte Zuordnung (Verknüpfung) von Messdaten zu der Messung, bei der die Daten erzeugt wurden. 3. Rückführbarkeit erfordert die korrekte Zuordnung (Verknüpfung) von Messdaten zum Messgerät, das die Messdaten erzeugt hat. 4. Die Rückführbarkeit auf Messungen erfordert eine Identifizierung der Messungen. 5. Die Rückführbarkeit auf ein Messgerät setzt eine Identifizierung der Messgeräte voraus. 6. Die Sicherung muss gegen beabsichtigte Änderungen wirksam sein, die von leicht verfügbaren und handhabbaren Softwaretools vorgenommen werden.		
		7. Der Schutz muss gegen vorsätzliche Änderungen wirken, die durch spezielle, anspruchsvolle Softwaretools ausgeführt werden. 8. Was Algorithmen und minimale Schlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden.
Erforderliche Dokumentation: • Beschreibung der Authentifizierungsmittel.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> dass die Authentifizierungsmittel angemessen sind.		
Beispiel einer akzeptablen Lösung: • Jeder Datensatz hat eine eindeutige (sequentielle) Identifikationsnummer, die den Zeitpunkt enthalten kann, zu dem die Messung genommen wurde (Zeitstempel). • Jeder Datensatz enthält Informationen über die Herkunft der Messdaten, d.h. die Seriennummer oder ein Identitätsmerkmal des Messgerätes, das den Wert erzeugt hat. • In offenen Netzwerken wird die Authentizität gewährleistet, wenn der Datensatz eine eindeutige Signatur trägt. Die Signatur deckt alle diese Felder des Datensatzes ab. • Der Empfänger des Datensatzes überprüft alle Daten auf Plausibilität.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software für das sendende und das empfangende Gerät.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die Maßnahmen angemessen sind, die zur Gewährleistung der Authentizität der übertragenen Daten ergriffen wurden.

Risikoklasse B	Risikoklasse C	Risikoklasse D
T5: Geheimhaltung der Schlüssel <i>Schlüssel und zugehörige Informationen müssen wie Messdaten behandelt, geheim gehalten und vor Kompromittierung geschützt werden.</i>		
Detaillierende Anmerkungen: 1. Diese Anforderung gilt nur, wenn überhaupt ein geheimer Schlüssel verwendet wird. 2. Die Sicherung muss gegen beabsichtigte Änderungen wirksam sein, die von leicht verfügbaren und handhabbaren Softwaretools vorgenommen werden. 3. Wenn der Zugang zu den geheimen Schlüsseln durch Hardware verhindert wird, so sind keine zusätzlichen Softwareschutzmaßnahmen erforderlich.		
	4. Die Sicherung muss gegen beabsichtigte Änderungen anwendbar sein, die von spezielle, anspruchsvolle Softwaretools ausgeführt werden. 5. Was Algorithmen und minimale Schlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden. 6. Eine technische Lösung mit einem Standard-PC reicht nicht aus, um das hohe Schutzniveau sicherzustellen, wenn es keine entsprechenden Hardwareschutzmaßnahmen für den Schlüssel und andere geheime Daten gibt (siehe Basisleitfaden für den Universalcomputer U6).	
Erforderliche Dokumentation: Beschreibung des Schlüsselmanagements und der Maßnahmen zur Geheimhaltung der Schlüssel und der zugehörigen Informationen.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die geheimen Informationen nicht kompromittiert werden können.	Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die getroffenen Maßnahmen dem geforderten hohen Schutzniveau gemäß dem Stand der Technik entsprechen.	
Beispiel einer akzeptablen Lösung: Der geheime Schlüssel und zugehörige Informationen sind in Binärformat im ausführbaren Code der rechtlich relevanten Software gespeichert. Es ist dann nicht ersichtlich, an welcher Adresse diese Daten gespeichert sind. Die Systemsoftware bietet keine Funktionen zur Anzeige und zum Bearbeiten dieser Informationen. Wenn der CRC-Algorithmus anstelle eines Signaturalgorithmus verwendet wird, spielen der Startvektor oder das Generatorpolynom die Rolle eines Schlüssels.	Beispiel einer akzeptablen Lösung: Der geheime Schlüssel befindet sich in einem Hardwareteil, der versiegelt werden kann. Die Software bietet keine Funktionen zur Anzeige und zum Bearbeiten dieser Daten. • Der öffentliche Schlüssel der unter gesetzlicher Kontrolle stehenden Speicherung wurde von einem akkreditierten Trust Center zertifiziert. • Es ist möglich, den öffentlichen Schlüssel des Messgerätes direkt an dem gesetzlich geregelten Gerät abzulesen, das den betreffenden Datensatz erzeugt.	

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software, der das Schlüsselmanagement umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für die Risikoklasse D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die für das Schlüsselmanagement getroffenen Maßnahmen angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
T6: Empfang, Verifizierung und Handhabung übertragener Messdaten <i>Es muss rechtlich relevante Software für die Anzeige oder den Ausdruck gespeicherter Messdaten geben.</i>		
Detaillierende Anmerkungen: 1. Obwohl Kommunikationsprotokolle normalerweise die Übertragung wiederholen, bis sie gelingt, ist es trotzdem möglich, dass ein beschädigter Datensatz empfangen wird. 2. Die angezeigten oder gedruckten Messdaten müssen einen möglichen Verstoß gegen die Rückführung und Integrität melden.		
Erforderliche Dokumentation: Beschreibung der Ermittlung beschädigter Daten.		
Validierungsanleitung: <i>Dokumentations- und funktionsabhängige Überprüfungen:</i> • Überprüfung, ob beschädigte Daten erkannt und markiert werden.		
Beispiel einer akzeptablen Lösung: Wenn das Programm, das Datensätze empfängt, verifiziert und behandelt, die Signatur nicht validieren kann, versucht es zunächst den ursprünglichen Wert zu rekonstruieren, wenn redundante Informationen verfügbar sind. Wenn das Wiederherstellen fehlschlägt, erzeugt es eine Warnung an den Benutzer, gibt den Messwert nicht aus und setzt in einem speziellen Feld des Datensatzes (Statusfeld) ein Flag mit der Bedeutung "nicht gültig".		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software im empfangenden Gerät.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die getroffenen Maßnahmen für die Handhabung mit beschädigten Daten angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
T7: Übertragungsverzögerung <i>Die Messung darf durch eine Übertragungsverzögerung nicht in unzulässiger Weise beeinflusst werden.</i>		
Detaillierende Anmerkungen: Das Zeitverhalten der Datenübertragung muss so organisiert werden, dass unter den ungünstigsten Bedingungen die Messung nicht unzulässig beeinflusst wird.		
Erforderliche Dokumentation: Beschreibung des Konzepts, wie die Messung bei Übertragungsverzögerungen geschützt wird.		
Validierungsanleitung: • Überprüfen des Konzeptes, das gewährleistet, dass die Messung durch Übertragungsverzögerungen nicht beeinflusst wird.		
Beispiel einer akzeptablen Lösung: Umsetzung der Übertragungsprotokolle für Feldbusse.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B, C und D geforderten Dokumentation): Quellcode der rechtlich relevanten Software, der die Datenübertragung umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> ob die für die Handhabung von Übertragungsverzögerungen getroffenen Maßnahmen angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
T8: Verfügbarkeit von Übertragungsdiensten <i>Wenn Netzwerkdienste nicht verfügbar sind, dürfen keine Messdaten verloren gehen.</i>		
Detaillierende Anmerkungen: - Es darf nicht möglich sein, Messdaten durch Verzögern oder Unterdrücken der Übertragung zu korrumpieren. - Das sendende Gerät muss in der Lage sein, mit zufällig auftretenden Übertragungsstörungen umzugehen. - Die Reaktion des Messgerätes, wenn die Übertragungsdienste nicht verfügbar sind, hängt vom Messprinzip ab (siehe Anhang I).		
Erforderliche Dokumentation: Beschreibung der Schutzmaßnahmen gegen Übertragungsunterbrechung oder andere Fehler.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - welche Maßnahmen angewendet werden, um die Messdaten bei Übertragungsstörungen und Unterbrechung zu schützen. <i>Funktionsprüfungen:</i> - Stichprobenüberprüfungen, ob keine relevanten Daten aufgrund einer Übertragungsunterbrechung verloren gehen.		
Beispiel einer akzeptablen Lösung: - Für unterbrechbare Messungen, deren Messung beendet wird, obwohl die Übertragung unterbrochen ist. Jedoch muss das Messgerät oder das Gerät, das die rechtlich relevanten Daten überträgt, einen Puffer haben, der groß genug für die Speicherung der aktuellen Messung ist. Danach kann keine neue Messung gestartet werden und die gepufferten Werte müssen für die spätere Übertragung aufbewahrt werden. Für weitere Beispiele siehe Anhang I. - Nicht unterbrechbare Messungen: Das kumulative Register kann zu einem späteren Zeitpunkt ausgelesen und übertragen werden, wenn die Verbindung wieder besteht.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software, der die Datenübertragung umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> ob die Maßnahmen für die Reaktion auf unterbrochenen Übertragungsdienste angemessen sind.

8 Anhang S: Softwaretrennung

Softwaretrennung ist eine optionale Entwurfsmethodik, die es ermöglicht, rechtlich relevante Software von rechtlich nicht relevanter Software zu trennen. Die Kommunikation zwischen diesen Softwareteilen wird über kontrollierte Schnittstellen durchgeführt. Befolgt der Hersteller die Bedingungen für die Softwaretrennung, so braucht er im Falle eines Austauschs von rechtlich nicht relevanter Software nicht die Konformitätsbewertungsverfahren zu durchlaufen.

Die spezifischen Anforderungen dieses Anhangs sind gegebenenfalls zusätzlich zu den Basisanforderungen für die Typen P oder U zu berücksichtigen, die in den Kapiteln 4 bzw. 5 dieses Leitfadens beschrieben sind.

8.1 Technische Beschreibung

Softwaregesteuerte Messgeräte oder -systeme haben im Allgemeinen komplexe Funktionen und enthalten Module, die rechtlich relevant sind, und Module, die es nicht sind. Es ist von Vorteil – wenn auch nicht vorgeschrieben – diese Softwaremodultypen zu trennen.

8.2 Spezifische Softwareanforderungen an die Softwaretrennung

Risikoklasse B	Risikoklasse C	Risikoklasse D
S1: Umsetzung der Softwaretrennung <i>Ein Teil der Software, der eindeutig von anderen Softwareteilen getrennt ist, muss alle rechtlich relevanten Software und Parameter enthalten.</i>		
Detaillierende Anmerkungen: 1. Alle <i>Programmteile</i> (Programmeinheiten, Unterprogramme, Prozeduren, Funktionen, Klassen, Programme, Bibliotheken usw.), - die zur Berechnung von Messwerten beitragen oder einen Einfluss darauf haben, - die zu Zusatzfunktionen wie Datenanzeige, Datensicherung, Datenspeicherung, Softwareidentifikation, Ausführung von Softwaredownload, Datenübertragung oder -speichern, Überprüfung empfangener oder gespeicherter Daten usw. beitragen. gehören zur rechtlich relevanten Software. Alle <i>Variablen, temporären Dateien und Parameter</i> , die Einfluss auf den Messwert oder auf rechtlich relevante Software haben, gehören ebenfalls zur rechtlich relevanten Software. 2. Die rückwirkungsfreie Softwareschnittstelle (siehe S3) ist Teil der rechtlich relevanten Software. 3. Die rechtlich nicht relevante Software umfasst die restlichen Programmeinheiten, Daten oder Parameter, die oben nicht aufgeführt wurden.		
Erforderliche Dokumentation: Benennung sämtlicher Komponenten, die zur rechtlich relevanten Software gehören.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> ob die Benennung korrekt und die Liste der genannten Komponenten vollständig ist.		
Beispiel einer akzeptablen Lösung:		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> ob alle Programmeinheiten, Programme oder Bibliotheken, die an der Messwertverarbeitung beteiligt sind, als rechtlich relevante Software aufgelistet sind. (Überprüfen z.B. durch Datenflussanalyse mit Softwaretools oder manuell).

Risikoklasse B	Risikoklasse C	Risikoklasse D
S2: Gemischte Anzeige <i>Informationen, die von rechtlich nicht relevanter Software erzeugt werden, müssen auf einem Display oder Ausdruck so angezeigt werden, dass sie nicht mit den Informationen verwechselt werden können, die aus der rechtlich relevanten Software stammen.</i>		
Detaillierende Anmerkungen: ---		
Erforderliche Dokumentation: Beschreibung der rechtlich relevanten Software, die die Anzeige erzeugt. Beschreibung, wie die Anzeige der rechtlich relevanten Informationen vor irreführenden Anzeigen geschützt ist, die durch rechtlich nicht relevante Software erzeugt werden.		
Validierungsanleitung: <i>Funktionsprüfungen:</i> Durch Sichtkontrolle beurteilen, ob Zusatzinformationen, die von rechtlich nicht relevanter Software erzeugt und auf dem Display dargestellt oder ausgedruckt werden, nicht mit den Informationen aus rechtlich relevanter Software verwechselt werden können.		
Beispiel einer akzeptablen Lösung: Falls zusätzliche Informationen, die nicht rechtlich relevant sind, neben den rechtlich relevanten Teilen, z.B. einem Produktidentifikator, angezeigt werden, wird eine Anzeigestruktur festgelegt, die von der rechtlich relevanten Software kontrolliert wird. Damit alle rechtlich relevanten Informationen aus einer Eingabereihe entnommen werden, sollten sie einen Filter durchlaufen, der Teil der rechtlich relevanten Software ist und unzulässige Informationen, wie z.B. Maßeinheiten, erkennt. Die zulässigen Informationen werden dann, gesteuert durch die rechtlich relevante Software, in die Anzeigestruktur eingefügt.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> - ob die rechtlich relevante Software die Anzeige der Messwerte erzeugt, - ob die durchgeführte Umsetzung der gemischten Anzeige korrekt ist. - ob diese Anzeige von rechtlich nicht relevanten Programmen nicht geändert oder unterdrückt werden kann.

Risikoklasse B	Risikoklasse C	Risikoklasse D
S3: Die rückwirkungsfreie Softwareschnittstelle <i>Der Datenaustausch zwischen der rechtlich relevanten und der rechtlich nicht relevanten Software muss ausschließlich über eine rückwirkungsfreie Softwareschnittstelle durchgeführt werden</i>		
Detaillierende Anmerkungen: 1. Diese Anforderung gilt für alle Arten von Wechselwirkungen und den Datenaustausch zwischen der rechtlich relevanten und der rechtlich nicht relevanten Software. 2. Die gesamte Kommunikation muss ausschließlich über die definierte rückwirkungsfreie Softwareschnittstelle ausgeführt werden. 3. Es sind nur Wechselwirkungen und Datenflüsse erlaubt, die den Messprozess, und insbesondere die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten nicht unzulässig beeinflussen. 4. Zeitablaufsteuerung und Laufzeit des Messprozesses dürfen nicht von der rechtlich nicht relevanten Software beeinflusst werden.		
Erforderliche Dokumentation: Beschreibung der Softwareschnittstelle • Beschreibung der Schnittstelle einschließlich der Beschreibung der erlaubten Wechselwirkungen und Datenflüsse.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die Funktionen der rechtlich relevanten Software und Aktionen des Messprozesses, die über die rückwirkungsfreie Softwareschnittstelle ausgelöst werden können, definiert und beschrieben sind, • ob die Daten, die über die rückwirkungsfreie Softwareschnittstelle ausgetauscht werden können, definiert und beschrieben sind, • Es sind Plausibilitätsprüfungen durchzuführen, ob die Beschreibung der Wechselwirkungen und des Datenaustauschs vollständig ist.		
Beispiel einer akzeptablen Lösung: • Die Datenbereiche der rechtlich relevanten Software sind durch Vereinbarung als nur lokale Variable im rechtlich relevanten Teil gekapselt. • Die Schnittstelle ist als ein Unterprogramm realisiert, das zur rechtlich relevanten Software gehört und von der rechtlich nicht relevanten Software aufgerufen wird. Die Daten, die zur rechtlich relevanten Software übermittelt werden, werden als Parameter des Unterprogramms weitergegeben. • Die rechtlich relevante Software filtert unzulässige Schnittstellenbefehle heraus.		
Zusätze für Risikoklasse E		
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.		
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob im Softwareentwurf der Datenfluss in der rechtlich relevanten Software eindeutig definiert ist und überprüft werden kann, • der Datenfluss über die Softwareschnittstelle (mittels geeigneter Softwaretools oder manuell). Es ist zu überprüfen, ob der vollständige Datenfluss zwischen den Softwareteilen dokumentiert wurde. Nach unzulässigen Datenflüssen ist zu suchen. • ob die von rechtlich nicht relevanter Software ausgelösten Wechselwirkungen dokumentiert sind. Nach unzulässigen Wechselwirkungen ist zu suchen.		

9 Anhang D: Download von rechtlich relevanter Software

Dieser Anhang ist zu verwenden, wenn Geräte so ausgestattet sind, dass bei einem Softwaredownload keine Versiegelung aufgebrochen wird. Die spezifischen Anforderungen dieses Anhangs sind gegebenenfalls zusätzlich zu den Basisanforderungen für Typ-P- bzw. Typ-U-Instrumente zu berücksichtigen, die in den Kapiteln 4 und 5 dieses Leitfadens beschrieben sind.

Der vorliegende Leitfaden schreibt nicht vor, ob ein Softwaredownload auf in Verwendung befindliche Geräte ohne Aufbrechen einer Versiegelung erlaubt ist oder nicht. Wenn jedoch ein Download ohne Aufbrechen der Versiegelung erlaubt ist, sind die unten aufgeführten spezifischen Anforderungen zu berücksichtigen.

9.1 Technische Beschreibung

Der Rahmen von Konfigurationen, die grundsätzlich für einen Softwaredownload geeignet sind, ist groß. Es wird in der folgenden Tabelle beschrieben:

Hardwarekonfiguration Das Gerät, welches für einen Softwaredownload ausgerüstet ist, kann ein Messgerät mit zweckgebundener Hard- und Software (Typ P) oder ein Gerät mit Universalrechner (Typ U) sein. Die Kommunikationsanschlüsse für die Softwareübertragung können direkt (z.B. RS 232, USB), über geschlossene Netze, (z.B. Ethernet, Token-Ring-LAN), oder über offene Netze (z.B. Internet) erfolgen.
Softwarekonfiguration Die gesamte herunterzuladende Software kann rechtlich relevant sein oder es kann eine Trennung zwischen rechtlich relevanter und rechtlich nicht relevanter Software geben. In letzterem Fall muss nur der Download der rechtlich relevanten Software die im Folgenden aufgeführten Anforderungen erfüllen. Ein Download von rechtlich nicht relevanter Software ist uneingeschränkt erlaubt, vorausgesetzt, die Softwaretrennung wurde zertifiziert.

Tabelle 9-1: Technische Beschreibung der Konfigurationen für den automatischen Softwaredownload

Der Softwaredownload besteht aus zwei (logischen) Phasen: 1) Aus dem Übertragungsprozess zum Messgerät und 2) aus der Installation der übertragenen Software.

9.2 Spezifische Softwareanforderungen

Risikoklasse B	Risikoklasse C	Risikoklasse D
D1: Download-Mechanismus <i>Beide Phasen des Softwaredownloads, die Übertragung und die anschließende Installation der Software müssen automatisch erfolgen und dürfen den Schutz der rechtlich relevanten Software nicht beeinträchtigen.</i>		

Detaillierende Anmerkungen:

1. Das Gerät muss mit rechtlich relevanter Software ausgestattet werden, welche die in D2 bis D4 geforderten Prüffunktionen durchführt.
2. Das Gerät muss in der Lage sein zu erkennen, wenn die Übertragung der Software oder die anschließende Installation fehlschlagen. Es muss eine Warnung ausgegeben werden. Wenn Übertragung oder Installation nicht erfolgreich sind oder unterbrochen werden, muss der ursprüngliche Zustand des Messgerätes erhalten bleiben. Alternativ kann das Gerät eine ständige Fehlermeldung anzeigen und seine Messfunktion sperren, bis der Fehler behoben ist.
3. Bei erfolgreichem Abschluss der Installation müssen alle Schutzmaßnahmen aktiviert werden.
4. Während der Übertragung und der anschließenden Installation der Software, muss die Messung durch das Gerät gesperrt werden oder es muss sichergestellt sein, dass die Messung korrekt abläuft.
5. Die Anzahl der Übertragungswiederholungen und Installationsversuche muss sinnvoll begrenzt werden.

Erforderliche Dokumentation:

Die Dokumentation muss beschreiben, wie die in den Detaillierenden Anmerkungen genannten Bedingungen umgesetzt werden.

Validierungsanleitung:

Es ist zu überprüfen, ob die in den detaillierenden Anmerkungen angegebenen Bedingungen erfüllt sind.

Funktionsprüfungen:

- Durchführen von mindestens einem Softwaredownload zur Überprüfung seines korrekten Ablaufs.

Beispiel einer akzeptablen Lösung:

Der gesamte rechtlich relevante Softwareteil ist festgeschrieben, d.h. er kann nicht ohne Brechen eines Siegels heruntergeladen oder geändert werden.

Ein im rechtlich relevanten Teil der Software angesiedeltes Hilfsprogramm, das:

- a. sich mit dem Sender synchronisiert und die Genehmigung überprüft,
- b. automatisch das Messen während der Übertragung und Installation sperrt,
- c. automatisch die rechtlich relevante Software auf einen sicheren Zwischenspeicher herunterlädt,
- d. automatisch die nach D2 bis D4 erforderlichen Überprüfungen ausführt,
- e. automatisch die Software an der richtigen Stelle installiert,
- f. sich um die Verwaltung kümmert, z.B. überflüssige Dateien löscht usw.,
- g. dafür sorgt, dass jeder Schutz, der zur Erleichterung von Übertragung und Installation entfernt wurde, nach Abschluss automatisch auf das erforderliche Niveau erneuert wird,
- h. die entsprechende Fehlerbehandlungsprozeduren einleitet, wenn ein Fehler auftritt.

Es muss möglich sein, in Mitgliedstaaten, in denen ein Softwaredownload für in Verwendung befindliche Geräte nicht erlaubt ist, den Software-Download-Mechanismus mittels einer versiegelbaren Einrichtung (Schalter, gesicherter Parameter) zu deaktivieren. In diesem Fall darf es nicht möglich sein, rechtlich relevante Software ohne Beschädigung des Siegels herunterzuladen.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode des rechtlich relevanten Softwareteils, der für die Handhabung des Downloadprozesses verantwortlich ist.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D):

Auf Basis des Quellcodes ist zu überprüfen:

- ob die zur Ausführung des Downloadprozesses getroffenen Maßnahmen angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
D2: Authentifizierung der übertragenen Software <i>Es müssen Maßnahmen getroffen werden, die sicherstellen, dass die übertragene Software authentisch ist.</i>		
Detaillierende Anmerkungen: - Bevor die übertragene Software installiert wird, ist zu überprüfen, ob: - die Software authentisch ist, - die Software zum Messgerät gehört, auf dem es installiert werden soll. - Ein negatives Prüfergebnis ist als Übertragungsfehler anzusehen und gemäß D1 zu behandeln		
		3. Was Algorithmen und minimale Schlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden.
Erforderliche Dokumentation: Die Dokumentation muss beschreiben, wie die in den Detaillierenden Anmerkungen genannten Überprüfungen ausgeführt werden.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - ob die beschriebenen Überprüfungen angemessen sind <i>Funktionsprüfungen:</i> - Überprüfung, dass die Installation nicht authentischer oder nicht zum Gerät gehörender Software gesperrt ist.		
Beispiel einer akzeptablen Lösung: Authentizität: Aus Gründen der Integrität (siehe D3) wird eine elektronische Signatur über den Softwareteil erzeugt, der heruntergeladen werden soll. Die Authentizität ist gewährleistet, wenn ein Schlüssel, der im rechtlich relevanten Softwareteil des Geräts gespeichert ist, die Herkunft der Signatur von der autorisierten Stelle bestätigt. Der Abgleich der Signatur erfolgt automatisch. Der Schlüssel kann nur durch Brechen eines Siegels ausgetauscht werden. Richtige Messgerätebauart Die Überprüfung der Gerätebauart erfordert den automatischen Abgleich der Gerätebauartidentifikation, die im rechtlich relevanten Softwareteil des Gerätes gespeichert ist, mit einer Kompatibilitätsliste, die der Software beigelegt ist.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode des rechtlich relevanten Softwareteils, der für die Authentizitätsüberprüfung zuständig ist.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> ob Maßnahmen für die Überprüfung der in den detaillierenden Anmerkungen aufgeführten Bedingungen getroffen werden.

Risikoklasse B	Risikoklasse C	Risikoklasse D
D3: Integrität der heruntergeladenen Software <i>Es müssen Maßnahmen getroffen werden, die sicherstellen, dass die Software während der Übertragung nicht verändert wurde.</i>		
Detaillierende Anmerkungen: 1. Bevor die übertragene Software installiert wird, ist zu überprüfen, ob die Software während der Übertragung unverändert blieb. 2. Ein negatives Prüfergebnis ist als Übertragungsfehler anzusehen und gemäß D1 zu behandeln		
		3. Was Algorithmen und minimale Schlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden.
Erforderliche Dokumentation: Die Dokumentation muss beschreiben, wie die Überprüfungen durchgeführt werden.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die beschriebene Überprüfung angemessen ist. <i>Funktionsprüfungen:</i> • Überprüfung, ob die Installation von geänderter Software verhindert wird.		
Beispiel einer akzeptablen Lösung: • Integrität kann dadurch nachgewiesen werden, dass eine Prüfsumme über die rechtlich relevante Software gebildet und mit der Prüfsumme verglichen wird, die der Software beigelegt ist. • Akzeptabler Algorithmus: CRC, geheimer Startvektor, Länge 32 Bit. Der Startvektor ist im rechtlich relevanten Softwareteil gespeichert.		Beispiel einer akzeptablen Lösung: • SHA mit RSA wird als ein Signaturalgorithmus verwendet. Der Schlüssel für die Entschlüsselung wird im rechtlich relevanten Softwareteil gespeichert und kann nicht ohne Brechen eines Siegels ausgetauscht werden.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode des rechtlich relevanten Softwareteils, der für die Integritätsüberprüfung der Software verantwortlich ist.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die zur Integritätsüberprüfung ergriffenen Maßnahmen angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
D4: Rückverfolgbarkeit des Downloads rechtlich relevanter Software <i>Mit Hilfe geeigneter technischer Mittel muss gewährleistet werden, dass Downloads rechtlich relevanter Software für spätere Kontrollen im Gerät in geeigneter Form zurückverfolgt werden können.</i>		
Detaillierende Anmerkungen: 1. Sämtliche relevanten Daten, die einen Download oder einen Downloadversuch nachvollziehbar machen, müssen aufgezeichnet und gesichert werden. Relevante Daten umfassen Datum und Zeit des Downloads, Identifikator(en) der Software, Herkunft der Übertragung sowie eine Erfolgsnotiz. 2. Die aufgezeichneten Daten müssen für einen angemessenen Zeitraum zur Verfügung stehen (der Zeitraum hängt von Regelungen außerhalb der MID ab). 3. Die aufgezeichneten Daten müssen auf Verlangen vorgezeigt werden. 4. Die Mittel und Aufzeichnungen zur Sicherung der Rückverfolgbarkeit sind Teil der rechtlich relevanten Software und müssen als solche geschützt werden.		
Erforderliche Dokumentation: Die Dokumentation muss beschreiben, • wie die Mittel zur Rückverfolgbarkeit umgesetzt und geschützt sind. • welche Struktur die Aufzeichnungen haben, • wie die aufgezeichneten Daten dargestellt werden können		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die umgesetzten Mittel zur Sicherung der Rückverfolgbarkeit die in den Detaillierenden Anmerkungen aufgeführten Bedingungen erfüllen. <i>Funktionsprüfungen:</i> • Überprüfung der Funktionalität dieser Mittel während eines Softwaredownloads		Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die getroffenen Maßnahmen dem geforderten hohen Schutzniveau gemäß dem Stand der Technik entsprechen.
Beispiel einer akzeptablen Lösung: • Logbuch. Das Messgerät ist mit einem Logbuch ausgestattet, das automatisch zumindest das Datum und den Zeitpunkt des Downloads, den Identifikator der heruntergeladenen rechtlich relevanten Software, den Identifikator der herunterladenden Stelle und einen Erfolgseintrag aufzeichnet. Für jeden Downloadversuch, unabhängig davon, ob dieser erfolgreich war oder nicht, wird ein Eintrag erzeugt. • Nachdem die Kapazität des Logbuchs erreicht wurde, wird durch technische Mittel sichergestellt, dass weitere Downloads nicht möglich sind. Das Logbuch kann nur durch Aufbrechen eines Siegels gelöscht und nur von den Prüfstellen neu versiegelt werden.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode des rechtlich relevanten Softwareteils, der für die Überwachung von Downloadprozessen verantwortlich ist.
Validierungsanleitung (zusätzlich zur Anleitung für die Risikoklasse D): <i>Auf Basis des Quellcodes ist zu überprüfen:</i> • ob die für die Überwachung des Downloadprozesses ergriffenen Maßnahmen angemessen sind, • ob die zum Schutz der aufgezeichneten Logbucheinträge ergriffenen Maßnahmen angemessen sind.

10 Anhang I: Gerätespezifische Softwareanforderungen

Dieser Anhang ist als Zusatz zu den allgemeinen Softwareanforderungen der vorangegangenen Kapitel gedacht und darf nicht getrennt von den Teilen P oder U und den übrigen Anhängen betrachtet werden (siehe Kapitel 2). Er spiegelt die gerätespezifischen Anhänge der MID (MI-x) wieder und enthält spezielle Aspekte und Anforderungen an Messgeräte oder Messsysteme (oder Teilgeräte). Diese Anforderungen gehen jedoch nicht über die Anforderungen der MID hinaus. Auf OIML-Empfehlungen oder ISO-/IEC-Normen wird nur dann verwiesen, wenn diese als normative Dokumente im Sinne der MID betrachtet werden können und dies zu einer harmonisierten Auslegung der MID-Anforderungen beiträgt.

Neben den gerätespezifischen Softwareaspekten und -anforderungen enthält Anhang I auch die geräte- (oder kategorie-)spezifische Einstufung in Risikoklassen, was ein harmonisiertes Niveau von Softwareprüfung, Softwareschutz und Softwarekonformität gewährleistet.

Derzeit ist Anhang I ein erster Entwurf, der von der jeweiligen WELMEC-Arbeitsgruppe mit den entsprechenden Fachkenntnissen vervollständigt werden muss. Daher hat Anhang I eine "offene Struktur", d.h. er bietet lediglich ein Gerüst, das neben der ersten Einstufung in Risikoklassen nur teilweise ausgefüllt ist (z.B. für Verbrauchszähler und selbsttätige Waagen). Er kann auch für andere MID-(oder Nicht-MID-)Geräte verwendet werden, je nach den Erfahrungen und Entscheidungen der zuständigen WELMEC-Arbeitsgruppen. Die Nummerierung x der Unterkapitel 10.x entspricht der Nummerierung des spezifischen MID-Anhangs MI-x. Nicht-MID-Geräte könnten – mit 10.11 beginnend – hinzugefügt werden.

Es gibt verschiedene gerätespezifische Softwareaspekte, die für ein bestimmtes Messgerät vom Typ x in Betracht gezogen werden können. Diese Aspekte sollten systematisch wie folgt behandelt werden: Jedes Unterkapitel 10.x sollte in Unterkapitel 10.x.y untergliedert werden, in denen y die folgenden Aspekte abdeckt.

10.x.1 Spezifische Vorschriften, Normen und andere normative Dokumente

Hier sollten geräte- (oder kategorie-)spezifische Vorschriften, Normen oder andere normative Dokumente (z.B. OIML-Empfehlungen) oder WELMEC-Richtlinien erwähnt werden, die bei der Entwicklung von geräte- oder (kategorie-)spezifischen Softwareanforderungen als Auslegung der Anforderungen der MID, Anhang I, und der spezifischen Anhänge MI-x helfen könnten.

Normalerweise gelten die spezifischen Softwareanforderungen zusätzlich zu den allgemeinen Anforderungen in den vorangegangenen Kapiteln. Sonst sollte deutlich angegeben werden, ob eine spezifische Softwareanforderung eine (oder mehrere) der allgemeinen Softwareanforderungen ersetzt oder ob und warum eine (oder mehrere) allgemeine Softwareanforderungen nicht zutreffen.

10.x.2 Technische Beschreibung

Hier können

- Beispiele für die gebräuchlichsten speziellen technischen Konfigurationen,
- die Anwendung der Teile P, U und der Anhänge zu diesen Beispielen, sowie
- nützliche (gerätespezifische) Checklisten sowohl für den Hersteller als auch für den Prüfer

aufgeführt werden. In der Beschreibung sollte erwähnt werden:

- das Messprinzip (kumulative Messung oder unabhängige Einzelmessung; wiederholbare oder nicht wiederholbare Messung; statische oder dynamische Messung) und
- die Fehlererkennung und -reaktion, wobei zwei Fälle möglich sind:
 - a) das Vorhandensein eines Defektes ist offensichtlich, kann mit einfachen Mitteln überprüft werden oder es gibt Hardwarehilfsmittel zur Fehlererkennung,
 - b) das Vorhandensein eines Defektes ist nicht offensichtlich, kann nicht mit einfachen Mitteln überprüft werden und es gibt keine Hardwarehilfsmittel zur Fehlererkennung.

Im letzteren Fall (b) erfordern Fehlererkennung und -reaktion angemessene Softwarehilfsmittel und daher angemessene Softwareanforderungen.

- die Hardwarekonfiguration; mindestens die folgenden Bereiche sollten angesprochen werden:
 - a) Handelt es sich um ein modulares, allgemein verwendbares, computergestütztes System oder um ein dediziertes Gerät mit einem eingebetteten System, das der gesetzlichen Kontrolle unterliegt?
 - b) Handelt es sich bei dem Computersystem um ein Stand-alone-System oder ist es Teil eines geschlossenen Netzwerks, z.B. Ethernet, Token-Ring-LAN oder Teil eines offenen Netzwerks, z.B. Internet?
 - c) Ist der Sensor getrennt (separates Gehäuse und separate Stromversorgung) vom Typ-U-System oder ist er teilweise oder vollständig darin integriert?
 - d) Unterliegt die Benutzerschnittstelle immer der gesetzlichen Kontrolle (sowohl für Typ-P als auch für Typ-U-Geräte) oder kann sie auf eine Betriebsart umgeschaltet werden, die nicht der gesetzlichen Kontrolle unterliegt?
 - e) Ist eine Langzeitdatenspeicherung vorgesehen? Wenn ja, ist der Speicher dann lokal (z.B. Festplatte) oder entfernt (z.B. Fileserver)?
 - f) Ist das Speichermedium fest (z.B. internes ROM) oder entfernbar (z.B. Floppy Disk, CD-RW, Smart-Media-Karte, Memory-Stick)?
- die Softwarekonfiguration und -umgebung; zumindest die folgenden Bereiche sollten angesprochen werden:
 - a) Welches Betriebssystem wird verwendet oder kann verwendet werden?
 - b) Befinden sich außer der rechtlich relevanten Software andere Softwareanwendungen in dem System?
 - c) Ist eine nicht der gesetzlichen Kontrolle unterliegende Software vorhanden, für die geplant ist, dass sie nach der Zulassung frei modifiziert werden kann?

10.x.3 Spezielle Softwareanforderungen

Hier sollen die speziellen Softwareanforderungen aufgeführt und in ähnlicher Form wie in den vorangegangenen Kapiteln kommentiert werden.

10.x.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Hier können Beispiele für

- gerätespezifische Parameter (z.B. Individualkonfiguration und Kalibrierparameter eines bestimmten Messgeräts),
- bauartspezifische Parameter (z.B. spezielle Parameter, die bei der Bauartprüfung festgelegt werden) oder
- spezielle, rechtlich relevante Funktionen aufgeführt werden.

10.x.5 Weitere Aspekte

Hier können weitere Aspekte erwähnt werden, z.B. spezielle Dokumentation, die für die (Software-)Bauartprüfung erforderlich ist, spezielle Beschreibungen und Anweisungen, die in den Bauartprüfscheinen bereitgestellt werden sollen, oder andere Aspekte (z.B. Anforderungen hinsichtlich der Prüfbarkeit).

10.x.6 Einstufung in Risikoklassen

Hier sollte die angemessene Risikoklasse für Messgeräte vom Typ x festgelegt werden. Dies kann

- entweder allgemein (für alle Kategorien innerhalb des entsprechenden Typs) oder
- abhängig vom Anwendungsbereich, der Kategorie oder gegebenenfalls anderen Aspekten erfolgen.

10.1 Wasserzähler

10.1.1 Spezifische Vorschriften, Normen und andere normative Dokumente

Die Mitgliedstaaten können – gemäß Artikel 2 der MID – festlegen, dass Wasserzähler für Privathaushalte, Gewerbe und Leichtindustrie normalerweise den Bestimmungen der MID unterliegen. Die spezifischen Anforderungen des vorliegenden Kapitels beruhen ausschließlich auf Anhang III (MI-001).

10.1.2 Technische Beschreibung

10.1.2.1 Hardwarekonfiguration

Geräte, die dazu bestimmt sind, das Volumen des zu Messbedingungen durch den Aufnehmer fließenden Wassers kontinuierlich zu messen, zu speichern und anzuzeigen. Ein Wasserzähler besteht aus mindestens einem Aufnehmer, einem Zähler (mit Justier- oder Korrekturereinrichtung, falls vorhanden) und einer Anzeigeeinrichtung. Diese drei Einrichtungen können sich in unterschiedlichen Gehäusen befinden.

Hinweis: Volumen im Sinne von kumulierten Volumenmengen über einen Zeitraum.

10.1.2.2 Softwarekonfiguration

Die Softwarekonfiguration wird vom Hersteller festgelegt, sollte sich aber normalerweise nach den Empfehlungen im Hauptteil dieses Leitfadens richten.

10.1.2.3 Messprinzip

Wasserzähler kumulieren kontinuierlich die verbrauchte Wassermenge. Die kumulierte Menge wird auf dem Messgerät angezeigt. Es werden verschiedene Prinzipien angewendet.

Die Mengenummessung kann normalerweise nicht wiederholt werden.

10.1.2.4 Fehlererkennung und -reaktion

Die Anforderung Anlage III (MI-001), 7.1.2 behandelt elektromagnetische Störungen. Es ist notwendig, diese Anforderung für softwaregesteuerte Geräte zu interpretieren, da das Entdecken einer Störung sowie das Beheben nur durch das Zusammenwirken

spezieller Hardwareteile und spezieller Software möglich ist. Aus Softwaresicht macht es keinen Unterschied, was der Grund für eine Störung war (elektromagnetisch, elektrisch, mechanisch usw.): die Wiederaufnahme des Normalbetriebs verläuft immer gleich.

Nach der Einwirkung einer elektromagnetischen Störgröße muss der Wasserzähler

- einen Betrieb innerhalb der Fehlergrenzen wieder aufnehmen und
- muss die Durchführbarkeit sämtlicher Messfunktionen gewährleistet sein, und
- eine Wiederherstellung aller unmittelbar vor dem Auftreten der Störgröße vorhandenen Messdaten ermöglichen" (siehe ISO 4064-1:2014 A3, A5 und OIML R 49:2013-1 A3, A5)

10.1.3 Spezielle Softwareanforderungen

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-1: Fehlerbehebung <i>Die Software muss nach einer Störung wieder zur normalen Verarbeitung zurückkehren.</i>		
Detaillierende Anmerkungen: Datumstempel-Flags zur Unterstützung der Protokollierung von Zeiträumen im Fehlbetrieb müssen eingerichtet werden.		
Erforderliche Dokumentation: • Kurze Beschreibung der Fehlerbehebungsmechanismen und Erklärung, wann er aktiviert wird. • Kurze Beschreibung der diesbezüglichen vom Hersteller durchgeführten Tests. • Eine kurze Beschreibung der Schritte für den Software-Wiederherstellungsmechanismus nach einem Fehler (vom Hersteller des Zählers), falls dies für die Software-Validierung erforderlich ist.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die Umsetzung der Fehlerbehebung geeignet ist. <i>Funktionsprüfungen:</i> • Bestätigen der korrekten Funktion bei Vorhandensein definierter Störgrößen und provozierte Fehler.		
Beispiel einer akzeptablen Lösung: Ein Hardware-Watchdog wird von einem zyklisch ausgeführten Mikroprozessor-Unterprogramm zurückgesetzt, um das Auslösen des Watchdogs zu verhindern. Wurde irgendeine Funktion nicht ausgeführt oder – im schlimmsten Fall – befindet sich der Mikroprozessor in einer fehlerbedingten Endlosschleife, wird der Watchdog nicht zurückgesetzt und nach einer bestimmten Zeitspanne ausgelöst.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-2: Rechtlich nicht relevante Software und dynamisches Verhalten <i>Die rechtlich nicht relevante Software darf das dynamische Verhalten eines Messprozesses nicht nachteilig beeinflussen.</i>		
Detaillierende Anmerkungen: Diese Anforderung stellt sicher, dass das dynamische Verhalten der rechtlich relevanten Software bei Echtzeitanwendungen von Zählern nicht in unzulässiger Weise durch rechtlich nicht relevante Software beeinflusst wird, d.h. dass die Ressourcen der rechtlich relevanten Software nicht in unzulässiger Weise vom rechtlich nicht relevanten Teil gemindert werden.		
Erforderliche Dokumentation: • Beschreibung der Unterbrechungshierarchie. • Zeitdiagramm der Softwareaufgaben. Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die Dokumentation der Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben dem Programmierer des rechtlich nicht relevanten Softwareteils zur Verfügung steht. <i>Funktionsprüfungen:</i> • Bestätigen der korrekten Funktion bei Vorhandensein definierter Störgrößen und provozierte Fehler.		
Beispiel einer akzeptablen Lösung: Die Unterbrechungshierarchie ist so entworfen, dass nachteilige Einflüsse vermieden werden.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-3: Zusätzliche Funktionalität² <i>Die zusätzliche Funktionalität, beispielsweise die Vorauszahlung oder Intervallmessung³, sollte die rechtlich relevanten Messfunktionen nicht beeinflussen, wie in MID Anhang III Wasserzähler (MI-001).</i>		
Detaillierende Anmerkungen: Eine zusätzliche Funktionalität ist zugelassen, beeinflussen jedoch nicht die in der MID, Anhang III Wasser rechtlich relevanten Messfunktionen, wie in der MID III Wasserzähler (MI-001).		
Erforderliche Dokumentation: Siehe S1 bis S3.		
Validierungsanleitung: Siehe S1 bis S3.		
Beispiel einer akzeptablen Lösung: Siehe S1 bis S3.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-4: Backup-Einrichtungen <i>Es kann eine Einrichtung vorhanden sein, die für ein regelmäßiges Backup von Messdaten (wie z.B. Messwerte und der aktuelle Prozessstatus) sorgt. Diese Daten müssen in einem nichtflüchtigen Speicher gehalten werden.</i>		
Detaillierende Anmerkungen: Wird die Sicherungsmöglichkeit für die Fehlerbehebung verwendet, muss der Mindestabstand für das Backup berechnet werden, um sicherzustellen, dass der kritische Wechselwert nicht überschritten wird.		
Erforderliche Dokumentation: • Eine kurze Beschreibung, welche Daten gesichert werden und wann dies geschieht. • Die Berechnung des Mindestabstands für das Backup, um sicherzustellen, dass der kritische Wechselwert nicht überschritten wird.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob Messdaten im nichtflüchtigen Speicher gesichert werden und wiederhergestellt werden können. <i>Funktionsprüfungen:</i> • Bestätigen der korrekten Funktion bei Vorhandensein definierter Störgrößen und provozierter Fehler.		
Beispiel einer akzeptablen Lösung: Für die Messdaten wird ein Backup wie gefordert ausgeführt.		

² Der Hersteller sollte immer die nationalen Anforderungen bezüglich der zusätzlichen Funktionalität berücksichtigen.

³ Bezüglich der Intervallmessung sind zusätzliche Anweisungen im WELMEC-Leitfaden 13.3 enthalten.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-5: Software-Download <i>Während der Software-Installation sollte der Messvorgang insgesamt nicht länger als eine Minute gesperrt werden.</i> <i>Falls die Software-Installation mehr als eine Minute braucht, müssen zusätzliche Maßnahmen getroffen werden (z. B. findet die Installation bei niedrigem Wasserverbrauch statt).</i>		
Detaillierende Anmerkungen: • Diese Anforderung gilt zusätzlich zu D1, D2, D3 und D4, wenn eine Softwaretrennung durchgeführt wurde. • Die zusätzliche Anforderung stellt sicher, dass für Echtzeit-Anwendungen des Zählers Messungen nicht zu lange unterbrochen werden.		
Erforderliche Dokumentation: Siehe D1, D2, D3 und D4.		
Validierungsanleitung: Siehe D1, D2, D3 und D4.		
Beispiel einer akzeptablen Lösung: Siehe D1, D2, D3 und D4.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-6: MID-Anhang I, 8.5 (Rücksetzen kumulierter Messwerte verhindern) <i>Bei Versorgungsmessgeräten darf während des Betriebes ein Rücksetzen der Anzeige der gelieferten Gesamtmenge oder der Anzeigen, aus denen die gelieferte Gesamtmenge abgeleitet werden kann, die vollständig oder teilweise eine Grundlage für die Bezahlung ist, nicht möglich sein.</i>		
Detaillierende Anmerkungen: • Kumulative Register eines Messgeräts dürfen vor der Inbetriebnahme zurückgesetzt werden. Während eines Konformitätsbewertungsverfahrens gemäß Anhang D, F oder H1, müssen die Wasserzähler mit sämtlichen Sicherungsvorrichtungen gemäß TEC ausgerüstet sein, wonach das Rücksetzen der kumulativen Messwerte ohne das Hinterlassen einer Spur nicht möglich sein darf. • Totalisatoren der kumulativen Register eines Messgeräts muss zurückgesetzt werden, bevor das relevante Konformitätsbewertungsverfahren beendet ist. Während des Konformitätsbewertungsverfahrens gemäß Anhang Annex D, F oder H1 müssen die Wasserzähler mit allen Sicherungsvorrichtungen gemäß TEC ausgerüstet sein, die den Nachweis eines Eingriffs in die Meterregister ermöglichen sollen, nachdem die kumulativen Messwerte zurückgesetzt worden sind. Kumulative Register dürfen nicht während der Verwendung im Verteilernetz zurückgesetzt werden. Hinweis: festgelegt in ISO 4064 unter 6.8.2. - Elektronische Versiegelungen		
Erforderliche Dokumentation: Dokumentation der Schutzmaßnahmen vor dem Rücksetzen der Mengenregister.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob das Rücksetzen der kumulierten, rechtlich relevanten Messwerte gesichert ist und ob die vorgesehenen Sicherungsmaßnahmen den Nachweis eines Eingriffs ermöglichen. <i>Funktionsprüfungen:</i> • Bestätigung der korrekten Funktion der vorgesehenen Sicherungsmaßnahmen, siehe also P3/U3 und P4/U4.		
Beispiel einer akzeptablen Lösung: Der Register für die gesamte gemessene Menge muss durch eine Hardware-Versiegelung geschützt sein. Andere Register, zum Beispiel Tages- oder Nachttarifregister, müssen mit denselben Mitteln geschützt werden wie Parameter (siehe P7/U7), vorausgesetzt, dass ein Gesamtzählwerk (insgesamt kumulativ) verfügbar ist, welches von einer Hardware-Versiegelung geschützt ist. Weitere Einzelheiten sind im WELMEC-Leitfaden 11.1/13 und in der ISO 4064 Abschnitt 6.8.2. – elektronische Versiegelung enthalten.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-7: MID Anhang I, Artikel 10.5 Ablesen der Messergebnisse <i>Die Messergebnisse, die als Grundlage für den zu zahlenden Preis dienen, können Werte verschiedener Register sein, die durch eine Fernbedienung, Uhr oder andere Vorrichtungen aktiviert werden. Jeder Register steht für die Gesamtmenge, die mit einem Tarif im Fakturierungsprozess verbunden ist. Die Ergebnisse müssen mit Hilfe der Benutzerschnittstelle auf verschiedenen Anzeigen periodisch oder auf Anfrage angezeigt werden können.</i>		
Detaillierende Anmerkungen: - Kumulative Register oder totalisierte Register der Wasserzähler können vor dem anwendbaren Konformitätsbewertungsverfahren zurückgesetzt werden. Während eines Konformitätsbewertungsverfahrens gemäß Anhang D, F oder H1 müssen die Verbrauchszähler mit sämtlichen Sicherungsvorrichtungen gemäß TEC vom Hersteller ausgestattet sein, wonach die kumulativen Messwerte nicht ohne das Hinterlassen einer Spur zurückgesetzt werden können, siehe I1-6. - Wenn der größte Anzeigebereich der Volumentotalisierung erreicht ist, misst der Anzeigebereich weiter beginnend bei null Kubikmeter, siehe auch I1-9 (Anzahl der Dezimalstellenzahlen).		
Erforderliche Dokumentation: Dokumentation der Erzielung der Messergebnisse, was als Grundlage für den zu zahlenden Preis dient.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - ob die Messergebnisse korrekt bearbeitet wurden. <i>Funktionsprüfungen:</i> - Bestätigen der korrekten Bearbeitung der Messergebnisse.		
Beispiel einer akzeptablen Lösung: Wenn ein Zähler für die Zählung der Mengen in verschiedenen Registern gemäß MID (MI-001) ausgelegt ist, muss ein Zähler die Gesamtmengen jedes Registers auf der Anzeige mit Hilfe der Benutzerschnittstelle (siehe P3/U3, z.B.: Tasten auf Geräten) sowie die derzeit aktiven Tarifregister darstellen können. Die Ergebnisse dürfen mit Hilfe der Benutzerschnittstelle periodisch oder auf Anfrage auf verschiedenen Anzeigen dargestellt werden. Bei der Anzeige verschiedener Messergebnisse muss jedoch klar sein, welche Anzeige zu welchem Register gehört; es darf diesbezüglich keine Unklarheiten geben. Falls notwendig, können zusätzliche Beschriftungen auf dem Wasserzähler angebracht werden, wobei die verschiedenen Register oder die Anzeige des Testmodus zu klären sind (siehe I1-9).		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-8: Schutz vor vorsätzlichen Änderungen bei Wasserzähler vom Typ P (mit mechanischem Register) <i>Die berechnete Prüfsumme oder eine Alternativanzeige der Softwareänderung ist auf Befehl für Kontrollzwecke sichtbar zu machen, siehe P6. Für Wasserzähler wäre als Ausnahme ein Aufprägen des Software-Identifikators auf das Typenschild eines Messgeräts eine akzeptable Lösung, wenn die folgenden Bedingungen A, B und C erfüllt sind:</i> <i>A Die Benutzerschnittstelle hat keinerlei Steuerungsfähigkeiten, um die Anzeige des Software-Identifikators auf dem Display zu aktivieren, oder das Display gestattet die Anzeige des Software-Identifikators aus technischen Gründen nicht (mechanischer Zähler).</i> <i>B. Das Messgerät hat keine Schnittstelle, um den Software-Identifikator zu übermitteln.</i> <i>C. Nach der Fertigung eines Zählers ist eine Änderung der Software nicht mehr möglich oder nur dann möglich, wenn auch die Hardware oder ein Hardwareteil, der die Software enthält, geändert wird.</i>		
Detaillierende Anmerkungen: - Der Hersteller der Hardware bzw. des entsprechenden Hardwareteils ist dafür verantwortlich, dass die Prüfsumme oder eine alternative Anzeige der Softwareänderungen ordnungsgemäß auf der betroffenen Hardware angegeben ist. - Es gelten alle anderen Detaillierenden Anmerkungen von P6.		
Erforderliche Dokumentation: Gemäß P6.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - Gemäß P6. <i>Funktionsprüfungen:</i> - Gemäß P6.		
Beispiel einer akzeptablen Lösung: Aufprägen der Prüfsumme oder einer alternativen Anzeige der Softwareänderung auf das Typenschild des Messgeräts		

Risikoklasse B	Risikoklasse C	Risikoklasse D
----------------	----------------	----------------

I1-9: Anzahl der Dezimalstellen

Die Anzeige der Gesamtmenge muss ausreichend Dezimalstellen haben. Gemäß ISO 4064, Teil 1, basieren die Dezimalstellen auf dem permanenten Durchfluss Q3:

Dauerdurchfluss Q3 [m³/h]	Mindestanzeigebereich [m³]
$Q3 \leq 6,3$	9 999
$6,3 < Q3 \leq 63$	99 999
$63 < Q3 \leq 630$	999 999
$630 < Q3 \leq 6300$	9 999 999

Gemäß ISO 4064 Teil 1 muss die Auflösung der Anzeigevorrichtung die folgende Anforderung erfüllen:

- Die Unterteilungen der Eichskala sollten ausreichend klein sein, um sicherzustellen, dass der Auflösungsfehler der Anzeigeeinrichtung 0,25 % (für Zähler der Genauigkeitsklasse 1) bzw. 0,5 % (für Zähler der Genauigkeitsklasse 2) des tatsächlichen Volumens, das bei Mindestdurchflussrate Q1 innerhalb von 90 Minuten durch den Zähler fließt, nicht überschreitet.
- Zusätzliche Eichhilfsmittel dürfen verwendet werden, sofern die Ablesunsicherheit 0,25 % (für Zähler der Genauigkeitsklasse 1) bzw. 0,5 % (für Zähler der Genauigkeitsklasse 2) der Prüfmenge nicht überschreitet und sofern die ordnungsgemäße Funktion des Registers überprüft wird.

Eignung gemäß Absatz 7.6 und 10.5 von Anhang I der Richtlinie 2014/32/EU (MID):

Ein Messgerät ist so auszulegen, dass die Messvorgänge kontrolliert werden können, nachdem das Messgerät auf den Markt gebracht und in Betrieb genommen wurde. Falls erforderlich muss das Messgerät eine spezielle Ausrüstung oder Software für diese Kontrolle besitzen.

Darüber hinaus muss ein Messgerät, das fernabgelesen werden kann, auf jeden Fall mit einer der messtechnischen Kontrolle unterliegenden Sichtanzeige ausgestattet werden, die für den Verbraucher ohne Hilfsmittel zugänglich ist.

Wenn der maximale Anzeigebereich der Mengentotalisierung erreicht ist, misst der Anzeigebereich weiter beginnend bei null Kubikmeter.

Detaillierende Anmerkungen:

Gemäß ISO 4064 Teil 1:

- Die Anzeigevorrichtung eines Wasserzählers sollte eine leicht ablesbare, zuverlässige und eindeutige visuelle Anzeige des angezeigten Volumens liefern. Ein kombinierter Zähler kann über zwei Anzeigeeinrichtungen verfügen, deren Summe dann das angezeigte Volumen bilden.
- Jede Anzeigevorrichtung muss mit Mitteln zur visuellen, eindeutigen Eichprüfung und Kalibrierung ausgestattet sein.
- Die visuelle Prüfanzeige darf entweder eine kontinuierliche oder eine nicht kontinuierliche Bewegung aufweisen.

Erforderliche Dokumentation:

- Eine Beschreibung der Anzeige und des Anzeige-Menüs.
- Eine Beschreibung der visuellen Prüfanzeige und eine Erklärung, wie die visuelle Prüfanzeige ausgelöst wird.

Validierungsanleitung:

Funktionsprüfungen:

- ob die Stellenanzahl auf dem Display für die der Gesamtmenge ausreicht
- Auslösung der visuellen Eichanzeige und Prüfung, ob die visuelle Prüfanzeige die Anforderungen erfüllt
 - ob eine spezielle Ausrüstung oder Software für diese Kontrolle (gegebenenfalls) Teil des Messgerätes ist.

Beispiel einer akzeptablen Lösung:

Auf der Anzeige des Wasserzählers gibt es genügend Dezimalstellen, die beide Anforderungen der Gesamtmenge mit der erforderlichen Auflösung erfüllen.

Umschalten von Anzeigemodi auf der Anzeigevorrichtung, um die Werte für die Gesamtmenge mit der korrekten Auflösung sowie den "Prüfmodus" mit den zusätzlichen Prüfelementen aufzuzeigen. Diese Anzeigemodi müssen mit Hilfe folgender Elemente angezeigt werden können:

- der Benutzerschnittstelle (siehe P3/U3, z. B.: Tasten auf Geräten) oder
- beim Durchlaufen der verschiedenen Anzeigemodi.

Es sollte jedoch klar sein, um welche Primäranzeige es sich handelt, wenn verschiedene Anzeigemodi verwendet werden. Es muss klar sein, wie diese Werte abgelesen werden müssen, und es darf keine Uneindeutigkeit bezüglich anderer Anzeigemodi geben. (siehe I1-7).

Anmerkung: Es steht nicht im Einklang mit den wesentlichen Anforderungen der Richtlinie 2014/32/EU (MID) gemäß Artikel 7.6, Anhang I, dass eine Eichbehörde, Prüfbehörde oder benannte Stelle beim Hersteller nach speziellen Prüfeinrichtungen oder Software nachfragen muss.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-10: Anzeigetest (Display-Test) <i>Zur Verifizierung der korrekten Funktion aller Segmente der Anzeige, muss ein Anzeigetest durchgeführt werden können.</i>		
Detaillierende Anmerkungen: Der Anzeigetest findet gemäß ISO 4064 statt: • Der Zähler soll eine Sichtprüfung der gesamten Anzeigeeinrichtung mit folgendem Verlauf erlauben: 1) bei sieben Segmenttypen: Anzeige aller Elemente (z. B. ein sogenannter "8er-Test"); 2) bei sieben Segmenttypen: Abschalten aller Elemente ("Abschalt"-Test). 3) bei grafischen Anzeigen: äquivalenter Test, der aufzeigt, dass Anzeigefehler nicht dazu führen können, dass irgendeine Ziffer fehlinterpretiert wird. • Jeder Schritt dieses Verfahrens muss mindestens 1 Sekunde dauern.		
Erforderliche Dokumentation: Eine Beschreibung des Anzeigetests und eine Erklärung, wie ein solcher Test gestartet wird.		
Validierungsanleitung: Starten des Anzeigetests und Prüfen, ob eine visuelle Prüfung der gesamten Anzeige möglich ist.		
Beispiel einer akzeptablen Lösung: Ein Anzeigetest wird auf Sonderbefehl durch die Benutzerschnittstelle gestartet (siehe P3/U3, z.B.: Tasten auf Geräten) oder ist Teil des Durchlaufverfahrens, welches die verschiedenen Anzeigemodi zeigt.		

10.1.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Der Zugang zu Mitteln für die Änderung der Software, Einstellungen und/oder Parameter, die die Bestimmung der Messergebnisse beeinflussen, muss gesichert werden⁴.

Parameter	Geschützt	Einstellbar	Anmerkung
Kalibrierfaktor	x		
Linearisierungsfaktor	x		
Rechtlich relevante Konfiguration der Register	x		
Zum Beispiel Einstellungen: • Korrekturgeräte • Kurvenanpassung	x		
Sonstige relevanten Parameter, die das Messergebnis beeinflussen könnten	x		
Software-Download des rechtlich relevanten Softwareteils	x		

10.1.5 Einstufung in Risikoklassen

Die folgende Risikoklasse wird als angemessen befunden und sollte angewendet werden, wenn auf diesem Leitfaden beruhende Softwareprüfungen für (softwaregesteuerte) Elektrizitätszähler für Wirkverbrauch durchgeführt werden:

- Risikoklasse C für Messgeräte vom Typ P

⁴. Bezüglich der Sicherung eines Wasserzählers wird im WELMEC Leitfaden 13.3 zusätzliche Anleitungen gegeben.

10.2 Gaszähler und Mengenumwerter

10.2.1 Spezifische Vorschriften, Normen, normative Dokumente und andere WELMEC-Leitfäden

Die spezifischen Anforderungen des vorliegenden Kapitels beruhen auf der MID, Anhang IV Gaszähler und Mengenumwerter (MI-002).

Eine Anleitung zur Sicherung von Gaszählern und Mengenumwertern sind auch im WELMEC-Leitfaden 11.3 enthalten.

Eine spezielle Anleitung bezüglich der Gaschromatographen, die als Live-Sensor an ein EVCD angeschlossen sind, sind in WELMEC-Leitfaden 11.1 enthalten.

Eine zusätzliche Anleitung oder Updates für Gaszähler und Mengenumwerter sind der WELMEC-Webseite zu entnehmen.

Die nationale Gesetzgebung bezüglich zusätzlicher Funktionalität, OIML-Empfehlungen, harmonisierte (EN) Normen und (IEC) Normen wurden nicht berücksichtigt.

10.2.2 Technische Beschreibung

Hardwarekonfiguration

Gaszähler und Mengenkonverter sind normalerweise getrennte Hardwareeinheiten.

Anzeigen oder Recheneinheiten von Gaszählern und Mengenumwertern können eine oder mehrere Schnittstellen haben, um externe Sensoreinheiten zu verbinden.

Falls ein Gaschromatograph als Live-Sensor mit einem EVCD verbunden ist, beeinflusst der Gaschromatograph das Messergebnis (Basisvolumen) des EVCD und sollte daher Teil des Konformitätsbewertungsverfahrens sein.

10.2.2.2 Softwarekonfiguration

Die Softwarekonfiguration hängt vom Zählertyp ab, sollte sich aber normalerweise nach den Empfehlungen im Hauptteil dieses Leitfadens richten.

10.2.2.3 Messprinzip

Gaszähler kumulieren kontinuierlich die verbrauchte Menge oder die Masse, die durch den Zähler fließt. Ein Mengenumwerter kann verwendet werden, um die Menge im Grundzustand zu berechnen.

Die Mengenummessung ist nicht wiederholbar.

10.2.2.4 Fehlererkennung und -reaktion

Die Anforderung in der MID, Anhang IV Gaszähler und Mengenumwerter (MI-002), Abschnitt 3.1 beschäftigt sich mit der zulässigen Auswirkung von Störungen. Aus Softwaresicht macht es keinen Unterschied, was der Grund für eine Störung war (elektromagnetisch, elektrisch, mechanisch usw.): die Wiederaufnahme des Normalbetriebs verläuft immer gleich.

- Nach der Einwirkung einer Störgröße muss der Gaszähler:
 - einen Betrieb innerhalb der Fehlergrenzen wieder aufnehmen und
 - muss die Durchführbarkeit sämtlicher Messfunktionen gewährleistet sein, und
 - eine Wiederherstellung aller unmittelbar vor dem Auftreten der Störgröße vorhandenen Messdaten ermöglichen.

- Siehe 3.1.2 der MID, Anhang IV Gaszähler und Mengenumwerter (MI-002)
- Ein elektronischer Mengenumwerter muss feststellen können, wenn er bei Parametern, die für die Messgenauigkeit relevant sind, außerhalb des vom Hersteller angegebenen Betriebsbereiches arbeitet. In diesem Fall muss der Mengenumwerter das Integrieren der umgewandelten Menge beenden, und die umgewandelte Menge kann während des Betriebs außerhalb des bzw. der Betriebsbereiche gesondert summiert werden.
- Siehe 9.1 der MID, Anhang IV Gaszähler und Mengenumwerter (MI-002).

10.2.3 Spezielle Softwareanforderungen

Gaszähler und Mengenumwerter

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-1: MID, Anhang IV Gaszähler und Mengenumwerter (MI-002) 3.1, Fehlerbehebung <i>Die Software muss nach einer Störung wieder zur normalen Verarbeitung zurückkehren.</i>		
Detaillierende Anmerkungen: Datumstempel-Flags zur Unterstützung der Protokollierung von Zeiträumen im Fehlbetrieb müssen eingerichtet werden.		
Erforderliche Dokumentation: Kurze Beschreibung der Fehlerbehebungsmechanismus und Erklärung, wann er aktiviert wird.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die Umsetzung der Fehlerbehebung geeignet ist. <i>Funktionsprüfungen:</i> • Funktionsprüfungen bei Vorhandensein definierter Störgrößen und provozierten Fehler.		
Beispiel einer akzeptablen Lösung: Der Hardware-Watchdog wird von einem zyklisch ausgeführten Mikroprozessor-Unterprogramm zurückgesetzt, um das Auslösen des Watchdogs zu verhindern.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-2: Rechtlich nicht relevante Software und dynamisches Verhalten <i>Die rechtlich nicht relevante Software darf das dynamische Verhalten eines Messprozesses nicht nachteilig beeinflussen.</i>		
Detaillierende Anmerkungen: Diese Anforderung stellt sicher, dass das dynamische Verhalten der rechtlich relevanten Software bei Echtzeitanwendungen von Zählern nicht in unzulässiger Weise durch rechtlich nicht relevante Software beeinflusst wird, d.h. dass die Ressourcen der rechtlich relevanten Software nicht in unzulässiger Weise vom rechtlich nicht relevanten Teil gemindert werden.		
Erforderliche Dokumentation: - Beschreibung der Unterbrechungshierarchie. - Zeitdiagramm der Softwareaufgaben. Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - ob die Dokumentation der Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben dem Programmierer des rechtlich nicht relevanten Softwareteils zur Verfügung steht. <i>Funktionsprüfungen:</i> - Bestätigen der korrekten Funktion bei Vorhandensein definierter Störgrößen und provozierte Fehler.		
Beispiel für eine akzeptable Lösung: Die Unterbrechungshierarchie ist so entworfen, dass nachteilige Einflüsse vermieden werden.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-3: MID, Anlage IV Gaszähler und Mengenumwerter (MI-002), 3.1.2 Backup-Einrichtungen <i>Es kann eine Einrichtung vorhanden sein, die für ein regelmäßiges Backup von Messdaten (wie z.B. Messwerte und der aktuelle Prozessstatus) sorgt. Diese Daten müssen in einem nichtflüchtigen Speicher gehalten werden.</i>		
Detaillierende Anmerkungen: Wird die Sicherungsmöglichkeit für die Fehlerbehebung verwendet, muss der Mindestabstand für das Backup berechnet werden, um sicherzustellen, dass der kritische Wechselwert nicht überschritten wird.		
Erforderliche Dokumentation: Eine kurze Beschreibung, welche Daten gesichert werden und wann dies geschieht. Berechnung des Mindestabstands, um sicherzustellen, dass der kritische Wechselwert nicht überschritten wird.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - ob Messdaten im nichtflüchtigen Speicher gesichert werden und wiederhergestellt werden können. <i>Funktionsprüfungen:</i> - Funktionsprüfungen bei Vorhandensein definierter Störgrößen und provozierte Fehler.		
Beispiel einer akzeptablen Lösung: Für die Messdaten wird ein Backup wie gefordert ausgeführt.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-4: Zusätzliche Funktionalität⁵ <i>Die zusätzliche Funktionalität, beispielsweise die Vorauszahlung oder Intervallmessung⁶, sollte die rechtlich relevanten Messfunktionen nicht beeinflussen, wie in MID Anhang IV Gaszähler und Mengenumwerter (MI-002).</i>		
Detaillierende Anmerkungen: • Eine zusätzliche Funktionalität ist zugelassen, wenn sie die rechtlich relevanten Messfunktionen nicht beeinflussen wie in der MID, Anhang IV Gaszähler und Mengenumwerter (MI-002) angegeben.		
Erforderliche Dokumentation: Siehe S1 bis S3.		
Validierungsanleitung: Siehe S1 bis S3.		
Beispiel für eine akzeptable Lösung: Siehe S1 bis S3.		

⁵ Der Hersteller sollte immer die nationalen Anforderungen bezüglich der zusätzlichen Funktionalität berücksichtigen.

⁶ Bezüglich der Intervallmessung sind zusätzliche Anweisungen im WELMEC-Leitfaden 11.2 enthalten.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-5: Software-Download <i>Während der Software-Installation sollte der Messvorgang insgesamt nicht länger als eine Minute gesperrt werden.</i> <i>Falls die Software-Installation mehr als eine Minute braucht, müssen zusätzliche Maßnahmen getroffen werden (z. B. findet die Installation bei niedrigem Wasserverbrauch statt).</i>		
Detaillierende Anmerkungen: • Diese Anforderung gilt zusätzlich zu D1, D2, D3 und D4, wenn ein Software-Download durchgeführt wurde. • Die zusätzliche Anforderung stellt sicher, dass für Echtzeit-Anwendungen des Zählers Messungen nicht zu lange unterbrochen werden.		
Erforderliche Dokumentation: Siehe D1.		
Validierungsanleitung: Siehe D1.		
Beispiel für eine akzeptable Lösung: Siehe D1.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-6: MID-Anhang I, 8.5 (Rücksetzen kumulierter Messwerte verhindern) <i>Bei Versorgungsmessgeräten darf während des Betriebes ein Rücksetzen der Anzeige der gelieferten Gesamtmenge oder der Anzeigen, aus denen die gelieferte Gesamtmenge abgeleitet werden kann, die vollständig oder teilweise eine Grundlage für die Bezahlung ist, nicht möglich sein.</i>		
Detaillierende Anmerkungen: Während eines Konformitätsbewertungsverfahrens gemäß Anhang D, F oder H1 müssen die Verbrauchszähler mit sämtlichen Sicherungsvorrichtungen gemäß TEC vom Hersteller ausgestattet sein, wonach die kumulativer Messwerte nicht ohne das Hinterlassen einer Spur zurückgesetzt werden können, siehe I1-6. Bei Gasmetern muss der Register für die gesamte gemessene Menge durch eine metrologische Hardware-Versiegelung geschützt sein. Bei Mengenumwertern muss die Menge im Normzustand durch eine metrologische Hardware-Versiegelung geschützt sein.		
Erforderliche Dokumentation: Dokumentation der Schutzmaßnahmen vor dem Rücksetzen der Mengenregister.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob das Rücksetzen der kumulierten, rechtlich relevanten Messwerte gesichert ist und ob die vorgesehenen Sicherungsmittel den Nachweis eines Eingriffs ermöglichen. <i>Funktionsprüfungen:</i> • Bestätigung der korrekten Funktion der vorgesehenen Sicherungsmaßnahmen.		
Beispiel einer akzeptablen Lösung: Bei Gasmetern muss der Register für die gemessene Gesamtmenge durch metrologische Hardware-Versiegelungen geschützt sein. Andere Register, zum Beispiel Tages- oder Nachttarifregister, müssen mit denselben Mitteln geschützt werden wie Parameter (siehe P7/U7), vorausgesetzt, dass ein Gesamtregister (insgesamt kumulativ) verfügbar ist, welches von einer Hardware-Versiegelung geschützt wird. Zusätzliche Anweisungen sind im WELMEC-Leitfaden 11.1 und 11.3 enthalten. Bei Mengenumwertern muss die Menge im Normzustand durch metrologische Hardware-Versiegelungen geschützt sein. Die Register, die die Menge bei Messbedingungen zeigen, können auch mit denselben Mitteln wie Parameter geschützt werden (siehe P7/U7). Hinweis: Die Menge bei Messbedingungen kann mit der Anzeige des angeschlossenen Gasmeters synchronisiert werden. Je nach nationaler Gesetzgebung müssen zusätzliche Maßnahmen ergriffen werden, z. B. Nacheichnungen.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-7: MID Anhang I, 10.5 (Ablesen der Messergebnisse) <i>A. Die Messergebnisse, die als Grundlage für den zu zahlenden Preis dienen, können Werte verschiedener Register sein, die durch eine Fernbedienung, Uhr oder andere Vorrichtungen aktiviert werden. Jedes Register steht für die Gesamtmenge, die mit einem Tarif im Abrechnungsprozess verbunden ist. Der Zähler sollte die Werte jedes Registers mit Hilfe der Benutzerschnittstelle periodisch oder auf Anfrage darstellen.</i>		
Detaillierende Anmerkungen: Kumulative Register eines Messgeräts können vor dem anwendbaren Konformitätsbewertungsverfahren zurückgesetzt werden. Während eines Konformitätsbewertungsverfahrens gemäß Anhang D, F oder H1 müssen die Verbrauchszähler mit sämtlichen Sicherungsvorrichtungen gemäß TEC vom Hersteller ausgestattet sein, wonach die kumulativen Messwerte nicht ohne das Hinterlassen einer Spur zurückgesetzt werden können.		
Erforderliche Dokumentation: Dokumentation der Erzielung der Messergebnisse, was als Grundlage für den zu zahlenden Preis dient.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die Messergebnisse korrekt bearbeitet wurden. <i>Funktionsprüfungen:</i> • Bestätigen der korrekten Funktion der Bearbeitung der Messergebnisse.		
Beispiel einer akzeptablen Lösung: <i>Wenn ein Zähler für die Zählung der Mengen in verschiedenen Registern gemäß MID, Anhang IV Gaszähler und Mengenumwerter (MI-002) ausgelegt ist, muss der Zähler die Gesamtmengen jedes Registers auf der Anzeige mit Hilfe der Benutzerschnittstelle (siehe dieser Leitfaden, z.B.: Tasten auf dem Geräte) sowie die derzeit aktiven Tarifregister darstellen können. Eine akzeptable Lösung ist ebenfalls, die Ergebnisse mit Hilfe der Benutzerschnittstelle periodisch oder auf Anfrage auf verschiedenen Anzeigen dargestellt werden. Bei der Anzeige verschiedener Messergebnisse muss jedoch klar sein, welche Anzeige zu welchem Register gehört; es darf diesbezüglich keine Unklarheiten geben.</i>		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-8: Schutz vor vorsätzlichen Änderungen bei Gaszählern vom Typ P mit einem mechanischen Register <i>Die berechnete Prüfsumme oder eine Alternativanzeige, um den Nachweis der Softwareänderung ist auf Befehl für Kontrollzwecke sichtbar zu machen, siehe P6, Risikoklasse C.</i> <i>Für Gaszähler und Mengenumwerter vom Typ P mit einem mechanischem Zähler wäre als Ausnahme ein Aufprägen der Prüfsumme oder einer Alternativanzeige für eine Softwareänderung auf das Typenschild eines Messgeräts eine akzeptable Lösung, wenn die folgenden Bedingungen A, B und C erfüllt sind:</i> <i>A Die Benutzerschnittstelle hat keinerlei Steuerungsfähigkeiten, um den Wert der Prüfsumme oder eine alternative Anzeige der Softwareänderung auf dem Display zu aktivieren, oder das Display gestattet die Anzeige dieser Werte aus technischen Gründen nicht (mechanischer Zähler).</i> <i>B. Das Messgerät hat keine Schnittstelle, um den Software-Identifikator zu übermitteln.</i> <i>C. Nach der Fertigung eines Zählers ist eine Änderung der Software nicht mehr möglich oder nur dann möglich, wenn auch die Hardware oder ein Hardwareteil, der die Software enthält, geändert wird.</i>		
Detaillierende Anmerkungen: - Der Hersteller ist dafür verantwortlich, dass die Prüfsumme oder eine Alternativanzeige der Softwareänderungen ordnungsgemäß auf der betroffenen Hardware angegeben ist. - Es gelten alle anderen Detaillierenden Anmerkungen von P6.		
Erforderliche Dokumentation: Gemäß P6.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - Gemäß P6. <i>Funktionsprüfungen:</i> - Gemäß P6.		
Beispiel für eine akzeptable Lösung: Aufprägen der Prüfsumme oder einer alternativen Anzeige der Softwareänderung auf das Typenschild des Messgeräts		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-9: MID, Anhang IV Gaszähler und Mengenumwerter (MI-002), 5.3 Anzahl der Dezimalstellen (Gaszähler und elektronische Mengenumwerter) <i>Die Anzeige der gesamten Menge muss über eine ausreichende Stellenanzahl verfügen, um sicherzustellen, dass sie bei 8000 Stunden Zählerbetrieb bei $Q_{\max}$ nicht auf ihren Ursprungswert zurückkehrt.</i>		
Detaillierende Anmerkungen: 		
Erforderliche Dokumentation: Dokumentation der internen Darstellung des Registers.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob es eine ausreichende Anzahl von Ziffern gibt, damit der Index nicht auf seinen anfänglichen Wert übergeht, wenn das Volumen, das bei $Q_{\max}$ innerhalb von 8000h fließt, durchgeflossen ist.		
Beispiel einer akzeptablen Lösung: Typische Werte für Hausgaszähler sind: $Q_{\max} = 6 \text{ m}^3/\text{h}$. Der erforderliche Bereich beträgt 48.000 m^3 und benötigt 5 Dezimalstellen, um dargestellt zu werden (derzeit zeigen mechanische und elektronische Gaszähler bis zu 99.999 m^3 an, was mehr als genug ist für diese Gerätgröße).		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-10: MID, Anhang IV Gaszähler und Mengenumwerter (MI-002), 5.2 Lebensdauer der Energiequelle <i>Eine dedizierte Energiequelle muss eine Lebensdauer von mindestens fünf Jahren haben. Nach Ablauf von 90% ihrer Lebensdauer muss eine geeignete Warnung angezeigt werden.</i>		
Detaillierende Anmerkungen: Lebensdauer wird hier im Sinne von verfügbarer Energiekapazität verwendet. Wenn die Energiequelle vor Ort ausgetauscht werden kann, dürfen die Parameter und Messdaten während des Wechsels nicht beschädigt werden. Zusätzliche Warnungen sind erlaubt, bevor die Schwelle von 90% erreicht ist, vorausgesetzt, dass diese Warnungen nicht verwirrend sind.		
Erforderliche Dokumentation: Dokumentation der Kapazität der Energiequelle, der Höchstlebensdauer (unabhängig vom Energieverbrauch), von Messungen zur Bestimmung der verbrauchten oder verfügbaren Energie, Beschreibung der Maßnahmen zur Warnung bei wenig verfügbarer Energie und beim Austauschvorgang der Batterie.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen,</i> ob die ergriffenen Maßnahmen zur Überwachung der verfügbaren Energie geeignet sind.		
Beispiel für eine akzeptable Lösung: Die Betriebsstunden oder die Weckereignisse des Geräts werden gezählt, in einem nichtflüchtigen Speicher gespeichert und mit dem Nennwert der Batterielebensdauer verglichen. Sind 90% der Lebensdauer aufgebraucht, wird eine geeignete Warnung angezeigt. Die Software erkennt den Austausch der Energiequelle und setzt den Zähler zurück. Eine weitere Lösung wäre die ständige Überwachung des Zustands der Energieversorgung. Eine Warnung wurde für angemessen gehalten im Falle einer sichtbaren Warnung, z.B. eine Botschaft auf der Anzeige oder eine Warnanzeige. Zusätzlich kann eine elektronische Schnittstelle die Warnung an den Netz-/Gerätebetreiber Eine versteckte "stille" Warnung (über die elektronische Schnittstelle) allein an den Netz-/Gerätebetreiber ist keine ausreichende Lösung.		

10.2.3.2 Gaszähler

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-11: MID, Anhang IV Gaszähler und Mengenumwerter (MI-002), 5.5. Prüfelement des Gaszählers <i>Der Gaszähler muss über ein Prüfelement verfügen, das das Ausführen von Prüfungen innerhalb eines vernünftigen Zeitraums gestattet.</i>		
Detaillierende Anmerkungen: Das Prüfelement zur Beschleunigung zeitaufwendiger Prüfverfahren wird normalerweise für die Prüfung vor Installation und Normalbetrieb verwendet. Während des Testbetriebs müssen dieselben Register und Softwareteile verwendet werden wie während des Standardbetriebsmodus.		
Erforderliche Dokumentation: Dokumentation des Prüfelements und der Anweisungen für die Aktivierung des Prüfmodus.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen,</i> ob alle zeitaufwendigen Prüfverfahren des Gaszählers mit Hilfe des Prüfelements ausgeführt werden können.		
Beispiel für eine akzeptable Lösung: Für Testzwecke muss die Erhöhung des Testelements oder des Impulses mindestens alles 60 Sekunden bei Q_{min} , siehe WELMEC-Leitfaden 11.1, Paragraph 2.4.4. erfolgen. Die Zeitbasis der internen Uhr kann beschleunigt werden. Prozesse, die z. B. eine Woche, einen Monat oder sogar ein Jahr dauern, und Registerüberlauf können im Prüfmodus innerhalb einer Zeitspanne von Minuten oder Stunden geprüft werden.		

10.2.3.3 Elektronischer Mengenumwerter

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-12: MID, Anhang IV Gaszähler und Mengenumwerter (MI-002), 9.1 (Elektronischer Mengenumwerter) <i>Ein elektronischer Mengenumwerter muss feststellen können, wenn er bei Parametern, die für die Messgenauigkeit relevant sind, außerhalb des vom Hersteller angegebenen spezifischen Messfeldes arbeitet. In diesem Fall muss der Mengenumwerter das Integrieren der umgerechneten Menge unterbrechen, und die umgerechnete Menge kann für die Zeit des Betriebs außerhalb des bzw. der Betriebsbereiche gesondert summiert werden.</i>		
Detaillierende Anmerkungen: Der Fehlerzustand muss angezeigt werden.		
Erforderliche Dokumentation: Dokumentation der verschiedenen Register für umgewandelte Menge und Ausfallmenge.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen,</i> • ob die ergriffenen Maßnahmen für den Umgang mit ungewöhnlichen Betriebszuständen geeignet sind.		
Beispiel für eine akzeptable Lösung: Die Software überwacht die relevanten Eingabewerte und vergleicht sie mit vordefinierten Grenzwerten. Wenn alle Werte innerhalb der Grenzen liegen, wird die umgewandelte Menge in das normale Register (eine dedizierte Variable) eingefügt. Ansonsten summiert die Software die Menge in einer anderen Variablen. Eine weitere Lösung wäre es, nur ein kumulierendes Register zu haben, jedoch das Anfangs- und Enddatum, die Zeit- und Registerwerte des Zeitraumes außerhalb des zulässigen Bereichs in einen Logbuch zu speichern (siehe P7). Beide Größen können angezeigt werden. Der Nutzer kann mittels einer Zustandsanzeige eindeutig zwischen der regulären und der Ausfallanzeige unterscheiden.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-13: Neuberechnung des Umrechnungsfaktors <i>Bei elektronischen Gasmengenumwertern muss der Umrechnungsfaktor bei Intervallen von nicht über einer 1 min für einen Temperaturmengenumwerter und bei Intervallen von nicht über 30 s für andere Gasmengenumwerter umgerechnet werden.</i> <i>Wenn der Gaszähler kein Signal empfangen hat:</i> - über 1 min für einen Temperaturmengenumwerter; oder - über 30 s bei anderen Typen; <i>Neuberechnung ist nicht erforderlich, bis das nächste Mengensignal empfangen wird.</i>		
Detaillierende Anmerkungen:		
Erforderliche Dokumentation: Dokumentation der Neuberechnungssequenz.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen, ob die getroffenen Maßnahmen angemessen sind.</i>		
Beispiel für eine akzeptable Lösung:		

10.2.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Der Zugang zu Mitteln für die Änderung der rechtlich relevanten Software, Einstellungen und/oder Parameter, die die Bestimmung der Ergebnisse für die Messungen beeinflussen, muss gesichert werden⁷.

Zum Beispiel aber nicht ausschließlich bei Gaszählern:

Parameter	Geschützt	Einstellbar	Anmerkung
Kalibrierfaktor	X		
Linearisierungsfaktor	X		
Rechtlich relevante Konfiguration der Register	X		
Zum Beispiel Einstellungen: • Korrekturgeräte • Kurvenanpassung • Pulszahl • Minstdurchfluss abgeschaltet • Einstellung des Ultraschall-Sensors • Geometrie der Umformer in Ultraschall-Gaszählern	X		
Sonstige relevanten Parameter, die das Messergebnis beeinflussen könnten	X		
Software-Download des rechtlich relevanten Softwareteils	X		

Zum Beispiel aber nicht ausschließlich bei Mengenumwertern

Parameter	Geschützt	Einstellbar	Anmerkung
Kalibrierfaktor	X		
Linearisierungsfaktor	X		
Rechtlich relevante Konfiguration der Register	X		
Zum Beispiel Einstellungen: • Rechtlich relevante Korrektoreinrichtung, wie Parameter, die auf der Fehlerkurve eines Gaszählers beruhen • Pulswert eines Gaszählers • Gaszusammensetzung und Parameter für die Kompressibilitätsberechnung	X		

⁷ Der Hersteller sollte immer die nationalen Anforderungen hinsichtlich der zusätzlichen Funktionalität berücksichtigen. Bezüglich der Intervallmessung sind zusätzliche Anweisungen im WELMEC-Leitfaden 11.2 enthalten.

<i>Sonstige relevanten Parameter, die das Messergebnis beeinflussen könnten</i>	<i>x</i>		
<i>Software-Download des rechtlich relevanten Softwareteils</i>	<i>x</i>		

10.2.5 Einstufung in Risikoklassen

Die folgende Risikoklasse wird als angemessen befunden und sollte angewendet werden, wenn Softwareprüfungen für (softwaregesteuerte) Gaszähler und Mengenumwerter durchgeführt werden:

- Risikoklasse C für Messgeräte vom Typ P und U.

10.3 Elektrizitätszähler für Wirkverbrauch

10.3.1 Spezifische Vorschriften, Normen und andere normative Dokumente

Die spezifischen Anforderungen des vorliegenden Kapitels beruhen auf der MID, Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003)

Eine Anleitung zur Sicherung von Elektrizitätszählern für Wirkverbrauch sind auch im WELMEC-Leitfaden 11.3 enthalten.

Eine zusätzliche Anleitung oder Updates für Elektrizitätszähler für Wirkverbrauch sind der WELMEC-Webseite zu entnehmen.

Die nationale Gesetzgebung bezüglich zusätzlicher Funktionalität, OIML-Empfehlungen, harmonisierte (EN) Normen und (IEC) Normen wurden nicht berücksichtigt.

10.3.2 Technische Beschreibung

Hardwarekonfiguration

Elektrizitätszähler für Wirkverbrauch verwenden Spannung und Strom als Eingangsmessgrößen, leiten von ihnen die aktive elektrische Leistung ab und integrieren diese über der Zeit, um die aktive elektrische Energie abzugeben.

Elektrizitätszähler für Wirkverbrauch können zusammen mit externen Messwandlern betrieben werden.

10.3.2.2 Softwarekonfiguration

Die Softwarekonfiguration hängt vom Zählertyp ab, sollte sich aber normalerweise nach den Empfehlungen im Hauptteil dieses Leitfadens richten.

10.3.2.3 Messprinzip

Elektrizitätszähler für Wirkverbrauch kumulieren kontinuierlich die in einem Stromkreis verbrauchte Energie. Der kumulierte konsumierte Energiewert wird vom Gerät angezeigt.

Die Mengenummessung ist nicht wiederholbar.

10.3.2.4 Fehlererkennung und -reaktion

Die Anforderung in der MID, Anhang IV Elektrizitätszähler für Wirkverbrauch (MI-003), Artikel 4.3.1, beschäftigt sich mit der zulässigen Auswirkung von Störungen. Aus Softwaresicht macht es keinen Unterschied, was der Grund für eine Störung war (elektromagnetisch, elektrisch, mechanisch usw.): die Wiederaufnahme des Normalbetriebs verläuft immer gleich.

- Nach der Einwirkung einer Störgröße muss der Zähler:
 - einen Betrieb innerhalb der Fehlergrenzen wieder aufnehmen und
 - muss die Durchführbarkeit sämtlicher Messfunktionen gewährleisten, und
 - eine Wiederherstellung aller unmittelbar vor dem Auftreten der Störgröße vorhandenen Messdaten ermöglichen, und
 - darf die Änderung der gemessenen Energie den kritischen Wechselwert nicht überschreiten.

10.3.3 Spezielle Softwareanforderungen

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-1: MID, Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003), 4.3.1 Fehlerbehebung <i>Die Software muss nach einer Störung wieder zur normalen Verarbeitung zurückkehren.</i>		
Detaillierende Anmerkungen: Datumstempel-Flags zur Unterstützung der Protokollierung von Zeiträumen im Fehlbetrieb müssen eingerichtet werden.		
Erforderliche Dokumentation: Kurze Beschreibung des Fehlerbehebungsmechanismus und Erklärung wann er aktiviert wird. Und kurze Beschreibung der diesbezüglichen vom Hersteller durchgeführten Tests.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die Umsetzung der Fehlerbehebung geeignet ist. <i>Funktionsprüfungen:</i> • Funktionsprüfungen bei Vorhandensein definierter Störgrößen und provozierter Fehler.		
Beispiel einer akzeptablen Lösung: Der Hardware-Watchdog wird von einem zyklisch ausgeführten Mikroprozessor-Unterprogramm zurückgesetzt, um das Auslösen des Watchdogs zu verhindern. Wurde irgendeine Funktion nicht ausgeführt oder – im schlimmsten Fall – befindet sich der Mikroprozessor in einer fehlerbedingten Endlosschleife, wird der Watchdog nicht zurückgesetzt und nach einer bestimmten Zeitspanne ausgelöst.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-2: Rechtlich nicht relevante Software und dynamisches Verhalten <i>Die rechtlich nicht relevante Software darf das dynamische Verhalten eines Messprozesses nicht nachteilig beeinflussen.</i>		
Detaillierende Anmerkungen: Diese Anforderung stellt sicher, dass das dynamische Verhalten der rechtlich relevanten Software bei Echtzeitanwendungen von Zählern nicht in unzulässiger Weise durch rechtlich nicht relevante Software beeinflusst wird, d.h. dass die Ressourcen der rechtlich relevanten Software nicht in unzulässiger Weise vom rechtlich nicht relevanten Teil gemindert werden.		
Erforderliche Dokumentation: - Beschreibung der Unterbrechungshierarchie. - Zeitdiagramm der Softwareaufgaben. Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - ob die Dokumentation der Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben dem Programmierer des rechtlich nicht relevanten Softwareteils zur Verfügung steht. <i>Funktionsprüfungen:</i> - Bestätigen der korrekten Funktion bei Vorhandensein definierter Störgrößen und provozierte Fehler.		
Beispiel für eine akzeptable Lösung: Die Unterbrechungshierarchie ist so entworfen, dass nachteilige Einflüsse vermieden werden.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-3: Zusätzliche Funktionalität ⁸ <i>Die zusätzliche Funktionalität, beispielsweise die Vorauszahlung oder Intervallmessung⁹, sollte die rechtlich relevanten Messfunktionen nicht beeinflussen, wie in MID Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003) angegeben,</i>		
Detaillierende Anmerkungen: Eine zusätzliche Funktionalität ist zugelassen, beeinflussen jedoch nicht die in der MID, Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003) angegebenen rechtlich relevanten Messfunktionen.		
Erforderliche Dokumentation: Siehe S1 bis S3.		
Validierungsanleitung: Siehe S1 bis S3.		
Beispiel für eine akzeptable Lösung: Siehe S1 bis S3.		

⁸ Der Hersteller sollte immer die nationalen Anforderungen bezüglich der zusätzlichen Funktionalität berücksichtigen.

⁹ Bezüglich der Intervallmessung sind zusätzliche Anweisungen im WELMEC-Leitfaden 11.2 enthalten.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-4: MID, Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003), 4.3.1 Fehlerbehebung <i>Es kann eine Einrichtung vorhanden sein, die für ein regelmäßiges Backup von Messdaten (wie z.B. Messwerte und der aktuelle Prozessstatus) sorgt. Diese Daten müssen in einem nichtflüchtigen Speicher gehalten werden.</i>		
Detaillierende Anmerkungen: Wird die Sicherungsmöglichkeit für die Fehlerbehebung verwendet, muss der Mindestabstand für das Backup berechnet werden, um sicherzustellen, dass der kritische Wechselwert nicht überschritten wird.		
Erforderliche Dokumentation: Eine kurze Beschreibung, welche Daten gesichert werden und wann dies geschieht. Berechnung des Mindestabstands, um sicherzustellen, dass der kritische Wechselwert nicht überschritten wird.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob Messdaten im nichtflüchtigen Speicher gesichert werden und wiederhergestellt werden können. <i>Funktionsprüfungen:</i> • Funktionsprüfungen bei Vorhandensein definierter Störgrößen und provozierter Fehler.		
Beispiel einer akzeptablen Lösung: Für die Messdaten wird ein Backup wie gefordert ausgeführt.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-5: Software-Download <i>Während der Software-Installation sollte der Messvorgang insgesamt nicht länger als eine Minute gesperrt werden.</i> <i>Falls die Software-Installation mehr als eine Minute braucht, müssen zusätzliche Maßnahmen getroffen werden (z. B. findet die Installation bei niedrigem Energieverbrauch statt).</i>		
Detaillierende Anmerkungen: • Diese Anforderung gilt zusätzlich zu D1, D2, D3 und D4, wenn ein Software-Download durchgeführt wurde. • Die zusätzliche Anforderung stellt sicher, dass für Echtzeit-Anwendungen des Zählers Messungen nicht zu lange unterbrochen werden.		
Erforderliche Dokumentation: Siehe D1.		
Validierungsanleitung: Siehe D1.		
Beispiel für eine akzeptable Lösung: Siehe D1.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-6: MID-Anhang I, 8.5 (Rücksetzen kumulierter Messwerte verhindern) <i>Bei Versorgungsmessgeräten darf während des Betriebes ein Rücksetzen der Anzeige der gelieferten Gesamtmenge oder der Anzeigen, aus denen die gelieferte Gesamtmenge abgeleitet werden kann, die vollständig oder teilweise eine Grundlage für die Bezahlung ist, nicht möglich sein.</i>		
Detaillierende Anmerkungen: Kumulative Register eines Messgeräts dürfen vor dem anwendbaren Konformitätsbewertungsverfahren zurückgesetzt werden. Während eines Konformitätsbewertungsverfahrens gemäß Anhang D, F oder H1 müssen die Verbrauchszähler mit sämtlichen Sicherungsvorrichtungen gemäß TEC vom Hersteller ausgestattet sein, wonach die kumulativen Messwerte nicht ohne das Hinterlassen einer Spur zurückgesetzt werden können.		
Erforderliche Dokumentation: Dokumentation der Schutzmaßnahmen vor dem Rücksetzen der Energieregister.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob das Rücksetzen der kumulierten, rechtlich relevanten Messwerte gesichert ist und ob die vorgesehenen Sicherungsmaßnahmen den Nachweis eines Eingriffs ermöglichen. <i>Funktionsprüfungen:</i> • Bestätigung der korrekten Funktion der vorgesehenen Sicherungsmaßnahmen, siehe also P3/U3 und P4/U4.		
Beispiel einer akzeptablen Lösung: Der Register für die gemessene Gesamtmenge muss durch eine Hardware-Versiegelung geschützt sein. Andere Register, zum Beispiel Tages- oder Nachtтарifregister, müssen mit denselben Mitteln geschützt werden wie Parameter (siehe P7/U7), vorausgesetzt, dass ein Gesamtregister (insgesamt kumulativ) verfügbar ist, welcher von einer Hardware-Versiegelung geschützt ist. Zusätzliche Anweisungen sind im WELMEC-Leitfaden 11.1 enthalten.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-7: MID-Annex I, 10.5 Ablesen der Messergebnisse <i>Die Messergebnisse, die als Grundlage für den zu zahlenden Preis dienen, können Werte verschiedener Register sein, die durch eine Fernbedienung, Uhr oder andere Vorrichtungen aktiviert werden. Jeder Register steht für die Gesamtmenge, die mit einem Tarif im Fakturierungsprozess verbunden ist. Die Ergebnisse müssen mit Hilfe der Benutzerschnittstelle auf verschiedenen Anzeigen periodisch oder auf Anfrage dargestellt werden können.</i>		
Detaillierende Anmerkungen: Kumulative Register eines Messgeräts können vor dem anwendbaren Konformitätsbewertungsverfahren zurückgesetzt werden. Während eines Konformitätsbewertungsverfahrens gemäß Anhang D, F oder H1 müssen die Verbrauchszähler mit sämtlichen Sicherungsvorrichtungen gemäß TEC vom Hersteller ausgestattet sein, wonach die kumulativen Messwerte nicht ohne das Hinterlassen einer Spur zurückgesetzt werden können.		
Erforderliche Dokumentation: Dokumentation der Erzielung der Messergebnisse, was als Grundlage für den zu zahlenden Preis dient.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die Messergebnisse korrekt bearbeitet wurden. <i>Funktionsprüfungen:</i> • Bestätigen der korrekten Funktion der Bearbeitung der Messergebnisse.		
Beispiel einer akzeptablen Lösung: Wenn ein Zähler für die Zählung der Mengen in verschiedenen Registern gemäß MID, Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003) ausgelegt ist, muss (a) der Zähler die Gesamtmengen jedes Registers auf der Anzeige mit Hilfe der Benutzerschnittstelle (siehe dieser Leitfaden, z.B.: Tasten auf dem Geräte) sowie die derzeit aktiven Tarifregister darstellen können. Die Ergebnisse dürfen mit Hilfe der Benutzerschnittstelle periodisch oder auf Anfrage auf verschiedenen Anzeigen dargestellt werden. Bei der Anzeige verschiedener Messergebnisse muss jedoch klar sein, welche Anzeige zu welchem Register gehört; es darf diesbezüglich keine Unklarheiten geben.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-8: Schutz vor vorsätzlichen Änderungen bei Elektrizitätszählern für Wirkverbrauch vom Typ P mit einem mechanischen Register <i>Die berechnete Prüfsumme oder eine Alternativanzeige der Softwareänderung ist auf Befehl für Kontrollzwecke sichtbar zu machen, siehe P6. Für Elektrizitätszähler für Wirkverbrauch vom Typ P mit mechanischem Zähler wäre als Ausnahme ein Aufprägen der Prüfsumme oder eine Alternativanzeige der Softwareänderung auf das Typenschild eines Messgeräts eine akzeptable Lösung, wenn die folgenden Bedingungen A, B und C erfüllt sind:</i> <i>A Die Benutzerschnittstelle hat keinerlei Steuerungsfähigkeiten, um den Wert der Prüfsumme oder eine alternative Anzeige der Softwareänderung auf dem Display zu aktivieren, oder das Display gestattet die Anzeige dieser Werte aus technischen Gründen nicht (mechanischer Zähler).</i> <i>B. Das Messgerät hat keine Schnittstelle, um den Software-Identifikator zu übermitteln.</i> <i>C. Nach der Fertigung eines Zählers ist eine Änderung der Software nicht mehr möglich oder nur dann möglich, wenn auch die Hardware oder ein Hardwareteil, der die Software enthält, geändert wird.</i>		
Detaillierende Anmerkungen: • Der Hersteller ist dafür verantwortlich, dass die Prüfsumme oder eine Alternativanzeige der Softwareänderungen ordnungsgemäß auf der betroffenen Hardware angegeben ist. • Es gelten alle anderen Detaillierenden Anmerkungen von P6.		
Erforderliche Dokumentation: Gemäß P6.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • Gemäß P6. <i>Funktionsprüfungen:</i> • Gemäß P6.		
Beispiel für eine akzeptable Lösung: Aufprägen der Prüfsumme oder einer alternativen Anzeige der Softwareänderung auf das Typenschild des Messgeräts		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-9: MID, Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003), 5.2 Anzahl der Dezimalstellen <i>Die Anzeige der Gesamtmenge muss eine ausreichende Anzahl an Ziffern haben, damit sichergestellt ist, dass die Anzeige nicht auf ihren ursprünglichen Wert zurückspringt, wenn der Zähler 4000 Stunden bei voller Kapazität betrieben wird ($I = I_{max}$, $U = U_n$ und $PF = 1$).</i>		
Detaillierende Anmerkungen: 		
Erforderliche Dokumentation: Dokumentation der internen Darstellung des Energieregisters und der Hilfsgrößen.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> ob die Anzahl der Dezimalstellen ausreichend ist (intern und auf der Anzeige)		
Beispiel einer akzeptablen Lösung: Typische Werte für Dreiphasen-Stromzähler sind: $E_{max}(4000h) = 3 \cdot 60 \text{ A} \cdot 230 \text{ V} \cdot 4000h / 1000 = 165600 \text{ kWh}$. Dies erfordert eine Darstellung von mindestens 6 Ziffern.		

10.3.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Der Zugang zu Mitteln für die Änderung der Software, Einstellungen und/oder Parameter, die die Bestimmung der Messergebnisse beeinflussen, muss gesichert werden¹⁰.

Parameter	Geschützt	Einstellbar	Anmerkung
Kalibrierfaktor	x		
Linearisierungsfaktor	x		
Rechtlich relevante Konfiguration der Register	x		
Zum Beispiel Einstellungen: • Rechtlich relevante Parameter einer Korrekturereinrichtung, z.B. Parameter, die auf der Fehlerkurve eines Elektrizitätszähler für Wirkverbrauch beruhen • Stromwandlerverhältnis	x		
Sonstige relevanten Parameter, die das Messergebnis beeinflussen könnten	x		
Software-Download des rechtlich relevanten Softwareteils	x		

¹⁰ Der Hersteller sollte immer die nationalen Anforderungen hinsichtlich der zusätzlichen Funktionalität berücksichtigen. Bezüglich der Intervallmessung sind zusätzliche Anweisungen im WELMEC-Leitfaden 11.2 enthalten.

10.3.5 Einstufung in Risikoklassen

Die folgende Risikoklasse wird als angemessen befunden und sollte angewendet werden, wenn auf diesem Leitfaden beruhende Softwareprüfungen für (softwaregesteuerte) Elektrizitätszähler für Wirkverbrauch durchgeführt werden:

- Risikoklasse C für Messgeräte vom Typ P und U.

10.4 Wärmezähler

10.4.1 Spezifische Vorschriften, Normen und andere normative Dokumente

Die Mitgliedstaaten können – gemäß Artikel 2 der MID – festlegen, dass Wärmezähler für Privathaushalte, Gewerbe und Leichtindustrie den Bestimmungen in der MID unterliegen. Die spezifischen Anforderungen des vorliegenden Kapitels beruhen ausschließlich auf Anhang VI (MI-004) der MID.

10.4.2 Technische Beschreibung

10.4.2.1 Hardwarekonfiguration

Die Wärmezähler sind Geräte zur Messung der Wärmeenergie, die von dem Wärmeträger übertragen wird. Ein Wärmeenergiezähler ist entweder ein vollständiges Gerät oder ein Kombigerät, das aus den Teilgeräten besteht (Modulkonzept), z. B. Durchflusssensor, Temperaturfühlerpaar und Rechenwerk, wie in der MID Artikel 4(b) definiert. Ein Wärmezähler kann eine Kombination aus beiden sein. Getrennte Baugruppen von Wärmezählern mit einer Auswerteeinheit (die Software enthält) müssen ebenfalls das Bewertungsverfahren durchlaufen.

10.4.2.2 Softwarekonfiguration

Die Softwarekonfiguration wird vom Hersteller festgelegt, sollte sich aber normalerweise nach den Empfehlungen im Hauptteil dieses Leitfadens richten.

10.4.2.3 Messprinzip

Wärmezähler kumulieren kontinuierlich die in einem Wärmekreislauf verbrauchte Energie. Der kumulierte Energiewert wird auf dem Gerät angezeigt. Es werden verschiedene Prinzipien angewendet. Die Energiemessung kann nicht wiederholt werden.

10.4.2.4 Fehlererkennung und -reaktion

Die Anforderung VI (MI-004), 4.1 und 4.2, behandeln elektromagnetische Störungen. Es ist notwendig, diese Anforderungen für softwaregesteuerte Geräte zu interpretieren, da das Entdecken einer Störung sowie das Beheben nur durch das Zusammenwirken spezieller Hardwareteile und spezieller Software möglich ist. Aus Softwaresicht macht es keinen Unterschied, was der Grund für eine Störung war (elektromagnetisch, elektrisch, mechanisch usw.): die Wiederaufnahme des Normalbetriebs verläuft immer gleich.

Nach der Einwirkung einer elektromagnetischen Störgröße muss der Wasserzähler

- einen Betrieb innerhalb der Fehlergrenzen wieder aufnehmen und
- muss die Durchführbarkeit sämtlicher Messfunktionen gewährleistet sein, und
- eine Wiederherstellung aller unmittelbar vor dem Auftreten der Störgröße vorhandenen Messdaten ermöglichen" (siehe EN 1434-4:2015 Kapitel 7)

10.4.3 Spezielle Softwareanforderungen

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-1: Fehlerbehebung <i>Die Software muss nach einer Störung wieder zur normalen Verarbeitung zurückkehren.</i>		
Detaillierende Anmerkungen: Datumstempel-Flags zur Unterstützung der Protokollierung von Zeiträumen im Fehlbetrieb müssen eingerichtet werden.		
Erforderliche Dokumentation: - Kurze Beschreibung der Fehlerbehebungsmechanismus und Erklärung, wann er aktiviert wird. - Kurze Beschreibung der diesbezüglichen vom Hersteller durchgeführten Tests.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - ob die Umsetzung der Fehlerbehebung geeignet ist. <i>Funktionsprüfungen:</i> - Bestätigen der korrekten Funktion bei Vorhandensein definierter Störgrößen und provozierter Fehler.		
Beispiel einer akzeptablen Lösung: Der Hardware-Watchdog wird von einem zyklisch ausgeführten Mikroprozessor-Unterprogramm zurückgesetzt, um das Auslösen des Watchdogs zu verhindern. Wurde irgendeine Funktion nicht ausgeführt oder – im schlimmsten Fall – befindet sich der Mikroprozessor in einer fehlerbedingten Endlosschleife, wird der Watchdog nicht zurückgesetzt und nach einer bestimmten Zeitspanne ausgelöst.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-2: Rechtlich nicht relevante Software und dynamisches Verhalten <i>Es muss eine Einrichtung vorhanden sein, die für ein regelmäßiges Backup von Messdaten (wie z.B. Messwerte und der aktuelle Prozessstatus) sorgt. Diese Daten müssen in einem nichtflüchtigen Speicher gehalten werden.</i>		
Detaillierende Anmerkungen: Diese Anforderung stellt sicher, dass das dynamische Verhalten der rechtlich relevanten Software bei Echtzeitanwendungen von Zählern nicht in unzulässiger Weise durch rechtlich nicht relevante Software beeinflusst wird, d.h. dass die Ressourcen der rechtlich relevanten Software nicht in unzulässiger Weise vom rechtlich nicht relevanten Teil gemindert werden.		
Erforderliche Dokumentation: - Beschreibung der Unterbrechungshierarchie. - Zeitdiagramm der Softwareaufgaben. Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - ob die Dokumentation der Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben dem Programmierer des rechtlich nicht relevanten Softwareteils zur Verfügung steht. <i>Funktionsprüfungen:</i> - Bestätigen der korrekten Funktion bei Vorhandensein definierter Störgrößen und provozierter Fehler.		
Beispiel einer akzeptablen Lösung: Die Unterbrechungshierarchie ist so entworfen, dass nachteilige Einflüsse vermieden werden.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-3: Zusätzliche Funktionalität ¹¹ <i>Die zusätzliche Funktionalität, beispielsweise die Vorauszahlung oder Intervallmessung¹², sollte die rechtlich relevanten Messfunktionen nicht beeinflussen, wie in MID Anhang VI Wärmezähler (MI-004).</i>		
Detaillierende Anmerkungen: Eine zusätzliche Funktionalität ist zugelassen, wenn sie die in der MID, Anhang VI Anhang Elektrizitätszähler für Wirkverbrauch (MI-004) genannten rechtlich relevanten Messfunktionen nicht beeinflusst.		
Erforderliche Dokumentation: Siehe S1 bis S3.		
Validierungsanleitung: Siehe S1 bis S3.		
Beispiel einer akzeptablen Lösung: Siehe S1 bis S3.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-4: Backup-Einrichtungen <i>Es kann eine Einrichtung vorhanden sein, die für ein regelmäßiges Backup von Messdaten (wie z.B. Messwerte und der aktuelle Prozessstatus) sorgt. Diese Daten müssen in einem nichtflüchtigen Speicher gehalten werden.</i>		
Detaillierende Anmerkungen: Wird die Sicherungsmöglichkeit für die Fehlerbehebung verwendet, muss der Mindestabstand für das Backup berechnet werden, um sicherzustellen, dass der kritische Wechselwert nicht überschritten wird.		
Erforderliche Dokumentation: • Eine kurze Beschreibung, welche Daten gesichert werden und wann dies geschieht. • Berechnung des Mindestabstands, um sicherzustellen, dass der kritische Wechselwert nicht überschritten wird.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob Messdaten im nichtflüchtigen Speicher gesichert werden und wiederhergestellt werden können. <i>Funktionsprüfungen:</i> • Bestätigen der korrekten Funktion bei Vorhandensein definierter Störgrößen und provozierter Fehler.		
Beispiel einer akzeptablen Lösung: Für die Messdaten wird ein Backup wie gefordert ausgeführt.		

¹¹ Der Hersteller sollte immer die nationalen Anforderungen bezüglich der zusätzlichen Funktionalität berücksichtigen.

¹² Bezüglich der Intervallmessung sind zusätzliche Anweisungen im WELMEC-Leitfaden 13.3 enthalten.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-5: Software-Download <i>Während der Software-Installation sollte der Messvorgang insgesamt nicht länger als eine Minute gesperrt werden.</i> <i>Falls die Software-Installation mehr als eine Minute braucht, müssen zusätzliche Maßnahmen getroffen werden (z. B. findet die Installation bei niedrigem Energieverbrauch statt).</i>		
Detaillierende Anmerkungen: • Diese Anforderung gilt zusätzlich zu D1, D2, D3 und D4, wenn eine Softwaretrennung durchgeführt wurde. • Die zusätzliche Anforderung stellt sicher, dass für Echtzeit-Anwendungen des Zählers Messungen nicht zu lange unterbrochen werden.		
Erforderliche Dokumentation: Siehe D1, D2, D3 und D4.		
Validierungsanleitung: Siehe D1, D2, D3 und D4.		
Beispiel einer akzeptablen Lösung: Siehe D1, D2, D3 und D4.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-6: MID-Anhang I, 8.5 Rücksetzen kumulierter Messwerte verhindern <i>Bei Versorgungsmessgeräten darf während des Betriebes ein Rücksetzen der Anzeige der gelieferten Gesamtmenge oder der Anzeigen, aus denen die gelieferte Gesamtmenge abgeleitet werden kann, die vollständig oder teilweise die Grundlage für die Bezahlung ist, nicht möglich sein.</i>		
Detaillierende Anmerkungen: • Kumulative Register eines Messgeräts dürfen vor der Inbetriebnahme zurückgesetzt werden. Während eines Konformitätsbewertungsverfahrens gemäß Anhang D, F oder H1 müssen die Wärmezähler mit sämtlichen Sicherungsvorrichtungen gemäß TEC vom Hersteller ausgestattet sein, wonach die kumulativen Messwerte nicht ohne das Hinterlassen einer Spur zurückgesetzt werden können. • Totalisatoren der kumulativen Register eines Messgeräts müssen zurückgesetzt werden, bevor das relevante Konformitätsbewertungsverfahren beendet ist. Während des Konformitätsbewertungsverfahrens gemäß Anhang Annex D, F oder H1 müssen die Wärmezähler mit allen Sicherungsvorrichtungen gemäß TEC ausgerüstet sein, die den Nachweis eines Eingriffs in den Meterregistern ermöglichen sollen, nachdem die kumulativen Messwerte zurückgesetzt worden sind. Kumulative Register dürfen nicht während der Verwendung im Verteilernetz zurückgesetzt werden. Anmerkung: festgelegt in der EN 1434-1:2015 unter 5.10 – Spezifische Anforderungen an Registriergeräte		
Erforderliche Dokumentation: Dokumentation der Schutzmaßnahmen vor dem Rücksetzen der Energieregister.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob das Rücksetzen der kumulierten, rechtlich relevanten Messwerte gesichert ist und ob die vorgesehenen Sicherungsmaßnahmen den Nachweis eines Eingriffs ermöglichen. <i>Funktionsprüfungen:</i> • Bestätigung der korrekten Funktion der vorgesehenen Sicherungsmaßnahmen, siehe also P3/U3 und P4/U4.		
Beispiel einer akzeptablen Lösung: Der Register für die gemessene Gesamtmenge muss durch eine Hardware-Versiegelung geschützt sein. Andere Register, zum Beispiel Tages- oder Nachtтарifregister, müssen mit denselben Mitteln geschützt werden wie Parameter (siehe P7/U7), vorausgesetzt, dass ein Gesamtregister (insgesamt kumulativ) verfügbar ist, welcher von einer Hardware-Versiegelung geschützt ist. Zusätzliche Anweisungen sind im WELMEC-Leitfaden 13.1 enthalten.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-7: MID Anhang I, 10.5 Ablesen der Messergebnisse <i>Die Messergebnisse, die als Grundlage für den zu zahlenden Preis dienen, können Werte verschiedener Register sein, die durch eine Fernbedienung, Uhr oder andere Vorrichtungen aktiviert werden. Jeder Register steht für die Gesamtmenge, die mit einem Tarif im Fakturierungsprozess verbunden ist. Die Ergebnisse müssen mit Hilfe der Benutzerschnittstelle auf verschiedenen Anzeigen periodisch oder auf Anfrage dargestellt werden können.</i>		
Detaillierende Anmerkungen: Kumulative Register eines Messgeräts können vor dem anwendbaren Konformitätsbewertungsverfahren zurückgesetzt werden. Während eines Konformitätsbewertungsverfahrens gemäß Anhang D, F oder H1 müssen die Verbrauchszähler mit sämtlichen Sicherungsvorrichtungen gemäß TEC vom Hersteller ausgestattet sein, wonach die kumulativen Messwerte nicht ohne das Hinterlassen einer Spur zurückgesetzt werden können. Wenn der größte Anzeigebereich der Wärmemengentotalisierung erreicht ist, misst der Anzeigebereich beginnend bei null Kubikmeter weiter, siehe auch I1-9 (Anzahl der Ziffern).		
Erforderliche Dokumentation: Dokumentation der Erzielung der Messergebnisse, was als Grundlage für den zu zahlenden Preis dient.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die Messergebnisse korrekt bearbeitet wurden. <i>Funktionsprüfungen:</i> • Bestätigen der korrekten Bearbeitung der Messergebnisse.		
Beispiel einer akzeptablen Lösung: Wenn ein Zähler für die Zählung der Mengen in verschiedenen Registern gemäß MID Anhang VI Wärmezähler (MI-004) ausgelegt ist, muss ein Zähler die Gesamtmengen jedes Registers auf der Anzeige mit Hilfe der Benutzerschnittstelle (siehe P3/U3, z.B.: Tasten auf Geräten) sowie die derzeit aktiven Tarifregister darstellen können. Die Ergebnisse dürfen mit Hilfe der Benutzerschnittstelle periodisch oder auf Anfrage auf verschiedenen Anzeigen dargestellt werden. Bei der Anzeige verschiedener Messergebnisse muss jedoch klar sein, welche Anzeige zu welchem Register gehört; es darf diesbezüglich keine Unklarheiten geben. Falls notwendig, können zusätzliche Beschriftungen auf dem Wärmezähler angebracht werden, wobei die verschiedenen Register oder die Anzeige des Testmodus zu klären sind (siehe I1-9).		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-8: MID Anhang I Schutz vor vorsätzlichen Änderungen bei Wärmezählern vom Typ P (mit mechanischem Zähler) <i>Die berechnete Prüfsumme oder eine Alternativanzeige, um den Nachweis der Softwareänderung zu unterstützen, ist auf Befehl für Kontrollzwecke sichtbar zu machen, siehe P6. Für Wärmezähler vom Typ P mit einem mechanischen Zähler wäre als Ausnahme ein Aufprägen der Prüfsumme oder einer Alternativanzeige der Softwareänderung auf das Typenschild eines Messgeräts eine akzeptable Lösung, wenn die folgenden Bedingungen A, B und C erfüllt sind:</i> A. <i>Die Benutzerschnittstelle hat keinerlei Steuerungsfähigkeiten, um die Anzeige des Prüfsummenwertes oder eine Alternativanzeige der Softwareänderung auf dem Display zu aktivieren, oder das Display gestattet die Anzeige der Werte aus technischen Gründen nicht (mechanischer Zähler).</i> B. <i>Das Messgerät hat keine Schnittstelle, um den Software-Identifikator zu übermitteln.</i> C. <i>Nach der Fertigung eines Zählers ist eine Änderung der Software nicht mehr möglich oder nur dann möglich, wenn auch die Hardware oder ein Hardwareteil, welches die Software enthält, geändert wird.</i>		
Detaillierende Anmerkungen: • Der Hersteller ist dafür verantwortlich, dass die Prüfsumme oder eine Alternativanzeige der Softwareänderungen ordnungsgemäß auf der betroffenen Hardware angegeben ist. • Es gelten alle anderen Detaillierenden Anmerkungen von P6.		
Erforderliche Dokumentation: Gemäß P6.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • Gemäß P6. <i>Funktionsprüfungen:</i> • Gemäß P6.		
Beispiel einer akzeptablen Lösung: Aufprägen der Prüfsumme oder einer alternativen Anzeige der Softwareänderung auf das Typenschild des Messgeräts		

Risikoklasse B	Risikoklasse C	Risikoklasse D
----------------	----------------	----------------

I4-9: Stellenanzahl

Gemäß EN1434-1:2015 Ziffer 6.3.7:

Die Anzeige, die die Wärmemenge darstellt, muss ohne Überlauf eine Wärmemenge registrieren können, die mindestens der übertragenen Energiemenge entspricht, die wiederum einem kontinuierlichen Betrieb über 3 000 h bei Obergrenze der Wärmeleistung des Wärmezählers entspricht. Die von einem Wärmezähler gemessene Wärmemenge, welcher 1h lang bei Obergrenze der Wärmeleistung betrieben wird, muss mindestens einer Ziffer der niedrigsten Signifikanz der Anzeige entsprechen.

Eignung gemäß Absatz 7.6 und 10.5 von Anhang I der Richtlinie 2014/32/EU (MID):

Ein Messgerät ist so auszulegen, dass die Messvorgänge kontrolliert werden können, nachdem das Messgerät in Verkehr gebracht und in Betrieb genommen wurde. Falls erforderlich muss das Messgerät eine spezielle Ausrüstung oder Software für diese Kontrolle besitzen. Darüber hinaus muss ein Messgerät, das fernabgelesen werden kann, auf jeden Fall mit einer der messtechnischen Kontrolle unterliegenden Anzeige ausgestattet sein, die für den Verbraucher ohne Hilfsmittel zugänglich ist.

Wenn der größte Anzeigebereich der Wärmemengentotalisierung erreicht ist, misst der Anzeigebereich beginnend bei null Kubikmeter weiter, siehe auch I1-9 (Anzahl der Ziffern).

Hinweis: Die Bezeichnungen Wärmezähler und thermischer Energiezähler werden identisch verwendet.

Detaillierende Anmerkungen:

- Für den Test muss der Signalausgang den Anforderungen der EN1434-2 Ziffer 5.3 genügen.
- Die Anzeigevorrichtung eines Wasserzählers sollte eine leicht ablesbare, zuverlässige und eindeutige visuelle Anzeige des angezeigten Volumens liefern. Ein kombinierter Zähler kann über zwei Anzeigeeinrichtungen verfügen, deren Summe dann das angezeigte Volumen bilden.
- Jede Anzeigevorrichtung muss mit Mitteln zur visuellen, eindeutigen Eichprüfung und Kalibrierung ausgestattet sein.
- Die visuelle Prüfanzeige darf entweder eine kontinuierliche oder eine nicht kontinuierliche Bewegung aufweisen.

Erforderliche Dokumentation:

- Dokumentation der internen Darstellung des Energierechners, Temperatursensors und der Durchflussmessgeräte.
- Eine Beschreibung der Anzeige und des Anzeige-Menüs.
- Eine Beschreibung der visuellen Prüfanzeige und eine Erklärung, wie die visuelle Prüfanzeige ausgelöst wird.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu überprüfen:

- ob die Anzahl der Dezimalstellen ausreichend ist (intern und auf der Anzeige)

Funktionsprüfungen:

- ob die Stellenanzahl auf dem Display für die Gesamtmenge ausreicht
- Auslösen der visuellen Anzeige und
 - ob die visuelle Eichanzeige die Anforderungen erfüllt
 - ob eine spezielle Ausrüstung oder Software für diese Kontrolle (gegebenenfalls) Teil des Messgerätes ist.

Beispiel einer akzeptablen Lösung:

Auf der Anzeige des Wärmezählers gibt es eine ausreichende Stellenanzahl, die beide Anforderungen an die Gesamtmenge mit der erforderlichen Auflösung erfüllt.

Umschalten von Anzeigemodi auf der Anzeigevorrichtung, um die Werte für die Gesamtmenge mit der korrekten Auflösung sowie den "Prüfmodus" mit den zusätzlichen Prüfelementen aufzuzeigen. Diese Anzeigemodi müssen mit Hilfe folgender Elemente angezeigt werden können:

- der Benutzerschnittstelle (siehe P3/U3, z. B.: Tasten auf Geräten) oder
- beim Durchlaufen der verschiedenen Anzeigemodi.

Es sollte jedoch klar sein, um welche Primäranzeige es sich handelt, wenn verschiedene Anzeigemodi verwendet werden. Es muss klar sein, wie diese Werte abgelesen werden müssen, und es darf keine Uneindeutigkeit bezüglich anderer Anzeigemodi geben. (siehe I1-7).

Anmerkung: Es steht nicht im Einklang mit den wesentlichen Anforderungen der Richtlinie 2014/32/EU (MID) gemäß Artikel 7.6, Anhang I, dass eine Eichbehörde, Prüfbehörde oder benannte Stelle beim Hersteller nach speziellen Prüfeinrichtungen oder Software nachfragen muss.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-10: Anzeigetest (Display-Test) <i>Zur Verifizierung der korrekten Funktion aller Segmente der elektronischen Anzeige muss ein Anzeigetest durchgeführt werden können.</i>		
Detaillierende Anmerkungen: Der Anzeigetest lautet wie folgt: - Der Zähler soll eine Sichtprüfung der gesamten Anzeigeeinrichtung mit folgendem Verlauf erlauben: - bei sieben Segmenttypen: Anzeige aller Elemente (z. B. ein sogenannter "8er-Test"); - bei sieben Segmenttypen: Abschalten aller Elemente ("Abschalt"-Test). - bei grafischen Anzeigen: äquivalenter Test, der aufzeigt, dass Anzeigefehler nicht dazu führen können, dass irgendeine Ziffer fehlinterpretiert wird. - Jeder Schritt dieses Verfahrens muss mindestens 1 Sekunde dauern.		
Erforderliche Dokumentation: Eine Beschreibung des elektronischen Anzeigetests und eine Erklärung, wie ein solcher Test gestartet wird.		
Validierungsanleitung: Starten des Anzeigetests und Prüfen, ob eine visuelle Prüfung der gesamten Anzeige möglich ist.		
Beispiel einer akzeptablen Lösung: Ein Anzeigetest wird auf Sonderbefehl durch die Benutzerschnittstelle gestartet (siehe P3/U3, z.B.: Tasten auf Geräten) oder ist Teil des Durchlaufverfahrens, welches die verschiedenen Anzeigemodi zeigt.		

10.4.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Der Zugang zu Mitteln für die Änderung der Software, Einstellungen und/oder Parameter, die die Bestimmung der Messergebnisse beeinflussen, muss gesichert werden¹³.

Parameter	Geschützt	Einstellbar	Anmerkung
Kalibrierfaktor	x		
Linearisierungsfaktor	x		
Rechtlich relevante Konfiguration der Register	x		
Sonstige relevanten Parameter, die das Messergebnis beeinflussen könnten – Einheit für Energiemessung (MWh, GJ), Installation des Durchflusssensors (Versorgung, Rückleitung des Wärmekreislaufs)	x		
Software-Download des rechtlich relevanten Softwareteils	x		

10.4.5 Einstufung in Risikoklassen

Die folgende Risikoklasse wird als angemessen befunden und sollte angewendet werden, wenn Softwareprüfungen für (softwaregesteuerte) Wärmezähler durchgeführt werden:

- Risikoklasse C für Messgeräte vom Typ P

10.5 Messsysteme zur kontinuierlichen und dynamischen Mengenmessung von Flüssigkeiten außer Wasser

Messsysteme zur kontinuierlichen und dynamischen Mengenmessung von Flüssigkeiten außer Wasser unterliegen den Vorschriften der MID. Die spezifischen Anforderungen des vorliegenden Kapitels beruhen ausschließlich auf Anhang I und Anhang VII (MI-005).

10.5.3 Spezielle Softwareanforderungen (Messsysteme für Flüssigkeiten außer Wasser)

Risikoklasse B	Risikoklasse C	Risikoklasse D
-----------------------	-----------------------	-----------------------

¹³ Der Hersteller sollte immer die nationalen Anforderungen hinsichtlich der zusätzlichen Funktionalität berücksichtigen. Bezüglich der Intervallmessung sind zusätzliche Anweisungen im WELMEC-Leitfaden 13.3 enthalten.

I5-1: Aufgeprägter Software-Identifikator

Der Software-Identifikator wird normalerweise auf einem Display angezeigt. Für Messsysteme für Flüssigkeiten außer Wasser wäre als Ausnahme ein Aufprägen des Software-Identifikators auf das Typenschild eines Messgeräts eine akzeptable Lösung, wenn die folgenden Bedingungen A, B und C erfüllt sind:

- A Die Benutzerschnittstelle hat keinerlei Steuerungsfähigkeiten, um die Anzeige des Software-Identifikators auf dem Display zu aktivieren, oder das Display gestattet die Anzeige des Software-Identifikators auf dem Display aus technischen Gründen nicht oder es gibt kein Display am Gerät.*
- B. Das Messgerät hat keine Schnittstelle, um den Software-Identifikator zu übermitteln.*
- C. Nach der Fertigung eines Zählers ist eine Änderung der Software nicht mehr möglich oder nur dann möglich, wenn auch die Hardware oder ein Hardwareteil geändert wird.*

Detaillierende Anmerkungen:

- Der Aufkleber, der den Software-Identifikator aufweist, darf weder löschar noch übertragbar sein.
- Der Hersteller der Hardware bzw. des betroffenen Hardwareteils ist dafür verantwortlich, dass der Software-Identifikator ordnungsgemäß auf der betroffenen Hardware angegeben ist.
- Es gelten alle anderen Detaillierenden Anmerkungen von P2/U2.

Erforderliche Dokumentation:

- Gemäß P2/U2.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu überprüfen:

- Gemäß P2/U2.

Funktionsprüfungen:

- Gemäß P2/U2.

Beispiel für eine akzeptable Lösung:

Aufprägen des Software-Identifikators auf das Typenschild des Messgeräts

10.5.4 - 10.5.5 werden ausgefüllt, falls dies in Zukunft notwendig erscheint.

10.5.6 Einstufung in Risikoklassen

Gemäß dem Ergebnis, das der Fragebogen der WELMEC-Arbeitsgruppe 7 (2004) erbracht hat, und unter der Prämisse zukünftiger Entscheidungen der verantwortlichen WELMEC-Arbeitsgruppe sollte die folgende Risikoklasse angewendet werden, wenn Softwareprüfungen für (softwaregesteuerte) Messsysteme zur kontinuierlichen und dynamischen Mengemessung von Flüssigkeiten außer Wasser auf Grundlage dieses Leitfadens durchgeführt werden:

- **Risikoklasse C**

10.6 Waagen

Waagen werden in zwei Hauptkategorien unterteilt:

1. nicht selbsttätige Waagen (NSW) und
2. selbsttätige Waagen (SW)

Während die meisten selbsttätigen Waagen durch die MID geregelt sind, gilt dies nicht für NSW; diese werden immer noch durch die EU-Richtlinie 90/384/EEC geregelt. **Daher gilt der Softwareleitfaden WELMEC 2.3 für NSW, während der vorliegende Softwareleitfaden für SW gilt.**

Die speziellen Anforderungen des vorliegenden Kapitels beruhen auf Anhang MI-006 und den unter Punkt 10.6.1 genannten normativen Dokumenten, sofern diese die Auslegung der MID-Anforderungen unterstützen.

10.6.1 Spezifische Vorschriften, Normen und andere normative Dokumente

Fünf Kategorien von selbsttätigen Waagen (SW) sind Gegenstand der Regelungen der MID Anhang MI-006:

- selbsttätige Waagen für Einzelwägungen (R51)
- selbsttätige Waagen zum Abwägen (R61)
- selbsttätige Waagen zum diskontinuierlichen Totalisieren (R107)
- selbsttätige Waagen zum kontinuierlichen Totalisieren (Förderbandwaagen) (R50)
- selbsttätige Gleiswaagen (R106)

Die Nummern in Klammern beziehen sich auf die jeweiligen Empfehlungen der OIML, den normativen Dokumenten im Sinne der MID. Darüber hinaus hat WELMEC den WELMEC-Leitfaden 2.6 herausgegeben, der das Prüfen selbsttätiger Waagen für Einzelwägungen unterstützt.

Eine Kategorie der SW ist nicht in der MID geregelt:

- selbsttätige Waagen für Straßenfahrzeuge in Bewegung (R134)

Die selbsttätigen Waagen aller Kategorien können als Typ P oder Typ U umgesetzt werden, und alle Anhänge können für jede Kategorie relevant sein.

Von diesen sechs Kategorien wurde jedoch nur für die Kategorien "Selbsttätige Waagen zum **diskontinuierlichen Totalisieren**" und "Selbsttätige Waagen zum **kontinuierlichen Totalisieren** (Förderbandwagen)" die Notwendigkeit ausgemacht, messgerätespezifische Softwareanforderungen aufzustellen (siehe 10.6.3). Der Grund hierfür ist, dass die Messung über einen relativ langen Zeitraum kumulativ ist und nicht wiederholt werden kann, wenn ein signifikanter Fehler auftritt.

10.6.2 Technische Beschreibung

10.6.2.1 Hardwarekonfiguration

Eine "Selbsttätige Waage zum diskontinuierlichen Totalisieren" ist eine totalisierende Behälterwaage, die die Masse eines Schüttgutes (z.B. Getreide) durch seine Unterteilung in Einzellasten bestimmt. Das System besteht normalerweise aus einem oder mehreren Behältern, die mit Wägezellen, Stromversorgung, Steuerelektronik und Anzeigevorrichtung ausgerüstet sind.

Eine "Selbsttätige Waage zum kontinuierlichen Totalisieren" ist eine Förderbandwaage, die die Masse eines Produkts misst, während das Band über eine Wägezelle läuft. Das System besteht normalerweise aus einem Förderband, Walzen und einem Lastaufnehmer, die mit Wägezellen, Energieversorgung, Steuerelektronik und Anzeigevorrichtung ausgerüstet sind. Es gibt Mittel zum Anpassen der Förderbandspannung.

10.6.2.2 Softwarekonfiguration

Die Softwarekonfiguration wird vom Hersteller festgelegt, sollte sich aber normalerweise nach den Empfehlungen im Hauptteil dieses Leitfadens richten.

10.6.2.3 Messprinzip

Bei einer "Selbsttätigen Waage zum diskontinuierlichen Totalisieren" wird das Schüttgut in einen Behälter gefüllt und gewogen. Die Masse jeder Einzellast wird der Reihe nach bestimmt und aufsummiert. Jede Einzellast wird dann zur Gesamtmasse hinzugefügt.

Bei einer "Selbsttätigen Waage zum kontinuierlichen Totalisieren" wird die Masse kontinuierlich gemessen, während das Produkt über den Lastaufnehmer läuft. Die Messungen erfolgen in einzelnen Zeiteinheiten, die von der Bandgeschwindigkeit und dem Druck auf den Lastaufnehmer abhängen. Bei einer "Selbsttätigen Waage zum diskontinuierlichen Totalisieren" gibt es keine gezielte Unterteilung des Produkts oder Unterbrechung des Förderbands wie bei einer "Selbsttätigen Waage zum diskontinuierlichen Totalisieren". Die Gesamtmasse ist eine Integration der einzelnen Messungen. Es ist anzumerken, dass für den Lastaufnehmer Dehnungsmessstreifen-Wägezellen oder andere Techniken, z.B. Schwingfaden, verwendet werden können.

10.6.2.4 Defekte

Verbindungsstellen im Band können Stoßwirkungen erzeugen, die bei Nullstellung zu fehlerhaften Ereignissen führen können. Bei "Selbsttätigen Waagen zum diskontinuierlichen Totalisieren" können einzelne oder sämtliche Wägeergebnisse von Einzellasten verlorengehen, bevor sie aufsummiert werden.

10.6.3 Spezielle Softwareanforderungen (Selbsttätige Waagen zum diskontinuierlichen und zum kontinuierlichen Totalisieren)

MID Anhang MI-006, Kapitel IV, Abschnitt 8, und Kapitel V, Abschnitt 6 behandeln elektromagnetische Störungen. Es besteht die Notwendigkeit, diese Anforderungen für softwaregesteuerte Geräte zu interpretieren, da die Entdeckung einer Störung (eines Fehlers) sowie die nachfolgende Behebung nur durch das Zusammenwirken spezieller Hardwareteile und spezieller Software möglich sind. Aus Softwaresicht ist es gleichgültig, was der Grund für die Störung war (elektromagnetisch, elektrisch, mechanisch usw.); die Wiederaufnahme des Normalbetriebs verläuft immer gleich.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I6-1: Fehlererkennung <i>Die Software muss erkennen, dass die normale Verarbeitung gestört ist.</i>		
Detaillierende Anmerkungen: Bei Entdeckung eines Fehlers: - Die kumulativen Messwerte und andere rechtlich relevante Daten müssen automatisch in einem nichtflüchtigen Speicher gesichert werden (siehe Anforderung I6-2), und - die Behälterwaage oder Förderbandwaage muss automatisch angehalten oder ein sichtbares oder hörbares Alarmsignal muss gegeben werden (siehe "Erforderliche Dokumentation")		
Erforderliche Dokumentation: Kurze Beschreibung, auf welche Fehler geprüft wird, was für das Auslösen der Fehlererkennung erforderlich ist, welche Aktion bei Fehlererkennung zu ergreifen ist. Ist es nach Erkennung eines Fehlers nicht möglich, das Transportsystem ohne Verzögerung automatisch anzuhalten (z.B. aus Sicherheitsgründen), muss die Dokumentation eine Beschreibung beinhalten, wie das nicht gemessene Material zu behandeln oder richtig zu berücksichtigen ist.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> - ob die Umsetzung der Fehlererkennung geeignet ist. <i>Funktionsprüfungen:</i> - Falls möglich: Simulieren bestimmter Hardwarefehler und Überprüfen, ob die Software sie entdeckt und so wie in der Dokumentation beschrieben auf sie reagiert.		
Beispiel einer akzeptablen Lösung: Ein Hardware-Watchdog wird von einem zyklisch ausgeführten Mikroprozessor-Unterprogramm zurückgesetzt, um das Auslösen des Watchdogs zu verhindern. Vor dem Zurücksetzen prüft das Unterprogramm den Zustand des Systems, z.B. ob alle rechtlich relevanten Unterprogramme während des letzten Intervalls ausgeführt wurden. Wurde irgendeine Funktion nicht ausgeführt oder – im schlimmsten Fall – befindet sich der Mikroprozessor in einer beliebigen Endlosschleife, wird der Watchdog nicht zurückgesetzt und nach einer bestimmten Zeitspanne ausgelöst.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I6-2: Backup-Einrichtungen <i>Es muss eine Einrichtung vorhanden sein, die für ein regelmäßiges Backup von Messdaten (wie z.B. Messwerte und aktueller Prozessstatus) im Falle einer Störung sorgt.</i>		
Detaillierende Anmerkungen: a. Die Zustandsmerkmale und wichtige Daten müssen in einem nichtflüchtigen Speicher gespeichert werden. b. Diese Anforderung impliziert normalerweise eine kontrollierte Speichermöglichkeit, die im Falle einer Störung ein automatisches Backup gestattet. Periodisches Backup ist nur dann zulässig, wenn aufgrund von Hardware- oder Funktionsbeschränkungen keine kontrollierte Speichermöglichkeit vorhanden ist. In diesem Ausnahmefall müssen die Abstände zwischen den einzelnen Backups ausreichend klein sein, d.h. die größtmögliche Diskrepanz zwischen den laufenden und den gespeicherten Werten muss innerhalb eines festgelegten Bruchteils des höchstzulässigen Fehlers liegen (siehe unter "Erforderliche Dokumentation"). c. Die Backup-Einrichtungen sollten normalerweise geeignete Weckeinrichtungen beinhalten, damit das Wägesystem einschließlich seiner Software durch eine Störung nicht in einen undefinierten Zustand gerät.		
Erforderliche Dokumentation: Eine kurze Beschreibung des Backupmechanismus und der Daten, die gesichert werden, und wann dies geschieht. Angabe oder Berechnung des maximalen Fehlers, der bei kumulativen Werten auftreten kann, wenn ein zyklisches (periodisches) Backup durchgeführt wird.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • Sicherungsmöglichkeiten prüfen. <i>Funktionsprüfungen:</i> • Durch Simulierung einer Störung überprüfen, ob der Backupmechanismus so wie in der Dokumentation beschrieben funktioniert.		
Beispiel einer akzeptablen Lösung: Ein Hardware-Watchdog wird ausgelöst, wenn er nicht in regelmäßigen Abständen zurückgesetzt wird. Dieser Alarm erzeugt eine Unterbrechung im Mikroprozessor. Die zugewiesene Unterbrechungsroutine sammelt sofort Messwerte, Zustandswerte und andere relevante Daten und speichert sie in einem nichtflüchtigen Speicher, z.B. in einem EEPROM oder in einem anderen geeigneten Speicher. <u>Hinweis:</u> Es wird davon ausgegangen, dass die Watchdog-Unterbrechung höchste Unterbrechungspriorität hat und jede normale Verarbeitung oder jede beliebige Endlosschleife unterbrechen kann, d.h. die Ablaufsteuerung springt immer zur Unterbrechungsroutine, wenn der Watchdog ausgelöst wird.		

10.6.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Tabelle 10-1: Beispiele für rechtlich relevante, gerätespezifische und typenspezifische Funktionen und Daten (DF, DD, TF, TD) für selbsttätige Waagen im Vergleich zu nicht selbsttätigen Waagen (R76). VV bedeutet variable Werte ("variable values").

Funktionen/Daten	Typ	OIML-Empfehlung Nr.						
		50	51 (X)	51 (Y)	61	76	106	107
Gewichtsberechnung	TF, TD	X	X	X	X	X	X	X
Stabilitätsanalyse	TF, TD		X	X	X	X	X	X
Preisberechnung	TF, TD			X		X		
Rundungsalgorithmus für Preise	TF, TD			X		X		
Spanne (Empfindlichkeit)	DD	X	X	X	X	X	X	X
Korrekturen für Nicht-Linearität	DD (TD)	X	X	X	X	X	X	X
Max, Min, e, d	DD (TD)	X	X	X	X	X	X	X
Maßeinheiten (z. B. g, kg)	DD (TD)	X	X	X	X	X	X	X
Gewichtswert wie angezeigt (gerundet auf Vielfache von e oder d)	VV	X		X		X	X	X
Tara, Taraeingabe	VV		X	X	X	X	X	
Stückpreis, Kaufpreis	VV			X		X		X
Gewichtswert in interner Auflösung	VV	X	X	X	X	X	X	X
Statusanzeigen (z. B. Nullanzeige, Anzeige des stabilen Gleichgewichts)	TF	X	X	X	X	X	X	X
Vergleich des tatsächlichen Gewichts mit dem vorgegebenen Wert	TF		X		X			
Automatische Druckfreigabe, z. B. bei Unterbrechung des automatischen Betriebs	TF	X						X
Einlaufzeit	TF (TD)	X	X	X	X	X	X	X
Umschaltsperrung zwischen Funktionen z.B. Nulleinstellung/Tara	TF		X	X				
Betrieb automat./nicht automat.			X	X	X	X		
Nullstellung/Totalisieren		X					X	
Log für Änderung der dynamischen Justierung	TF (VV)		X	X				X
Maximaler Durchsatz/Geschwindigkeitsbereich (dynamisches Wiegen)	DD (TD)	X	X	X	X		X	X
(Produktspezifische) Parameter für die dynamische Gewichtsberechnung	VV		X	X			X	
Voreingestellter Gewichtswert	VV		X		X			
Breite des Einstellbereichs	DD (TD)		X	X				
Kriterium für automat. Nullstellung (z.B. Zeitintervall, Ende des Wägezyklus)	DD (TD)		X	X	X		X	X
Minimale Entnahmemenge, minimale Nennfüllung	DD				X			X
Grenzwert für Annahme einer bedeutenden Störung (wenn nicht 1e oder 1d)	DD (TD)	X			X			
Grenzwert für die Batterieleistung	DD (TD)	X	X	X	X	X	X	X

Tabelle 10-1: Beispiele für rechtlich relevante, gerätespezifische und typenspezifische Funktionen und Daten

Bei den angegebenen Funktionen und Parametern besteht die Wahrscheinlichkeit, dass sie bei den verschiedenen Waagentypen vorkommen. Wenn eine dieser Funktionen bzw. einer dieser Parameter vorkommt, müssen sie als "rechtlich relevant" behandelt werden. Die Tabelle ist jedoch nicht als obligatorische Liste zu verstehen, die anzeigt, dass jede der erwähnten Funktionen bzw. jeder der erwähnten Parameter in jeder Waage umzusetzen ist.

10.6.5 Weitere Aspekte

Keine

10.6.6 Einstufung in Risikoklassen

Gemäß Beschluss der zuständigen WELMEC-Arbeitsgruppe (24. Sitzung der Arbeitsgruppe WG2, 22./23. Januar 2004) ist derzeit **allgemein die Risikoklasse "B"** auf alle Kategorien der "Selbsttätigen Waagen" **anzuwenden**, unabhängig von ihrem Typ (P oder U).

Als Ergebnis des WG7-Fragebogens (2004) scheint die folgende Unterscheidung zwischen Geräten vom Typ P und U und zwischen diskontinuierlichen und kontinuierlichen Totalisatoren angemessen:

- **Risikoklasse B für Messgeräte vom Typ P (mit Ausnahme von "Selbsttätigen Waagen zum Totalisieren")**
- **Risikoklasse C für Messgeräte vom Typ U und für "Selbsttätige Waagen zum Totalisieren" der Typen P und U**

10.7 Taxameter

Taxameter unterliegen den Vorschriften der MID. Die spezifischen Anforderungen sind in Anhang MI-007 enthalten. Diese spezifischen Anforderungen, das normative Dokument OIML R 21 (2007) und WELMEC CT-007 (siehe Tabelle) wurden berücksichtigt.

10.7.1 Spezifische Vorschriften, Normen und normative Dokumente

Die OIML-Empfehlung R 21 zu Taxametern ist ein normatives Dokument im Sinne der MID. WELMEC CT-007 zu Taxametern zeigt den Zusammenhang zwischen den grundlegenden Anforderungen der MID und OIML R 21. WELMEC 12.1 gibt spezifische Interpretationen der MID und der jeweiligen Abschnitte der OIML R 21.

10.7.2 Technische Beschreibung

Gemäß Definition der MID misst ein Taxameter die Zeit und Entfernung (unter Verwendung eines Wegstreckensignalgebers, der nicht durch die MID abgedeckt ist) und berechnet den Fahrpreis für eine Fahrt gemäß den gültigen Tarifen.

Taxameter können eine eingebettete Architektur verwenden, d.h. Messgeräte mit zweckgebundener Hard- und Software (Typ P) im Sinne dieses Leitfadens oder eine Architektur, die mehrere Computer nutzt (Typ U).

10.7.3 Spezielle Softwareanforderungen

MID Anhang IX, 4:

Ein Taxameter muss über eine (oder mehrere) geeignete gesicherte Schnittstelle(n) folgende Daten übertragen können:

- Betriebseinstellung: "Frei", "Besetzt" oder "Kasse";
- Zählwerksdaten gemäß Nummer 15.1;
- allgemeine Daten: Konstante des Wegstreckensignalgebers, Datum der Sicherung, Taxikennung, Echtzeit, Tarifkennung;
- Preisdaten einer Fahrt: in Rechnung gestellte Gesamtsumme, Fahrpreis, Berechnung des Fahrpreises, Zuschlag, Datum, Fahrtbeginn, Fahrtende, zurückgelegte Strecke;
- Tarifdaten: Parameter des bzw. der Tarife.

Aufgrund nationaler Rechtsvorschriften besteht möglicherweise die Pflicht, bestimmte Geräte an die Schnittstelle(n) eines Taxameters anzuschließen. In diesem Fall muss es möglich sein, mittels einer Sicherheitseinstellung den Betrieb des Taxameters automatisch zu verhindern, wenn das erforderliche Gerät nicht vorhanden ist oder nicht vorschriftsmäßig funktioniert.

MID Anhang IX, 9:

Im Falle einer Verringerung der Spannungszufuhr auf einen Wert unterhalb der vom Hersteller festgelegten unteren Betriebsgrenze muss das Taxameter:

- korrekt weiterarbeiten oder die korrekte Arbeitsweise ohne Verlust von Daten, die vor dem Spannungsabfall verfügbar waren wiederaufnehmen, wenn der Spannungsabfall vorübergehender Art ist, z.B. bei Neustart des Motors
- eine vorhandene Messung abbrechen und zur Position "Frei" zurückkehren, wenn der Spannungsabfall über einen längeren Zeitraum andauert.

MID Anhang IX, 15.2:

Wenn das Taxameter von der Stromversorgung getrennt wird, muss die Möglichkeit bestehen, die darin aufsummierten Werte ein Jahr lang zu speichern, damit sie in ein anderes Medium ausgelesen werden können.

MID Anhang IX, 19:

Ein Taxameter ist so auszulegen und die Herstelleranweisungen für den Einbau sind so zu gestalten, dass bei Einbau nach den Herstelleranweisungen betrügerische Veränderungen des Messsignals für die zurückgelegte Wegstrecke hinreichend ausgeschlossen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
----------------	----------------	----------------

I7-1: Backup-Einrichtungen

Es muss eine Einrichtung vorhanden sein, die automatisch für wesentliche Daten (wie z.B. Messwerte oder den aktuellen Prozessstatus) ein Backup erzeugt, wenn die Spannung für längere Zeit abfällt.

Detaillierende Anmerkungen:

- 1) Diese Daten sollten normalerweise in einem nichtflüchtigen Speicher gespeichert werden.
- 2) Ein Spannungsdetektor ist notwendig, um zu erkennen, wann Messwerte gespeichert werden müssen.
- 3) Die Backup-Einrichtungen müssen geeignete Weckfunktionen haben, damit das Taxameter einschließlich seiner Software nicht in einen undefinierten Zustand gerät.

Erforderliche Dokumentation:

Eine kurze Beschreibung, welche Daten gesichert werden und wann dies geschieht.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu überprüfen:

- ob im Falle einer Störung alle rechtlich relevanten Daten gerettet sind.

Funktionsprüfungen:

- Funktionsprüfungen bei Vorhandensein definierter Störgrößen und provozierter Fehler.

Beispiel einer akzeptablen Lösung:

Der Spannungspegeldetektor löst eine Unterbrechung aus, wenn die Spannung für die Dauer von 15 s abfällt. Die zugehörige Unterbrechungsroutine sammelt Messwerte, Statuswerte und andere relevante Daten und speichert sie in einem nichtflüchtigen Speicher, z.B. EEPROM. Wenn der Spannungspegel wieder steigt, werden die Daten wiederhergestellt und die Funktion läuft weiter oder wird gestoppt (siehe MI-007, 9.)

Hinweis: Es wird davon ausgegangen, dass die Spannungsunterbrechung eine hohe Unterbrechungspriorität hat und jede normale Verarbeitung oder jede beliebige Endlosschleife unterbrechen kann, d.h. die Programmsteuerung springt immer zu der Unterbrechungsroutine, wenn die Spannung abfällt.

Risikoklasse B	Risikoklasse C	Risikoklasse D
7-2: Langzeitdatenspeicher <i>Es muss eine Einrichtung vorhanden sein, die die aufsummierten Werte speichert, wenn sie von der Stromversorgung getrennt wird.</i>		
Detaillierende Anmerkungen: 1) Diese aufsummierten Werte sollten normalerweise in einem nichtflüchtigen Speicher gespeichert werden. 2) Die Einrichtung soll die aufsummierten Werte kontinuierlich oder mit einer Update-Rate speichern, welche die Zeit abdeckt, die benötigt wird, um einen Leistungsabfall zu entdecken, bis die (innere) Spannung unter die Betriebsspannung fällt.		
Erforderliche Dokumentation: Eine kurze Beschreibung, welche Daten gespeichert werden und wann dies geschieht.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob alle aufsummierten Werte im Falle der Trennung von der Stromversorgung gespeichert sind. <i>Funktionsprüfungen:</i> • Bestätigen der korrekten Funktion bei Vorhandensein definierter Störgrößen und provozierte Fehler.		
Beispiel einer akzeptablen Lösung: Der Spannungspegeldetektor löst eine Unterbrechung aus, wenn der Spannungspegel abfällt. Die zugehörige Unterbrechungsroutine sammelt die aufsummierten Werte und speichert sie in einem Permanentenspeicher, bevor die (innere) Spannung unter die Betriebsspannungspegel fällt. Oder diese totalisierten Daten werden kontinuierlich in einem Permanentenspeicher gespeichert. <i>Hinweis:</i> Es wird davon ausgegangen, dass die Spannungsunterbrechung eine hohe Unterbrechungspriorität hat und jede normale Verarbeitung oder jede beliebige Endlosschleife unterbrechen kann, d.h. die Programmsteuerung springt immer zu der Unterbrechungsroutine, wenn die Spannung abfällt.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I7-3: Betrügerische Verwendung <i>Es muss eine Einrichtung vorhanden sein, die die Plausibilität des Abstandsmesssignals prüft.</i>		
Detaillierende Anmerkungen: 1) Die Einrichtung muss geeignete Routinen zur Prüfung umfassen, ob die empfangenen Impulse oder Informationen plausibel sind.		
Erforderliche Dokumentation: Eine kurze Beschreibung, wie die Routinen die Plausibilität prüfen.		
Validierungsanleitung: <i>Auf Basis der Dokumentation ist zu überprüfen:</i> • ob die Routinen die Plausibilität prüfen. <i>Funktionsprüfungen:</i> • Bestätigen der korrekten Funktion bei Vorhandensein provozierte Fehler.		
Beispiel einer akzeptablen Lösung: Der Ausgang des Wegstreckensignalgebers wird kontinuierlich auf seine festgelegten Eigenschaften hinsichtlich Spannungspegel, Impulsbreite und Zusammenhang zwischen Geschwindigkeit und Frequenz (Stabilität des Signals) geprüft. <i>Hinweis:</i> der Ausgang könnte digitale Informationen enthalten, zum Beispiel vom CAN-Bus des Fahrzeugs.		

10.7.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Zusätzlich zu den unter 10.7.2 genannten Funktionen, können die folgenden typischen Parameter von Taxametern betrachtet werden.

Parameter	Geschützt	Einstellbar	Anmerkung
Taxameter-Konstante k	x		Impulse pro km
Datum/Uhrzeit	x	x	-
Tarife (einschließlich der Parameter für automatische Tarifwechsel)	x	x	Währungseinheit/km, Währungseinheit/h
länder-/regionenspezifisch	x	x	Währungseinheit, Berechnungsmodus S / D, Wortlaut/Sprache, usw.
Schnittstellenparameter		x	Baud-Rate usw.

Die Tarife müssen mindestens separat gesichert werden.

Die folgenden Daten können ebenfalls berücksichtigt werden:

Daten	Anmerkung
Schnittstellenparameter	Baud-Rate usw.
Anhang IX, 4:	
Betriebseinstellung	"Frei", "Besetzt" oder "Kasse";
Zählwerksdaten:	gemäß Punkt 15.1, (Währungseinheit, km, h)
Allgemeine Information:	Konstante des Wegstreckensignalgebers (Impulse/km) Sicherungsdatum, (ddmmyyyy) Taxikennung, (Kfz-Kennzeichnung) Echtzeit, (hh:mm) Identifikation des Tarifs (Prüfsumme)
Preisdaten einer Fahrt:	in Rechnung gestellte Gesamtsumme (Währungseinheit) Fahrpreis (Währungseinheit) die Berechnung des Fahrpreises, (Währungseinheit, km, h) Zuschlag, (Währungseinheit) Datum, (ddmmyyyy) Fahrtbeginn, (hh:mm) Fahrtende, (hh:mm) Zurückgelegte Wegstrecke (km)
Tarifinformation:	Parameter des bzw. der Tarife, (Währungseinheit/km, Währungseinheit/h)

10.7.5 Weitere Aspekte

Es wird empfohlen, die Kfz-Richtlinie zu überarbeiten oder eine sonstige Verordnung mit Anforderungen an die Wegstreckensignalgeber für als Taxi genutzte Fahrzeuge zu erstellen. Ein vorläufiger Vorschlag lautet:

Für Fahrzeuge, die als Taxi genutzt werden sollen, gelten die folgenden Anforderungen:

1. Der Wegstreckensignalgeber gibt ein Signal mit einer Auflösung von mindestens 2 m.
2. Der Wegstreckensignalgeber gibt bei jeder Geschwindigkeit ein stabiles Signal.
3. Der Wegstreckensignalgeber besitzt festgelegte Eigenschaften hinsichtlich Spannungspegel, Impulsbreite und Zusammenhang zwischen Geschwindigkeit und Frequenz.
4. Prüfbarkeit...

10.7.6 Einstufung in Risikoklassen

Gemäß dem Ergebnis der WELMEC-WG7-Befragung (2004) und nach Bestätigung der Taxameter der verantwortlichen WELMEC-Arbeitsgruppe 12 muss die folgende Risikoklasse angewandt werden, wenn Softwareprüfungen auf der Grundlage des vorliegenden Leitfadens für (softwaregesteuerte) Taxameter durchgeführt werden:

- **Risikoklasse C für Geräte vom Typ P**
- **Risikoklasse D für Geräte vom Typ U**

10.8 Maßverkörperungen

Maßverkörperungen unterliegen den Regelungen der MID. Die besonderen Anforderungen sind in Anhang MI-008 enthalten.

Abhängig von künftigen Entwicklungen und Entscheidungen werden Maßverkörperungen im Sinne der MID Anhang MI-008 nicht als softwaregesteuerte Messinstrumente betrachtet. Daher gilt der vorliegende Software-Leitfaden derzeit nicht für Maßverkörperungen.

10.9 Längenmessgeräte

Längenmessgeräte unterliegen den Regelungen der MID. Die spezifischen Anforderungen sind in Anhang MI-009 enthalten. Bisher sind weder diese spezifischen Anforderungen noch irgendwelche normativen Dokumente berücksichtigt worden.

10.9.1 - 10.9.5 werden eingetragen, wenn dies in Zukunft für notwendig erachtet wird.

10.9.6 Einstufung in Risikoklassen

Gemäß dem Ergebnis der WELMEC-WG7-Befragung (2004) und unter der Prämisse zukünftiger Entscheidungen der verantwortlichen WELMEC-Arbeitsgruppe sollte die folgende Risikoklasse angewandt werden, wenn Softwareprüfungen auf der Grundlage des vorliegenden Leitfadens für (softwaregesteuerte) Längenmessgeräte durchgeführt werden:

- **Risikoklasse B für Messgeräte vom Typ P**
- **Risikoklasse C für Messgeräte vom Typ U**

10.10 Abgasanalysatoren

Abgasanalysatoren unterliegen den Vorschriften der MID. Die spezifischen Anforderungen sind in Anhang MI-010 enthalten. Bisher sind weder diese spezifischen Anforderungen noch irgendwelche normativen Dokumente berücksichtigt worden.

10.10.1 - 10.10.5 werden eingetragen, wenn dies in Zukunft für notwendig erachtet wird.

10.10.6 Einstufung in Risikoklassen

Gemäß dem Ergebnis der WELMEC-WG7-Befragung (2004) und unter der Prämisse zukünftiger Entscheidungen der verantwortlichen WELMEC-Arbeitsgruppe sollte die folgende Risikoklasse angewandt werden, wenn Softwareprüfungen auf der Grundlage des vorliegenden Leitfadens für (softwaregesteuerte) Abgasanalysatoren durchgeführt werden:

- **Risikoklasse B für Messgeräte vom Typ P**
- **Risikoklasse C für Messgeräte vom Typ U**

11 Muster eines Prüfberichts (einschließlich Checklisten)

Es handelt sich um ein Muster für einen Prüfbericht, der aus einem Hauptteil und zwei Anhängen besteht. Der Hauptteil enthält allgemeine Aussagen zum Prüfgegenstand. Dieser Teil muss der Praxis entsprechend angepasst werden. Anhang 1 besteht aus zwei Checklisten zur Auswahlunterstützung für die geeigneten Teile des Leitfadens, die anzuwenden sind. Anhang 2 besteht aus speziellen Checklisten für die entsprechenden technischen Teile des Leitfadens. Sie werden Herstellern und Prüfern als Nachweishilfe dafür empfohlen, dass sie alle anwendbaren Anforderungen berücksichtigt haben.

Zusätzlich zum Muster für den Prüfbericht und die Checklisten sind die für den Baumusterprüfschein benötigten Informationen im letzten Unterkapitel dieses Kapitels aufgelistet.

11.1 In die Baumusterprüfbescheinigung einzubeziehende Informationen

Während der Prüfbericht insgesamt eine Dokumentation des Prüfgegenstands, der durchgeführten Validierung und der Ergebnisse ist, wird für das Zertifikat nur eine bestimmte Auswahl der Informationen aus dem Prüfbericht benötigt. Dies betrifft folgende Informationen, die in die Baumusterprüfbescheinigung bezüglich der Software angemessen einbezogen werden sollten:

1. Softwaretyp

- Angabe der Ausgabe des WELMEC-Leitfadens 7.2, Typ (P oder U), der Risikoklasse (A bis E) und der entsprechenden Anhänge (L, T, S, D, Ix)

Risikoklasse [A-E] _	P ☐	U ☐	L ☐	T ☐	S ☐	D ☐	Ix ☐ [1-6] _
----------------------	-------------------------------	-------------------------------	-------------------------------	-------------------------------	-------------------------------	-------------------------------	--

Abbildung 11-1: Anzeige des gewählten Typs, der Risikoklasse sowie der entsprechenden Anhänge

2. Softwareidentifikation

- Anzeige des bzw. der Software-Identifikator(s)(en) der rechtlich relevanten Software.
- Beschreibung, wie der Software-Identifikator bzw. die Software-Identifikatoren der rechtlich relevanten Software zu prüfen sind.

3. Software-Integritätsprüfung

- Bei den Risikoklassen C und weiteren, Angabe der Prüfsumme oder alternativen Methode mit derselben Anforderungsstufe.
- Bei den Risikoklassen C und weiteren, genaue Angabe, wie die Prüfsumme oder alternative Methode mit derselben Anforderungsstufe zu prüfen ist.
- Hinweis: Verweis auf ein Dokument (z.B. Benutzerhandbuch) ist ungeeignet.

- Beschreibung, wie die Ereigniszähler / Ereignislogbücher gegebenenfalls zu prüfen sind.
- Beschreibung der Hardwareversiegelung(en) und ggf. anderer Versiegelungstypen hinsichtlich der Software.
- Gegebenenfalls andere Mittel zum Schutz der Integrität.

4. Kurze Beschreibung der Softwareumgebung

- Anzeige der relevanten Information hinsichtlich:
- Software-Umgebung, die für die Betreibung der Software notwendig ist (z.B. Betriebssystem).
- Rechtlich relevante Softwaremodule (einschließlich SW-Trennung, falls implementiert).
- Hardware- und Softwareschnittstellen (z.B. Infrarot, Bluetooth, Wireless LAN...).
- Elektronische (Hardware-) Teilreferenzen und ihre Positionen im Messgerät einschließlich ihrer Sicherung, falls erforderlich.

11.2 Muster für den allgemeinen Teil des Prüfberichts

Prüfbericht Nr. XYZ122344

Durchflussmessgerät Dynaflow Model DF101

Validierung der Software

(n Anhänge)

Auftrag

Die Messgeräte-richtlinie (MID) legt die grundlegenden Anforderungen für bestimmte in der Europäischen Union verwendete Messgeräte fest. Die Software des Messgeräts wurde validiert, um die Konformität mit den grundlegenden Anforderungen der MID zu zeigen.

Die Validierung basierte auf dem Bericht WELMEC MID Software Requirements Guide WELMEC Guide 7.2, in dem die grundlegenden Anforderungen für die Software interpretiert und erklärt werden. Dieser Bericht beschreibt die Prüfung der Software, die zur Bestätigung der Übereinstimmung mit der MID notwendig ist.

Kunde

Dynaflow
P.O. Box 1120333
100 Reykjavik
Island
Ansprechpartner: Herr Bjarnur Sigfridson

Prüfgegenstand

Das Durchflussmessgerät Dynaflow DF100 ist ein Messgerät für die Messung des Durchflusses in Flüssigkeiten. Der vorgesehene Bereich reicht von 1 l/s bis zu 2000 l/s. Zu den Grundfunktionen des Geräts gehören:

- die Messung des Durchflusses in Flüssigkeiten
- die Anzeige der gemessenen Menge
- die Schnittstelle zum Messumformer

Gemäß WELMEC-Leitfaden 7.2 wird das Durchflussmessgerät wie folgt beschrieben:

- ein Messgerät mit zweckgebundener Hard- und Software (ein eingebettetes System)
- Langzeitspeicherung von Messdaten

Das Durchflussmessgerät DF100 ist ein unabhängiges Gerät mit einem angeschlossenen Messumformer. Der Messumformer ist am Gerät befestigt und kann nicht entfernt werden. Die gemessene Menge wird auf einem Display angezeigt. Eine Verbindung zu anderen Geräten ist nicht möglich.

Die eingebettete Software des Messgeräts wurde entwickelt von

Dynaflow, P.O. Box 1120333, 100 Reykjavik, Island.

Die Version der überprüften Software lautet **V1.2c**. Der Quellcode umfasst die nachstehenden Dateien:

main.c	12301 byte	23 Nov 2003
int.c	6509 byte	23 Nov 2003
filter.c	10897 byte	20 Oct 2003
input.c	2004 byte	20 Oct 2003
display.c	32000 byte	23 Nov 2003
Ethernet.c	23455 byte	15 June 2002
driver.c	11670 byte	15 June 2002
calculate.c	6788 byte	23 Nov 2003

Die Validierung stützte sich auf die folgenden Dokumente des Herstellers:

- Benutzerhandbuch DF 100
- Wartungshandbuch DF 100
- Softwarebeschreibung DF100 (Internes Entwicklungsdokument vom 22. Nov 2003)
- Stromlaufplan DF100 (Zeichnung Nr. 222-31 vom 15. Oktober 2003)

Die endgültige Version des Prüfgegenstands wurde am 25. November 2003 an das National Testing & Measurement Laboratory geliefert.

Ablauf der Prüfung

Die Validierung wurde gemäß WELMEC 7.2 Softwareleitfaden 2015, Ausgabe 6 durchgeführt (Download von www.welmec.org).

Die Validierung wurde zwischen dem 1. November und dem 23. Dezember 2003 durchgeführt. Eine Entwurfsdurchsicht wurde am 3. Dezember von Dr. K. Fehler am Hauptsitz von Dynaflo in Reykjavik abgehalten. Weitere Validierungsarbeiten wurden am National Testing & Measurement Lab von Dr. K. Fehler und M. S. Problème durchgeführt.

Die nachstehenden Anforderungen wurden validiert:

- Besondere Anforderungen an eingebettete Software für ein Messgerät mit zweckgebundener Hard- und Software (Typ P)
- Anhang L: Langzeitspeicherung von Messdaten

Eine Checkliste für die vorliegende Konfiguration ist in Anlage 1 dieses Berichts enthalten.

Für dieses Gerät wurde die Risikoklasse C angewandt.

Folgende Validierungsmethoden wurden angewandt:

- Vollständigkeit der Dokumentation
- Prüfung des Betriebshandbuchs
- Funktionstest
- Durchsicht des Softwareentwurfs
- Durchsicht der Softwaredokumentation
- Datenflussanalyse
- Simulation von Eingangssignalen

Ergebnis

Die folgenden Anforderungen des WELMEC Softwareleitfadens 7.2 wurde validiert, ohne dass Fehler gefunden wurden:

- P1, P2, P3, P5, P6, P7, P8
(Anforderung P4 gilt als nicht anwendbar.)

- L1, L2, L3, L4, L5, L6, L7, L8

Checklisten für die P-Anforderungen sind in Anhang 2.1 dieses Berichts enthalten.

Checklisten für die L-Anforderungen sind in Anhang 2.2 dieses Berichts enthalten.

Zwei Befehle wurden gefunden, die anfangs nicht im Bedienerhandbuch beschrieben worden waren. Die beiden Befehle wurden in das Bedienerhandbuch vom 10. Dezember 2003 aufgenommen.

Ein Softwarefehler, bei dem der Monat Februar auch in einem Schaltjahr nur 28 Tage hatte, tauchte im Softwarepaket V1.2b auf. Dies wurde in V1.2c korrigiert.

Die Software des Dynaflo DF100 V1.2c erfüllt die wesentlichen Anforderungen der Messgeräte-richtlinie.

Das Ergebnis bezieht sich nur auf die geprüfte Einheit.

National Testing & Measurement Lab
Software-Abteilung

Dr. K.E.I.N. Fehler
Technical Manager

M. S.A.N.S Problème
Technical Officer

Datum: 23. Dezember 2003

11.3 Anhang 1 des Prüfberichts: Checklisten zur Unterstützung der Wahl der geeigneten Anforderungssätze

Die erste Kontrollliste unterstützt den Nutzer bei der Entscheidung, welche der Grundkonfiguration P oder U für das zu prüfende Gerät anwendbar ist.

Entscheidung zum Gerätetyp			
		(P)	Anmerkungen
1	Wurde die gesamte Anwendersoftware für den Messzweck konzipiert?	(Y)	
2	Sind die Anforderungen für die Aufnahme eines Betriebssystems oder dazugehörigen Subsystems erfüllt?	(Y)	
3	Wird dem Nutzer der Zugang zum Betriebssystem verweigert, wenn es möglich ist, auf eine rechtlich nicht relevante Betriebsart umzuschalten?	(Y)	
4	Sind die implementierten Programme und die Softwareumgebung unveränderlich (mit Ausnahme von Updates)?	(Y)	
5	Gibt es Mittel für die Programmierung?	(N)	
Zutreffendes bitte ankreuzen			

Nur wenn alle Antworten auf die 5 Fragen wie in der (P-)Spalte gegeben werden können, treffen die Anforderungen von Teil P (Kapitel 4) zu. In allen anderen Fällen treffen notwendigerweise die Anforderungen von Teil U (Kapitel 5) zu.

Die zweite Checkliste unterstützt die Entscheidung, welche IT-Konfiguration auf das zu prüfende Gerät zutrifft.

Entscheidung zu notwendigen Ergänzungen					
Notwendiger Anhang		JA	NEIN	Entfällt	Anmerkungen
L	Ist das Gerät in der Lage, die Messdaten entweder in einen integrierten Speicher oder auf einem Fern- oder Wechselspeicher zu speichern?				
T	Werden Messdaten über Kommunikationsnetze zu einem entfernten Gerät übertragen werden, wo sie für rechtlich relevante Zwecke weiter verarbeitet und/oder verwendet werden.				
S	Gibt es Softwareteile mit Funktionen, die nicht der gesetzlichen Kontrolle unterliegen UND sollen diese Softwareteile nach der Bauartzulassung geändert werden können?				
D	Ist nach Inbetriebnahme des Messgerätes ein Laden von Software möglich oder erwünscht?				
Beachten Sie den notwendigen Anhang für jede mit JA beantwortete Frage!					

11.4 Anhang 2 des Prüfberichts: Spezielle Checklisten für die entsprechenden technischen Teile

1) Checkliste für die Grundanforderungen an ein Gerät vom Typ P

Checkliste für Anforderungen vom Typ P						
Anforderung	Prüfverfahren		Bestanden	Durchgefallen	Entfällt	Anmerkungen*
P1		Erfüllt die erforderliche Herstellerdokumentation die Anforderung P1(a-f)?				
P2		Wird die Softwareidentifikation wie in P2 gefordert umgesetzt?				
P3		Wird bei der Befehlseingabe über die Benutzerschnittstelle die unzulässige Beeinflussung der rechtlich relevanten Software und Messdaten verhindert?				
P4		Beeinflussen die über Kommunikationsschnittstellen des Geräts eingegebenen Befehle die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten nicht unzulässig?				
P5		Sind die rechtlich relevante Software und Messdaten vor zufälligen oder unbeabsichtigten Änderungen geschützt?				
P6		Ist die rechtlich relevante Software gegen unzulässige absichtliche Veränderungen, unzulässiges Laden oder Austauschen des Hardwarespeichers gesichert?				
P7		Sind die rechtlich relevanten Parameter gegen unzulässige Veränderungen gesichert?				
P8		Ist die Authentizität der dargestellten Messdaten gesichert?				

* Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.

2) Checkliste für die Grundanforderungen für ein Gerät vom Typ U

Checkliste für Anforderungen vom Typ U						
Anforderung	Prüfverfahren		Bestanden	Durchgefallen	Entfällt	Anmerkungen*
U1		Erfüllt die geforderte Herstellerdokumentation die Anforderung U1(a-g)?				
U2		Wird die Softwareidentifikation wie in U2 gefordert umgesetzt?				
U3		Wird bei der Befehlseingabe über die Benutzerschnittstelle die unzulässige Beeinflussung der rechtlich relevanten Software und Messdaten verhindert?				
U4		Wird bei der Befehlseingabe über Kommunikationsschnittstellen des Gerätes die unzulässige Beeinflussung der rechtlich relevanten Software, gerätespezifischen Parameter und Messdaten verhindert?				
U5		Sind die rechtlich relevante Software und Messdaten vor zufälligen oder unbeabsichtigten Änderungen geschützt?				
U6		Sind die rechtlich relevante Software und Messdaten vor unzulässigen absichtlichen Veränderungen oder Austausch geschützt?				
U7		Sind die rechtlich relevanten Parameter gegen unzulässige Veränderungen gesichert?				
U8		Ist die Authentizität der dargestellten Messdaten gesichert?				
U9		Ist die rechtlich relevante Software so aufgebaut, dass sie von keiner anderen Software unzulässig beeinflusst werden kann?				

** Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.*

3) Checkliste für besondere Anforderungen aus Anhang L

Checkliste für Anforderungen von Anhang L						
Anforderung	Prüfverfahren		Bestanden	Durchgefallen	Entfällt	Anmerkungen*
L1		Enthalten die gespeicherten Messdaten alle Informationen, die für rechtlich relevante Zwecke erforderlich sind?				
L2		Sind die gespeicherten Daten vor zufälligen und unbeabsichtigten Änderungen geschützt?				
L3		Sind die gespeicherten Daten vor vorsätzlichen Änderungen geschützt?				
L4		Sind die gespeicherten Messdaten auf die Messung rückführbar, bei der sie erzeugt wurden?				
L5		Werden die Schlüssel und zugehörige Informationen als rechtlich relevante Daten behandelt und geheim gehalten sowie vor Kompromittierung geschützt?				
L6		Ist rechtlich relevante Software für die Anzeige oder den Ausdruck gespeicherter Messdaten vorhanden?				
L7		Werden die Messdaten automatisch gespeichert, wenn die Messung abgeschlossen ist?				
L8		Verfügt der Langzeitspeicher über eine für den beabsichtigten Zweck ausreichende Kapazität?				

* Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.

4) Checkliste für besondere Anforderungen aus Anhang T

Checkliste für Anforderungen aus Anhang T						
Anforderung	Prüfverfahren		Bestanden	Durchgefallen	Entfällt	Anmerkungen*
T1		Enthalten die übertragenen Daten alle relevanten Informationen, die in der Empfangseinheit für die Anzeige oder Weiterverarbeitung des Messergebnisses notwendig sind?				
T2		Sind die übertragenen Daten vor zufälligen und unbeabsichtigten Änderungen geschützt?				
T3		Sind die übertragenen rechtlich relevanten Daten vor vorsätzlicher Änderung geschützt?				
T4		Sind die übertragenen Messdaten auf die Messung und das Messgerät rückführbar, die die Daten erzeugt haben?				
T5		Werden die Schlüssel und zugehörigen Informationen als Messdaten behandelt und geheim gehalten sowie vor Kompromittierung geschützt?				
T6		Ist rechtlich relevante Software für die Ablesung, Verifizierung und Bearbeitung gespeicherter Messdaten vorhanden?				
T7		Ist sichergestellt, dass die Messung durch eine Übertragungsverzögerung nicht unzulässig beeinflusst wird?				
T8		Ist sichergestellt, dass keine Messdaten verloren gehen, wenn Netzwerkdienste nicht mehr verfügbar sind?				

* Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.

5) Checkliste für besondere Anforderungen aus Anhang S

Checkliste für Anforderungen aus Anhang S						
Anforderung	Prüfverfahren		Bestanden	Durchgefallen	Entfällt	Anmerkungen*
S1		Gibt es einen Softwareteil, der sämtliche rechtlich relevante Software und Parameter enthält und eindeutig von anderen Softwareteilen getrennt ist.				
S2		Ist sichergestellt, dass Informationen, die von der rechtlich nicht relevanten Software auf einem Display oder einem Ausdruck angezeigt werden, nicht mit den Informationen verwechselt werden können, die von der rechtlich relevanten Software stammen?				
S3		Erfolgt der Datenaustausch zwischen der rechtlich relevanten und der rechtlich nicht relevanten Software über eine geschützte Softwareschnittstelle?				

* Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.

6 Checkliste für besondere Anforderungen aus Anhang D

Checkliste für Anforderungen aus Anhang D						
Anforderung	Prüfverfahren		Bestanden	Durchgefallen	Entfällt	Anmerkung n*
D1		Erfolgen beide Phasen des Softwaredownloads, die Übertragung und die nachfolgende Installation der Software automatisch und beeinträchtigen sie den Schutz der rechtlich relevanten Software nicht?				
D2		Werden Mittel eingesetzt, die garantieren, dass die heruntergeladene Software authentisch ist,				
D3		Werden Mittel eingesetzt, die garantieren, dass die heruntergeladene Software während des Downloads nicht unzulässig verändert wurde?				
D4		Wird mittels geeigneter technischer Hilfsmittel garantiert, dass Downloads von rechtlich relevanter Software innerhalb des Geräts für spätere Kontrollen geeignet rückverfolgbar sind?				
* Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.						

12 Querverweise zwischen den MID-Softwareanforderungen und MID-Artikeln bzw. -Anhängen

(in Bezug auf MID-Version: Richtlinie 2014/32/EG, 26. Februar 2014)

12.1 Softwareanforderungen und ihr Bezug zur MID

Anforderung		MID	
Nein	Bezeichnung	Artikel / Anhang Nr. (AI = Anhang I)	Bezeichnung
	Basis-Typ P		
P1	Herstellerdokumentation	AI-9.3 AI-12 Artikel 18	Informationen, die auf dem Gerät angegeben oder mit ihm zusammen geliefert werden Konformitätsbewertung Technische Unterlagen
P2	Softwareidentifikation	AI-7.6 AI-8.3	Eignung Schutz vor Verfälschung
P3	Beeinflussung über Nutzerschnittstelle	AI-7.1	Eignung
P4	Beeinflussung über Kommunikationsschnittstelle	AI-7.1 AI-8.1	Eignung Schutz vor Verfälschung
P5	Schutz vor zufälligen oder unbeabsichtigten Änderungen	AI-7.1, AI-7.2 AI-8.4	Eignung Schutz vor Verfälschung
P6	Schutz vor beabsichtigten Änderungen	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Eignung ¹⁴ Schutz vor Verfälschung
P7	Parameterschutz	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Eignung Schutz vor Verfälschung
P8	Softwareauthentizität und Anzeige der Ergebnisse	AI-7.1, AI-7.2, AI-7.6 AI-8.3 AI-10.2, AI-10.3, AI-10.4	Eignung Schutz vor Verfälschung Anzeige des Ergebnisses
	Basis-Typ U		
U1	Herstellerdokumentation	AI-9.3 AI-12 Artikel 18	Informationen, die auf dem Gerät angegeben oder mit ihm zusammen geliefert werden Konformitätsbewertung Technische Unterlagen
U2	Softwareidentifikation	AI-7.6 AI-8.3	Eignung Schutz vor Verfälschung
U3	Beeinflussung über Nutzerschnittstellen	AI-7.1	Eignung
U4	Beeinflussung über Kommunikationsschnittstelle	AI-7.1 AI-8.1	Eignung Schutz vor Verfälschung
U5	Schutz vor zufälligen oder unbeabsichtigten Änderungen	AI-7.1, AI-7.2 AI-8.4	Eignung Schutz vor Verfälschung
U6	Schutz vor beabsichtigten Änderungen	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Eignung Schutz vor Verfälschung
U7	Parameterschutz	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Eignung Schutz vor Verfälschung
U8	Softwareauthentizität und Anzeige der Ergebnisse	AI-7.1, AI-7.2, AI-7.6 AI-8.3 AI-10.2, AI-10.3, AI-10.4	Eignung Schutz vor Verfälschung Anzeige des Ergebnisses
U9	Beeinflussung der übrigen Software	AI-7.6	Eignung
	Anhang L		
L1	Vollständigkeit der gespeicherten Daten	AI-7.1 AI-8.4 AI-10.2	Eignung Schutz vor Verfälschung Anzeige des Ergebnisses

¹⁴ Anmerkung: Was den Inhalt betrifft, so handelt es sich bei Absatz 7.1 des MID-Anhangs I nicht um "Eignung", sondern um "Schutz vor Verfälschung" (Absatz 8)

Anforderung		MID	
Nein	Bezeichnung	Artikel / Anhang Nr. (AI = Anhang I)	Bezeichnung
L2	Schutz vor zufälligen oder unbeabsichtigten Änderungen	AI-7.1, AI-7.2 AI-8.4	Eignung Schutz vor Verfälschung
L3	Datenintegrität	AI-7.1 AI-8.4	Eignung Schutz vor Verfälschung
L4	Authentizität der gespeicherten Daten	AI-7.1 AI-8.4 AI-10.2	Eignung Schutz vor Verfälschung Anzeige des Ergebnisses
L5	Vertraulichkeit der Schlüssel	AI-7.1 AI-8.4	Eignung Schutz vor Verfälschung
L6	Abruf gespeicherter Daten	AI-7.2 AI-10.1, AI-10.2, AI-10.3, AI-10.4	Eignung Anzeige des Ergebnisses
L7	Automatische Speicherung	AI-7.1 AI-8.4	Eignung Schutz vor Verfälschung
L8	Speicherkapazität und -dauer	AI-7.1	Eignung
Lx	Gesamter Anhang L	AI-11.1	Weiterverarbeitung von Daten zum Abschluss des Geschäftsvorgangs
Anhang T			
T1	Vollständigkeit der übertragenen Daten	AI-7.1 AI-8.4	Eignung Schutz vor Verfälschung
T2	Schutz vor zufälligen Änderungen	AI-7.1, AI-7.2 AI-8.4	Eignung Schutz vor Verfälschung
T3	Datenintegrität	AI-7.1 AI-8.4	Eignung Schutz vor Verfälschung
T4	Authentizität der übertragenen Daten	AI-7.1 AI-8.4	Eignung Schutz vor Verfälschung
T5	Vertraulichkeit der Schlüssel	AI-7.1 AI-8.4	Eignung Schutz vor Verfälschung
T6	Umgang mit beschädigten Daten	AI-7.1 AI-8.4	Eignung Schutz vor Verfälschung
T7	Übertragungsverzögerung	AI-7.1 AI-8.4	Eignung Schutz vor Verfälschung
T8	Verfügbarkeit von Übertragungsdiensten	AI-7.1 AI-8.4	Eignung Schutz vor Verfälschung
Anhang S			
S1	Rückwirkungsfreie Softwareschnittstelle	AI-7.6, AI-10.1	Eignung Anzeige des Ergebnisses
S2	Gemischte Anzeige	AI-7.1, AI-7.2, AI-7.6 AI-10.2	Eignung Anzeige des Ergebnisses
S3	Schutzschnittstelle für die Software	AI-7.6	Eignung
Anhang D			
D1	Download-Mechanismus	AI-8.2, AI-8.4	Schutz vor Verfälschung
D2	Authentifizierung der heruntergeladenen Software	AI-7.6 AI-8.3, AI-8.4 AI-12	Eignung Schutz vor Verfälschung Konformitätsbewertung
D3	Integrität der heruntergeladenen Software	AI-7.1, AI-8.4	Eignung Schutz vor Verfälschung
D4	Rückverfolgbarkeit des Downloads von rechtlich relevanter Software	AI-7.1, AI-7.6 AI-8.2, AI-8.3 AI-12	Eignung Schutz vor Verfälschung Konformitätsbewertung
Anhang I (Gerätespezifische Softwareanforderungen)			

Anforderung		MID	
Nein	Bezeichnung	Artikel / Anhang Nr. (AI = Anhang I)	Bezeichnung
I1-1, I2-1, I3-1, I4-1	Fehlerbehebung	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Zuverlässigkeit Besondere Anforderungen für Verbrauchszähler
I1-2, I2-2, I3-2, I4-2	Backup-Einrichtungen	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Zuverlässigkeit Besondere Anforderungen für Verbrauchszähler
I1-4, I2-4, I3-4, I4-4	Interne Auflösung, Tauglichkeit der Anzeige	MI-002-5.3, MI-003-5.2	Besondere Anforderungen für Verbrauchszähler
I1-3, I2-4, I3-4, I4-3	Rücksetzen kumulierter Messwerte verhindern	AI-8.5	Schutz vor Verfälschung
I1-4, I2-8, I3-5, I4-4	Dynamisches Verhalten	AI-7.6	Eignung Schutz vor Verfälschung
I2-5	Lebensdauer der Batterie	MI-002-5.2	Besondere Anforderungen für Gaszähler
I2-6	Elektronische Mengenumwerter	MI-002-9.1	Besondere Anforderungen für Gaszähler
I2-7	Prüfelement	MI-002-5.5	Besondere Anforderungen für Gaszähler
I6-1	Fehlererkennung	MI-006-IV, MI-006-V	Selbsttätige Waagen zum diskontinuierlichen und zum kontinuierlichen Totalisieren
I6-2	Backup-Einrichtungen, Fehlererkennung	MI-006-IV, MI-006-V	Selbsttätige Waagen zum diskontinuierlichen und zum kontinuierlichen Totalisieren

12.2 Auslegung von MID-Artikeln und -Anhängen durch MID-Softwareanforderungen

MID			Softwareleitfa den
Artikel / Anhang Nr. (AI = Anhang I)	Bezeichnung	Anmerkung	Anforderung Nein
	Artikel-Teil		
1, 2, 3		Keine besondere Softwarerelevanz	
4(b)	Definitionen, Anordnung von Teilgeräten	Übertragung der Messdaten Grundleitfäden anwendbar auf Teilgeräte	T P, U
5 bis 9		Keine besondere Softwarerelevanz	

MID			Softwareleitfa den
Artikel / Anhang Nr. (AI = Anhang I)	Bezeichnung	Anmerkung	Anforderung Nein
10	Technische Dokumentation	Dokumentation des Entwurfs, der Herstellung und des Betriebs. Konformitätsbewertung ermöglichen. Allgemeine Beschreibung des Geräts. Beschreibung der elektronischen Geräte mit Hilfe von Zeichnungen, Flussdiagrammen der Logik, allgemeine Software-Informationen. Anbringungsstelle für Siegel und Kennzeichnungen. Bedingungen für die Kompatibilität mit Schnittstellen und Teilgeräten.	P1, U1
11 bis 27		Keine besondere Softwarerelevanz	
Anhang I			
AI-1 bis AI-5		Keine besondere Softwarerelevanz	
AI-6	Zuverlässigkeit	Fehlererkennung, Backup, Rückstellung, Neustart	I1-1, I1-2, I2-1, I2-2, I3-1, I3-2, I4-1, I4-2, I6-1, I6-2
AI-7	Eignung	Keine Merkmale zum Erleichtern betrügerischer Verwendung; minimale Möglichkeiten für unbeabsichtigte Fehlnutzung.	P3 – P8, U3 - U8, L1 – L5, L7, L8, T1 – T8, S2, D3, D4, I1-4, I2-8, I3-5, I4-4
AI-8	Schutz vor Verfälschung		
AI-8.1		Keine Beeinflussung durch den Anschluss von anderen Geräten.	P4, U4
AI-8.2		Sicherung; Nachweis von Eingriffen	P6, P7, U6, U7, D1, D4
AI-8.3		Identifikation der Software; Nachweis von Eingriffen	P2, P6, P7, P8 U2, U6, U7, U8, D2, D4
AI-8.4		Schutz von gespeicherten oder übertragenen Daten	P5 - P7, U5 - U7, L1 - L5, T1 - T8 D1 - D3
AI-8.5		Kein Rücksetzen von kumulierten Registern	I1-3, I2-4, I3-4, I4-3
AI-9	Informationen, die auf dem Gerät angegeben oder mit ihm zusammen geliefert werden		
AI-9.1		Messkapazität (restliche Einheiten nicht relevant für die Software)	L8
AI-9.2		Keine besondere Softwarerelevanz	
AI-9.3		Anweisungen für die Installation, ..., Bedingungen für Kompatibilität mit der Schnittstelle, Teilgeräten oder Messgeräten.	P1, U1

MID			Softwareleitfa den
Artikel / Anhang Nr. (AI = Anhang I)	Bezeichnung	Anmerkung	Anforderung Nein
AI-9.4 bis AI-9.8		Keine besondere Softwarerelevanz	
AI-10	Anzeige des Ergebnisses		
AI-10.1		Anzeige mittels Display oder Ausdruck.	U8, L6, S2
AI-10.2		Bedeutung des Ergebnisses, keine Verwechslung mit zusätzlichen Anzeigen.	P8, U8, L1, L4, L6, S2
AI-10.3		Abdruck oder Aufzeichnung leicht leserlich und nicht löschar.	P8, U8, L6, S2
AI-10.4		Für Direktverkäufe: Ergebnisanzeige für beide Parteien.	P8, U8, S2
AI-10.5		Für Verbrauchszähler: Display für den Kunden.	I1-3, I2-3, I3-3/4, I4-3
AI-11	Weiterverarbeitung von Daten zum Abschluss des Geschäftsvorgangs		
AI-11.1		Dauerhafte Aufzeichnung der Messergebnisse	L1 - L8
AI-11.2		Dauerhafter Nachweis des Messergebnisses und Information zur Identifikation einer Transaktion.	L1, L6
AI-12	Konformitätsbewertung	Bequeme Bewertung der Konformität mit den Anforderungen der Richtlinie.	P1, P2, U1, U2, D2, D4
	Anhänge A1 bis H1		
A1 bis H1		Keine Anforderungen an Gerätemerkmale	
	Annex MI-001		
MI-001-1 bis MI-001-6		Keine besondere Softwarerelevanz	
MI-001-7.1.1, MI-001-7.1.2	Elektromagnetische Störfestigkeit	Fehlerbehebung Backup-Einrichtungen Weckeinrichtungen und Rekonstruktion	I1-1, I1-2
MI-001-7.1.3 bis MI-001-9		Keine besondere Softwarerelevanz	
	Anhang MI-002		
MI-002-1 bis MI-002-2		Keine besondere Softwarerelevanz	
MI-002-3.1	Elektromagnetische Störfestigkeit	Fehlerbehebung Backup-Einrichtungen Weckeinrichtungen und Rekonstruktion	I2-1, I2-2
MI-002-3.1.3 bis MI-002- 5.1		Keine besondere Softwarerelevanz	
MI-002-5.2	Eignung	Annehmbare Lösung zur Überwachung der Batterie-Lebensdauer	I2-5
MI-002-5.3	Eignung	Interne Auflösung	I2-3

MID			Softwareleitfa den
Artikel / Anhang Nr. (AI = Anhang I)	Bezeichnung	Anmerkung	Anforderung Nein
MI-002-5.4 bis MI-002-8		Keine besondere Softwarerelevanz	
MI-002-5.5	Eignung	Prüfelement	I2-7
MI-002-5.6 bis MI-002-8		Keine besondere Softwarerelevanz	
MI-002-9.1	Mengenumwerter Eignung	Zulässige Lösung für die Überwachung des Gasmengenumwerterers	I2-6
MI-002-9.2 bis MI-002- 10		Keine besondere Softwarerelevanz	
	Anhang MI-003		
MI-003-1 bis MI-003-4.2		Keine besondere Softwarerelevanz	
MI-003-4.3	Zulässige Auswirkung transienter elektromagnetischer Phänomene	Fehlerbehebung Backup-Einrichtungen Weckeinrichtungen und Rekonstruktion	I3-1, I3-2
MI-003-5.1		Keine besondere Softwarerelevanz	
MI-003-5.2	Eignung	Interne Auflösung	I3-3
MI-003-5.3 bis MI-003-7		Keine besondere Softwarerelevanz	
	Anhang MI-004		
MI-004-1 bis MI-004-4.1		Keine besondere Softwarerelevanz	
MI-004-4.2	Zulässige Einflüsse von elektromagnetischen Störungen	Fehlerbehebung Backup-Einrichtungen Weckeinrichtungen und Rekonstruktion	I4-1, I4-2
MI-004-4.3 bis MI-004-7		Keine besondere Softwarerelevanz	
	Anhang MI-005		
	Anhang MI-006		
MI-006-IV, MI-006-V	Selbsttätige Waagen zum diskontinuierlichen und zum kontinuierlichen Totalisieren	Fehlererkennung Backup-Einrichtungen	I6-1, I6-2
	Anhang MI-007		
MI-007-8	Zulässige Einflüsse von elektromagnetischen Störungen	Backup-Einrichtungen	I7-1
	Anhang MI-008		

MID			Softwareleitfa den
Artikel / Anhang Nr. (AI = Anhang I)	Bezeichnung	Anmerkung	Anforderung Nein
	Anhang MI-009		
	Anhang MI-010		

13 Verweise und Literatur

- [1] Software Requirements and Validation Guide, Version 1.00, 29 October 2004, European Growth Network “MID-Software”, contract number G7RT-CT-2001-05064, 2004
- [2] 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, 29.3.2014
- [3] Richtlinie 2004/22/EG des Europäischen Parlaments und des Rates vom 31. März 2004 über Messgeräte. Amtsblatt der Europäischen Union L 135/1, 30.4.2004
- [4] Internet Security Glossary, <http://www.ietf.org/rfc/rfc2828.txt>
- [5] ISO/IEC JTC1/SC7 3941, 2008-03-14, <http://pef.czu.cz/~papik/doc/MHJS/pdf/IT-VOCABULARY.pdf>

14 Revisionshistorie

Nr.	Datum	Wichtige Änderungen
1	Mai 2005	Leitfaden erstmals herausgegeben.
2	April 2007	Ergänzen und Verbessern der Begriffe in Abschnitt 2 Redaktionelle Änderungen in den Abschnitten 4.1 und 5.1 Änderung einer Präzisierung für die Softwareidentifikation in Abschnitt 4.2, Anforderung P2 und Abschnitt 5.2, Anforderung U2. Ergänzung in Anforderung L8, Detaillierende Anmerkungen 1. Ergänzung um eine Erklärung zu Anforderung S1, Detaillierende Anmerkung 1. Ersetzen von Anforderung D5 durch eine Bemerkung. Ändern der Risikoklasse für Messsysteme für Flüssigkeiten außer Wasser. Ändern der Risikoklassen für Waagen. Verschiedene kleinere redaktionelle Änderungen im Dokument. Ergänzen um diese Revisionstabelle.
3	März 2008	Ergänzen von Ausnahmen für die Anzeige der Softwareidentifikation: neue Anforderungen I1-5, I2-9, I3-6, I4-5 und I5-1.
4	Mai 2009	Einschränkung des Anwendungsbereiches des Software-Downloads, Klärung der Identifizierungsanforderungen im Zusammenhang mit Software-Download Überarbeitung der Anforderungen P2 und U2: Streichen nichtiger Textfragmente.
5	Mai 2011	Überarbeitung des Kapitels 5 (Teil U): Weiterentwicklung in Bezug auf Betriebssysteme Ersetzen des Begriffs "Komponente" im gesamten Leitfaden durch andere geeignete Begriffe, um Missverständnisse zu vermeiden Ergänzen von Anforderung D1 in Abschnitt 9.2 durch Einführung einer versiegelbaren Einstellung für den Download-Mechanismus. Verfeinerung der Erläuterungen zu den Anforderungen P2 und U2 in Abschnitt 4.2 bzw. 5.2 bzgl. der Softwareidentifikation. Erweiterung der Beispiele für akzeptable Lösungen in Anforderung L2 (Abschnitt 6.2) und in Anforderung U8 (Abschnitt 5.2).
6	März 2015	Hauptrevision: - Charakteristisches Merkmal des Leitfadens: Der Leitfaden gilt als rein technisches Dokument, das softwarebezogene wesentliche Anforderungen

		interpretiert. Aussagen, die diesem Grundsatz widersprechen, wurden entfernt. - Adressaten des Leitfadens: Der Leitfaden ist für Softwareentwickler und -prüfer bestimmt, kann jedoch auch von anderen Parteien verwendet werden, insbesondere von Marktaufsichtsbehörden, wo und wann immer es angebracht ist. - Es hat sich herausgestellt, dass die Umsetzung der beiden vorherigen Aktualisierungen im Einzelnen viel redaktionelle Arbeit erfordert. Diese Änderungen führen zu einer besseren Lesbarkeit des Leitfadens, bedeuten jedoch keine technischen Spezifikationen. - Software-Identifizierung (P2/U2): Im Leitfaden 7.2 wird nicht mehr gefordert, dass der Software-Identifikator von der Software selbst zur Verfügung gestellt wird. Es genügt, wenn gefordert wird, dass der Software-Identifikator gesichert vom Gerät zur Verfügung gestellt wird. - Unterscheidung zwischen Identifikation und Integrität (P2/U2, P6/U6): MID Anhang 1 unterscheidet zwischen Identifikation der Software (Anhang 1, 7.6) und Integrität, z.B. Schutz der Software (Anhang 1, 8.4). Die Unterscheidung hat keine weniger strengen Anforderungen zur Folge. - Unterstützung der Konformität mit der Bauart: Die für die Softwareintegrität erforderlichen technischen Mittel werden als geeignet für die Verwendung für Prüfung der Konformität mit der Bauart angesehen. Die erforderlichen Mittel sind z.B. Prüfsummen oder gleichwertige Mittel auf verschiedenen Ebenen für sämtliche Geräte der Risikoklasse C und höher. - Risikoklassen: Risikoklasse C wurde geändert, so dass nun die gesamte rechtlich relevante Software für Geräte in Risikoklasse C als festgelegt gelten. Auf diese Weise wurden Unstimmigkeiten darüber beseitigt, welcher Softwareteil als festgelegt gilt. In Risikoklasse C und höher muss die Softwareidentität auf der Bit-Ebene (z.B. durch Prüfsummen) umgesetzt werden. - Risikoklassifikation von Geräten mit Universalcomputern (Geräte vom Typ U): Aufgrund eines grundsätzlich höheren Risikos bei Geräten vom Typ U wird ihre Einteilung in Risikoklasse B als ungeeignet angesehen. Geräte vom Typ U können nur in Risikoklasse C und höher eingestuft werden. - Akzeptable Sicherheitsmaßnahmen für höhere Risikoklassen (D und höher): Was Algorithmen und minimale Schlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institute, die für die Datensicherheit verantwortlich sind, berücksichtigt werden (z.B. NIST (USA), DCSSI (Frankreich), CESS (Vereinigtes Königreich), CCN (Spanien), NCSC (Niederlande), BSI (Deutschland)).
--	--	--

		- Rechtlich relevante Software: Es scheint nicht mehr notwendig zu sein, zwischen rechtlich relevanter Software und fester rechtlich relevanter Software zu unterscheiden. Sämtliche in Anhang I aufgeführten Schutzanforderungen gelten für rechtlich relevante Software.
7	März 2018	Ergänzung von P7 um eine akzeptable Lösung, die sicherstellt, dass der Inhalt des Ereignislogbuchs auf der Anzeige dargestellt wird, wird hinzugefügt. Ergänzung von U8 und Einbindung der entsprechenden P8 zur allgemeineren Beschreibung von Kopplung und Handshake-Betrieb zwischen Einheiten. Verbesserte Anschaulichkeit von Anhang S mittels Streichung der Definition der Low-Level-/High-Level-Softwaretrennung.
8	April 2019	Redaktionelle Änderungen hinsichtlich des Übersetzungsabgleichs, Datenbereinigung, Erläuterung der Anwendung von Anhang T, Korrekturen in P6, U6, T2, T6 und L2 Umstrukturierung zwischen "Akzeptable Lösungen" and "Detaillierende Anmerkungen" für jede Anforderung. Die beiden gerätespezifischen Anhänge 10.2 Gaszähler und Mengenumwerter sowie 10.3 Elektrizitätszähler für Wirkverbrauch wurden vollständig überarbeitet. Kapitel 11.1 "In die Baumusterprüfbescheinigung einzubeziehende Informationen" wurde angepasst.
9	Oktober 2020	Revision der Anhänge 10.1 Wasserzähler, 10.4 Wärmezähler, 10.5 Messsysteme zur kontinuierlichen und dynamischen Mengenmessung von Flüssigkeiten außer Wasser und 10.7 Taxameter.

Tabelle 14-1: Revisionshistorie