WELMEC 7.2

Ausgabe 5

WELMEC

European Cooperation in Legal Metrology

Softwareleitfaden

(Europäische Messgeräterichtlinie 2004/22/EC)

Mai 2011

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.

Veröffentlicht durch:
WELMEC Sekretariat

Thijsseweg 11
NL – 2629 JA Delft
The Netherlands

e-mail : secretary@welmec.org
tel : + 31 15 269 17 09
fax : + 31 15 285 05 07

Website: www.welmec.org

W72Ausgabe5_DE_120208.docx

Softwareleitfaden

(Europäische Messgeräterichtlinie 2004/22/EC)

Inhalt

Vorwort

Der vorliegende Leitfaden basiert auf dem “Software Requirements and Validation Guide”, Version 1.00, 29. Oktober 2004, der im Netzwerk “MID-Software” 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 Messgeräterichtlinie (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 5 berücksichtigt weitere Erfahrungen aus der Anwendung des Leitfadens.

Vorwort zur deutschen Ausgabe

Die deutschsprachige Fassung des WELMEC Leitfadens ist inhaltlich identisch zum englischsprachigen Original. Veränderungen sind nur dann vorgenommen worden, wenn bei der Übertragung in die deutsche Sprache eindeutige Fehler im Original festgestellt worden sind. Solche Änderungen sind durch Fußnoten gekennzeichnet.

Mit der Übertragung in die deutsche Sprache hat ansonsten keine weitere inhaltliche Bearbeitung stattgefunden. Die Weiterentwicklung des Leitfadens bleibt der WELMEC Arbeitsgruppe „Software“ vorbehalten.

Sollte sich im Einzelfall doch eine inhaltliche Differenz zwischen dem englischsprachigen Original und der deutschsprachigen Fassung ergeben, gilt die englischsprachige Originalversion.

1 Einleitung

Dieses Dokument bietet all jenen eine Anleitung, die die Messgeräterichtlinie (Measuring Instruments Directive, MID) anwenden, insbesondere für mit Software ausgestattete Messgeräte. Der Leitfaden richtet sich sowohl an Messgerätehersteller als auch an die Benannten Stellen, die für die Konformitätsüberprüfung der Messgeräte verantwortlich sind.

Wird nach diesem Leitfaden verfahren, kann das Erfüllen der softwarebezogenen MID-Vorschriften unterstellt 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 beigefügt (Kapitel 13).

Vorgänger des vorliegenden Leitfadens war der von der WELMEC-Arbeitsgruppe 7 ausgearbeitete Leitfaden 7.1. Beide Leitfäden basieren auf denselben Grundsätzen und wurden aus den Anforderungen der MID abgeleitet. Der Leitfaden 7.1 wurde überarbeitet und besteht weiter (Ausgabe 2), hat aber jetzt nur noch informativen Charakter, während der Leitfaden 7.2 der von der WELMEC empfohlene Leitfaden für Softwareerstellung und Prüfung und Bewertung von softwaregesteuerten Messgeräten ist, die der MID unterliegen.

Aktuelle Informationen zu den Leitfäden und zur Arbeit der WELMEC Arbeitsgruppe 7 sind auf folgender Webseite verfügbar: http://www.welmecwg7.ptb.de/index.html.

2 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 (Acceptable solution): 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.

Änderungsprotokoll (Audit trail): Ein Softwarezähler (z.B. Ereigniszähler) und/oder ein Informationsspeicher (z.B. Ereignislogbuch) zum Nachweis von Änderungen an rechtlich relevanter Software oder rechtlich relevanten Parametern.

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

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

Messgerät mit zweckgebundener Hard- und Software (Built-for-purpose measuring instrument) (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 Kapitel 4.1.

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

Kommunikationsschnittstelle (Communication interface): Eine elektronische, optische, Funk- oder andere technische Schnittstelle, die es ermöglicht, Informationen automatisch zwischen *Messgeräten*, *Teilgeräten* oder externen Geräten oder Teileinheiten von ihnen auszutauschen.

Gerätespezifische Parameter (Device-specific parameter): *Rechtlich relevante Parameter,* deren Wert vom einzelnen Gerät abhängt. Gerätespezifische Parameter umfassen Kalibrierparameter (z.B. Anpassung des Messbereichsumfang 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 einer berechtigten Person wie z.B. Gerätebesitzer oder Produktverkäufer zugänglich sind (setzbare Parameter).

Feste Software (Fixed software): Teil der Software, der bei der Baumusterprüfung als fest erklärt wird, d.h., nur mit Zustimmung einer Benannten Stelle änderbar ist. Der feste Teil ist in jedem einzelnen Gerät identisch.

Integrierter Speicher (Integrated storage): Nicht entfernbarer Speicher, der Teil des Messgerätes ist, wie z.B. RAM, EEPROM oder Festplatte.

Integrität von Daten und von Software (Integrity of data and software): Gewissheit, dass die Daten und die Software während ihrer Nutzung, Übertragung oder Speicherung nicht unbefugt geändert wurden.

IT-Konfiguration (IT configuration): Aufbau des *Messgerätes* hinsichtlich der IT-Funktionen und Eigenschaften, die - mit Blick auf die Anforderungen - unabhängig von der Messfunktion sind. 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 (Legally relevant parameter): Parameter eines *Messgerätes* oder eines *Teilgeräts*, der der gesetzlichen Kontrolle unterliegt. Es werden unterschieden: *bauartspezifische Parameter* und *gerätespezifische Parameter*.

Rechtlich relevante Software (Legally relevant software): Programme, Daten und *bauartspezifische Parameter*, die zum Messgerät oder zum *Teilgerät* gehören und Funktionen festlegen oder ausführen, die der gesetzlichen Kontrolle unterliegen.

Langzeitspeicherung von Messdaten (Long-term storage of measurement data): Speicherung von Messdaten, um diese nach Abschluss der Messung für spätere, rechtlich relevante Zwecke bereitzuhalten (z.B. für den Abschluss eines Handelsgeschäftes).

Messgerät (Measuring instrument): Jedes Gerät oder System mit einer Messfunktion. Der Vorsatz “Mess-” wird weggelassen, wenn Missverständnisse ausgeschlossen werden können. [MID, Artikel 4]

Messgeräte mit Universalrechner (Typ U) (Measuring instruments using a universal computer (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 (Open network): 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*).

Risikoklasse (Risk class): Klasse von *Messgerät*ebauarten mit gleichen Risikobewertungen.

Softwaredownload (Software download): Der Prozess der automatischen Übertragung von Software unter Nutzung 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).

Softwareidentifikation (Software identification): Eine Folge von lesbaren Zeichen, die der Software zugeordnet ist und die untrennbar mit der Software verbunden ist (z.B. Versionsnummer, Prüfsumme).

Softwaretrennung (Software separation): 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 (Sub-assembly): 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 (Transmission of measurement data): 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 (Type examination certificate): Baumusterprüfbescheinigung.
Hinweis: Es gibt in der MID „EC type examination certificates“ (EG Baumusterprüfbescheinigung) und „EC design examination certificates“ (EG Entwurfsprüfbescheinigungen)

Bauartspezifischer Parameter (Type-specific parameter): *Rechtlich relevanter Parameter* mit einem Wert, der nur von der Bauart des Gerätes abhängt. Bauartspezifische Parameter sind Teil der *rechtlich relevanten Software*. Sie werden bei der Baumuster-oder Entwurfsprüfung des Gerätes festgeschrieben.

Benutzerschnittstelle (User interface): Schnittstelle, die den Teil des Gerätes oder Messsystems bildet, der es ermöglicht, Informationen zwischen einem Menschen und dem Messge-

rät oder seinen Hardware- oder Softwareteilen auszutauschen, wie z.B. Schalter, Tastatur, Maus, Display, Monitor, Drucker, Touch-Screen.

Validierung (Validation): 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.

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

Hashalgorithmus (Hash algorithm): Algorithmus, der den Inhalt eines Datenblocks zu einer 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 (Signature algorithm): Ein kryptografischer Algorithmus, der unter Nutzung eines *Signaturschlüssels* den Hashcode eines Datenblocks verschlüsselt und der es ermöglicht, diesen mit dem entsprechenden Entschlüsselungs-*Signaturschlüssel* wieder zu entschlüsseln[1].

Signaturschlüssel (Signature key): Jede Zahl oder Zeichenfolge, die zum Verschlüsseln und Entschlüsseln von Informationen verwendet wird. Es gibt zwei verschiedene Arten von Signaturschlüsseln: symmetrische und asymmetrischen Schlüsselsysteme. Symmetrischer Schlüssel bedeutet, dass Sender und Empfänger von Informationen den gleichen Schlüssel verwenden. Das Schlüsselsystem heißt asymmetrisch, wenn die Schlüssel für Sender und Empfänger verschieden sind, aber in einem bestimmten Verhältnis zueinander stehen. Normalerweise ist der Schlüssel des Senders nur dem Sender und der Schlüssel des Empfängers in festgelegter Umgebung bekannt (öffentlich).

Public-Key-System (PKS): Ein Paar von *Signaturschlüsseln*: 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 (und damit signiert), 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-System*. Dies schließt die Gewährung und Verteilung von digitalen Zertifikaten an alle Mitglieder ein, die am Informationsaustausch teilnehmen.

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

Elektronische Signatur (Electronic signature): 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.

---

[1] Fehler im englischen Original, hier korrigiert: Falsche Definition

3 Verwendung des Leitfadens

Dieser Abschnitt beschreibt den Aufbau des Leitfadens und erläutert seine Verwendung.

3.1 Gesamtstruktur des Leitfadens

Der Leitfaden besteht aus einem strukturierten Satz von Anforderungsblöcken. Die Gesamtstruktur des Leitfadens berücksichtigt die Einteilung von Messinstrumenten in Basiskonfigurationen und 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 (Anhänge L, T, S und D),
3. gerätespezifische Anforderungen (Anhänge I.1, I.2, …).

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 3-1 dargestellt.

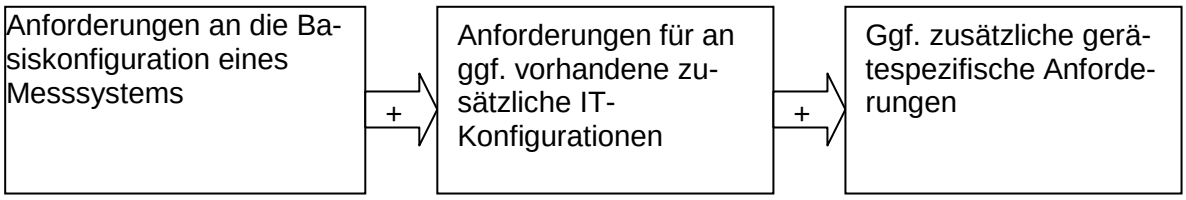

Abbildung 3-1: Arten von Anforderungssätzen, die auf ein Gerät angewandt werden müssen

Die Übersichten in der folgenden Abbildung 3-2 zeigen, welche Anforderungssätze vorhanden sind.

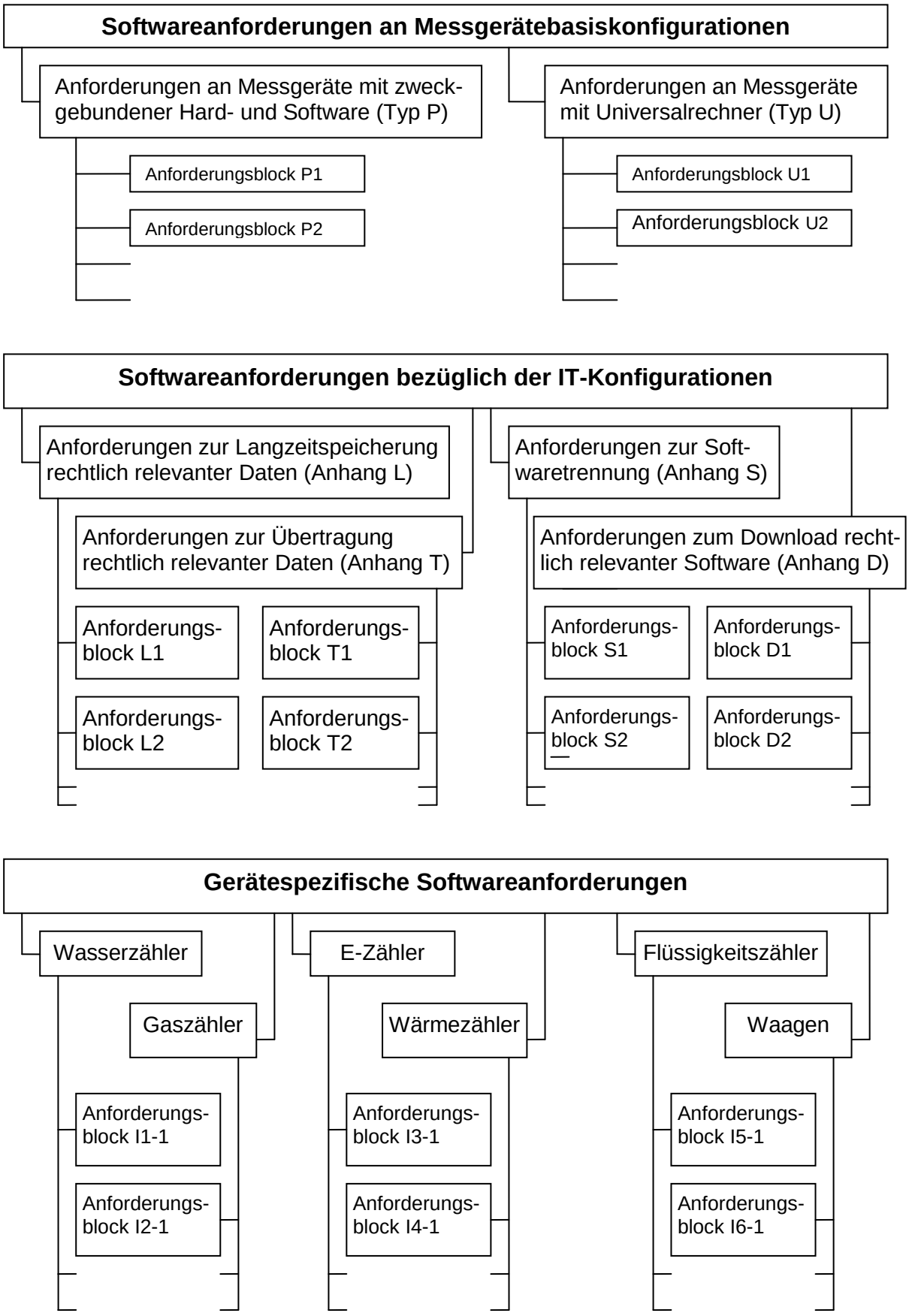

Abbildung 3-2: Übersicht über die Anforderungssätze

Zusätzlich zu der beschriebenen Struktur sind 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 höchste Risikoklasse F werden gegenwärtig nicht verwendet. Sie sind Platzhalter für den Fall, dass sie in Zukunft notwendig werden. Die verbleibenden Risikoklassen B bis E decken alle Geräteklassen ab, die in der MID geregelt sind. Darüber hinaus bieten sie genügend Spielraum für den Fall geänderter Risikobewertungen. Die Klassen werden in Kapitel 11 des Leitfadens definiert, das jedoch nur informativen Charakter besitzt.

Jedes Messgerät muss einer Risikoklasse zugeordnet werden, da die anzuwendenden Softwareanforderungen von der Risikoklasse abhängen, zu der das Messgerät gehört.

3.2 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 Kapitel 4.1) oder als Messgerät mit Universalrechner (Typ U, siehe Kapitel 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 Gerätekonfigurationen (Anhänge L, T, S und D)*

Die IT-Konfigurationen umfassen: Langzeitspeicherung rechtlich relevanter Daten (L), Übertragung rechtlich relevanter Daten (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 geeignet und dementsprechend anzuwenden sind (Abbildung 3-2).

Schritt 3: *Auswahl von gerätespezifischen Anforderungen (Anhang I)*

Mit Hilfe des jeweiligen gerätespezifischen Anhangs I.x ist auszuwählen, welche gerätespezifischen Anforderungen gegebenenfalls geeignet und dementsprechend anzuwenden sind (Abbildung 3-2).

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 ausgewählt wurde, brauchen nur noch die jeweiligen Anforderungen und die Validierungsanleitung berücksichtigt zu werden.

3.3 Arbeit mit einem Anforderungsblock

Jeder Anforderungsblock enthält eine eindeutige Anforderung. Er besteht aus einem definierenden Text, erklärenden Erläuterungen, der geforderten 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 3-3.

Titel der Anforderung		
Hauptaussage der Anforderung (eventuell nach Risikoklassen unterteilt)		
Erläuterungen (Anwendungsbereich, zusätzliche Erklärungen, Ausnahmen usw.)		
Erforderliche Dokumentation (eventuell nach Risikoklassen unterteilt)		
Validierungsanleitung für eine Risikoklasse	**Validierungsanleitung** für die 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 Erläuterungen.
- 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 Erläuterungen.
- Befolgen der Validierungsanleitung.
- Bestätigen der Vollständigkeit der bereitgestellten Dokumentation.

3.4 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.

Verfahren:

- Die Checklisten, die gemäß der in Schritt 1, 2 und 3 in Abschnitt 3.2 beschriebenen Auswahl notwendig sind, sind zu sammeln.
- Die Checklisten sind durchzugehen und es ist zu prüfen, ob alle Anforderungen erfüllt wurden.
- Die Checklisten sind nach Bedarf auszufüllen.

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

Die Anforderungen in diesem Kapitel sind gültig für ein Messgerät oder ein Teilgerät mit zweckgebundener Hard- und Software. Die Gültigkeit erstreckt sich selbst dann auch auf Teilgeräte, wenn es nicht ausdrücklich im Text erwähnt wird. Wenn das Messgerät einen Universalcomputer (All-Zweck-PC) benutzt, gelten die Anforderungen des folgenden Kapitels (Typ-U-Gerät). Die Anforderungen für Typ-U-Geräte müssen auch verwendet werden, wenn die folgende technische Beschreibung 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 (i.A. ist es ein Mikroprozessor- oder Mikrocontroller-basiertes System). Es ist durch die folgenden Merkmale charakterisiert:

- Die gesamte Anwendersoftware ist für den Messzweck konstruiert. Dies schließt sowohl rechtlich relevante als auch sonstige Funktionen ein.
- Die Benutzerschnittstelle ist ausgelegt für den Messzweck, d.h. sie wird normalerweise in einer rechtlich relevanten Betriebsart verwendet. Das Umschalten in eine rechtlich nicht relevante Betriebsart ist möglich.
- Wenn es ein Betriebssystem gibt, hat es keine Bedienoberfläche, die dem Benutzer zugänglich ist (um Programme zu laden oder zu ändern, um Befehle an das Betriebssystem zu schicken, die Anwendungsumgebung zu ändern usw.).

Das P-Typ-Gerät kann zusätzliche Eigenschaften und Merkmale haben, die dann die folgenden Anforderungserweiterungen erfüllen müssen:

- Die Software wird als Ganzes entworfen und behandelt, es sei denn, eine Softwaretrennung entsprechend Anhang S ist realisiert worden.
- Die Software ist unveränderbar und es gibt keine Möglichkeit zum Programmieren oder zum Ändern/Austauschen der rechtlich relevanten Software. Softwaredownload ist nur erlaubt, wenn Anhang D beachtet worden ist.
- Schnittstellen für Messdatenübertragung über offene oder geschlossene Kommunikationsnetze sind gestattet (Anhang T ist zu beachten).
- Die Speicherung von Messdaten in einem integrierten Speicher, einem Fernzugriffs- oder entfernbaren Speicher ist gestattet. (Anhang L ist zu beachten.)

4.2 Spezifische Anforderungen an Typ P

Risikoklassen B bis E

P1: Dokumentation

Zusätzlich zur spezifischen Dokumentation, die für jede der folgenden Anforderungen erforderlich ist, muss die Dokumentation grundsätzlich folgendes *umfassen:*

a. Eine Beschreibung der rechtlich relevanten Software.
b. Eine Beschreibung der Genauigkeit der Messalgorithmen (z.B. Preisberechnungs- und Rundungsalgorithmen).
c. Eine Beschreibung der Benutzerschnittstelle, der Menüs und der Dialoge.
d. Die eindeutige Softwareidentifikation.
e. Einen Überblick über die Systemhardware, z.B. Block-Schaltbild, Mikrocontrollertyp, Art des Netzwerkes, usw., wenn sie nicht im Betriebshandbuch beschrieben sind.
f. Das Betriebshandbuch.

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">P2: Softwareidentifikation
Die rechtlich relevante Software muss eindeutig gekennzeichnet sein. Die Softwareidentifikation muss untrennbar mit der Software verbunden sein. Sie muss auf Befehl oder laufend während des Betriebs dargestellt werden.</td></tr>
<tr><td>Erläuterungen
1. Änderungen an der rechtlich relevanten Software erfordern eine Information der Benannten Stelle. Die Benannte Stelle entscheidet, ob eine neue Softwareidentifikation notwendig ist oder nicht. Eine neue Softwareidentifikation ist erforderlich, wenn die Softwareänderungen zu Änderungen der zugelassenen Funktionen oder Charakteristika führen.</td><td colspan="2">Erläuterungen
1.Zusätzlich zu 1, Risikoklasse B: Jede Änderung an der rechtlich relevanten Software, die bei der Konformitätsbewertung/Baumusterprüfung als fest definiert wurde, erfordert eine neue Softwareidentifikation.
Wenn nicht die gesamte rechtlich relevante Software als fest definiert ist, kann es einen zusätzlichen Teil geben, der auch für Risikoklasse C entsprechend Risikoklasse B behandelt wird. Wenn es jedoch technisch nicht möglich ist, eine Softwareidentifikation für den festen Teil zu realisieren (z.B. eine ausschließlich über dem festen Teil des ausführbaren Codes erzeugte CRC-Prüfsumme) und eine für den Rest (z.B. eine Versionsnummer) muss die gesamte Software als fest definiert werden und durch eine Prüfsumme identifizierbar sein.</td></tr>
<tr><td colspan="3">2. Die Softwareidentifikation muss für Eich- und Inspektionszwecke einfach anzeigbar sein (einfach bedeutet über die Standardbenutzerschnittstelle, ohne zusätzliche Werkzeuge).
3. Die Softwareidentifikation muss eine Struktur haben, die eindeutig jene Versionen kennzeichnet, die Konformitätsbewertung/Baumusterprüfung erfordern, und solche, die sie nicht erfordern.
4. Wenn zwischen Funktionen der Software durch bauartspezifische Parameter umgeschaltet werden kann, kann jede Funktion oder Variante separat bzw. das komplette Paket als Ganzes mit einer Identifikation versehen werden.</td></tr>
<tr><td>Erforderliche Dokumentation
Die Dokumentation muss sowohl die Softwareidentifikationen auflisten als auch beschreiben, wie diese erzeugt werden, wie sie untrennbar mit der Software verbunden sind, wie sie zur Ansicht gebracht werden können und wie sie strukturiert sind, um zwischen Veränderungen unterscheiden zu können, die eine Konformitätsbewertung/Baumusterprüfung betreffen und denen die nicht.</td><td colspan="2">Erforderliche Dokumentation (Zusätzliche Dokumentation zu denen von Risikoklasse B und C)
Die Dokumentation muss die Maßnahmen aufzeigen, die ergriffen werden, um die Softwareidentifikation vor Fälschung zu schützen.</td></tr>
<tr><td>Validierungsanleitung
Auf Basis der Dokumentation ist zu überprüfen
• die Beschreibung der Erzeugung und Visualisierung der Softwareidentifikation,
• ob alle Programme, die rechtlich relevante Aufgaben ausführen, deutlich gekennzeichnet und beschrieben sind, so dass sowohl der Benannten Stelle als auch dem Hersteller klar ist, welche Softwarefunktionen durch die Softwareidentifikation abgedeckt werden und welche nicht,
• ob ein Sollwert der Identifikation (Versionsnummer oder Prüfsumme) vom Hersteller bereitgestellt wird. Dieser Sollwert muss im Prüfzertifikat aufgeführt sein.
Funktionsprüfungen:
• Die Softwareidentifikation kann so dargestellt werden, wie in der Dokumentation beschrieben.
• Die dargestellte Identifikation ist korrekt.</td><td colspan="2">Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C)
Auf Basis der Dokumentation ist zu überprüfen
• ob die Maßnahmen, die zum Schutz vor Fälschung der Softwareidentifikation ergriffen werden, angemessen sind.</td></tr>
<tr><td colspan="3">Beispiel einer akzeptablen Lösung
• Die Identifikation der rechtlich relevanten Software umfasst zwei Teile. Teil (A) muss geändert werden, wenn Änderungen an der Software eine neue Prüfung erfordern. Teil (B)</td></tr>
</table>

zeigt nur geringfügige Änderungen der Software, z.B. Fehlerbeseitigungen, die keine neue Prüfung erfordern. • Die Identifikation wird auf Befehl erzeugt und angezeigt.	
• Teil (A) der Identifikation. besteht aus einer Versionsnummer oder der TEC-Nummer.	• Teil (A) der Identifikation besteht aus einer automatisch erzeugten Prüfsumme über der rechtlich relevanten Software, die bei der Konformitätsbewertung/Baumusterprüfung als fest erklärt wurde. Für die verbleibende rechtlich relevante Software ist Teil (A) eine Versionsnummer oder TEC-Nummer. • Ein Beispiel einer akzeptablen Lösung für die Ausführung der Prüfsumme ist der CRC-16-Algorithmus.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Zusätzliche Dokumentation zu der bei Risikoklasse B und C genannten) Quellcode, der die Erzeugung der Identifikation enthält.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): *Auf Basis des Quellcodes ist zu überprüfen* • ob alle relevanten Softwareteile durch den Algorithmus für die Erzeugung der Identifikation abgedeckt sind, • ob der Algorithmus korrekt implementiert ist.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
P3: Einflussnahme über die Benutzerschnittstelle *Die über die Benutzerschnittstelle eingegebenen Befehle dürfen die rechtlich relevante Software und die Messdaten nicht unzulässig beeinflussen.*		
Erläuterungen 1. Befehle können einzelne oder eine Folge von Schalter- oder Tastenbetätigungen sein, die manuell ausgeführt werden. 2. Es muss eine eindeutige Zuordnung jedes Befehls zu einer angestoßenen Funktion oder Datenänderung geben. 3. Schalter- oder Tastenbetätigungen, die nicht als Befehle deklariert und dokumentiert sind, dürfen keine Wirkung auf die Funktionen des Gerätes und die Messdaten haben.		
Erforderliche Dokumentation Wenn das Gerät die Fähigkeit zum Befehlsempfang hat, muss die Dokumentation folgendes enthalten: • Eine vollständige Liste aller Befehle (z.B. Menüpunkte) zusammen mit einer Erklärung des Herstellers zur Vollständigkeit. • Eine Kurzbeschreibung ihrer Bedeutung und ihrer Wirkungen auf die Funktionen und die Daten des Messgerätes.		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) • Die Dokumentation muss die Maßnahmen aufzeigen, mit denen die Vollständigkeit der Befehlsdokumentation sichergestellt wird. • Die Dokumentation muss ein Protokoll enthalten, das die Tests aller Befehle anzeigt.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob alle dokumentierten Befehle zulässig sind, d.h. ob sie eine erlaubte oder überhaupt keine Auswirkung auf die Messfunktionen (und die relevanten Daten) haben. • ob der Hersteller eine ausdrückliche Erklärung zur Vollständigkeit der Befehlsdokumentation beigefügt hat. *Funktionsprüfungen:*		**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen und die Testprotokolle dem hohen

• Ausführen praktischer Tests (Stichproben) mit den dokumentierten und nicht dokumentierten Befehlen. Prüfen aller Menüpunkte, soweit vorhanden.	Schutzniveau entsprechen.

Beispiel einer akzeptablen Lösung
Es gibt ein Softwaremodul, das die Befehle von der Benutzerschnittstelle empfängt und interpretiert. Dieses Modul gehört zur rechtlich relevanten Software. Er leitet nur erlaubte Befehle an die anderen rechtlich relevanten Softwaremodule weiter. Gänzlich unbekannte oder nicht erlaubte Folgen von Schalter- oder Tastenbetätigungen werden zurückgewiesen und haben keine Auswirkung auf die rechtlich relevanten Software oder Messdaten.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Zusätzliche Dokumentation zu der bei Risikoklasse B und C genannten):
Quellcode des Gerätes.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C):
Auf Basis des Quellcodes ist zu überprüfen

- ob die Software so aufgebaut ist, dass der Datenfluss bezüglich der Schnittstellenbefehle nur in der rechtlich relevanten Software realisiert wird. und das anhand des Quellcodes nachvollzogen werden kann.
- dass kein unzulässiger Datenfluss von der Benutzerschnittstelle zu den zu schützenden Bereichen erfolgt.
- ob die Befehle richtig interpretiert werden und keine nicht dokumentierten Befehle existieren. Die Überprüfung kann mit Tools oder manuell erfolgen.

Risikoklasse B	Risikoklasse C	Risikoklasse D

P4: Einflussnahme über die Kommunikationsschnittstelle
Die über die Kommunikationsschnittstelle eingegebenen Befehle dürfen die rechtlich relevante Software und die Messdaten nicht unzulässig beeinflussen.

Erläuterungen

1. Es muss eine eindeutige Zuordnung jedes Befehls zu einer initiierten Funktion oder zu Datenänderungen geben.
2. Das bedeutet, dass Signale oder Codes, die nicht als Befehle erklärt und dokumentiert sind, keine Wirkung auf die Funktionen und die Daten des Gerätes haben dürfen.
3. Befehle können eine Folge von elektrischen (optischen, elektromagnetischen usw.) Signalen an Eingangskanälen oder Codes in Datenübertragungsprotokollen sein.
4. Die Einschränkungen dieser Anforderung werden ausgesetzt, wenn ein Softwaredownload entsprechend Anhang D durchgeführt wird.
5. Diese Anforderung trifft nur auf unversiegelte[2] Schnittstellen zu.

Erforderliche Dokumentation Hat das Gerät eine Schnittstelle, so muss die Dokumentation folgendes umfassen: • Eine vollständige Liste aller Befehle zusammen mit einer Erklärung der Vollständigkeit. • Eine Kurzbeschreibung ihrer Bedeutung und ihrer Wirkung auf die Funktionen und die Daten des Messgerätes.	**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) • Die Dokumentation muss die Maßnahmen aufzeigen, die zum Vollständigkeitsnachweis der Befehlsdokumentation ergriffen wurden. • Die Dokumentation muss ein Protokoll enthalten, das die Tests der Befehle

[2] Anmerkung des Übersetzers: mögliche Formen des Siegels:
Siegelmarke zum Kleben (zerstört sich beim Entfernen), Plombe, Siegellack auf Schraubkopf

	oder alternativ andere geeignete Maßnahmen zum Korrektheitsnachweis anzeigt.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob alle dokumentierten Befehle zulässig sind, d.h. ob sie eine erlaubte oder keine Auswirkung auf die Messfunktionen (und die relevanten Daten) haben. • ob der Hersteller eine ausdrückliche Erklärung zur Vollständigkeit der Befehlsdokumentation beigefügt hat. *Funktionsprüfungen:* • Ausführen praktischer Tests (Stichproben), falls verfügbar mit Zusatzequipment. *Anmerkung:* Wenn es nicht möglich ist, unzulässige Wirkungen über die Schnittstelle auf die Messfunktionen (oder relevante Daten) auszuschließen und die Software nicht entsprechend berichtigt werden kann, muss die Schnittstelle im Prüfbericht als nicht rückwirkungsfrei deklariert und die erforderlichen Sicherungs-/ Versiegelungsmaßnahmen müssen beschrieben sein. Dies trifft auch auf Schnittstellen zu, die nicht in der Dokumentation beschrieben werden.	**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffen Maßnahmen und die Testprotokolle dem hohen Schutzniveau entsprechen.
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. Alle unbekannten oder nicht erlaubten Signal- oder Codefolgen werden zurückgewiesen und haben keine Auswirkung auf die rechtlich relevante Software oder die Messdaten.	

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Zusätzliche Dokumentation zu denen von Risikoklasse B und C): Quellcode des Gerätes.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): *Auf Basis des Quellcodes ist zu überprüfen* • ob die Software so aufgebaut ist, dass der Datenfluss bezüglich der Schnittstellenbefehle eindeutig von der rechtlich relevanten Software realisiert wird und das anhand des Quellcodes bestätigt werden kann. • dass kein unzulässiger Datenfluss von der Schnittstelle zu den zu schützenden Bereichen erfolgt. • ob die Befehle richtig interpretiert werden und keine nicht dokumentierten Befehle existieren. Die Überprüfung kann mit Tools oder manuell erfolgen.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
P5: Schutz vor zufälligen oder unbeabsichtigten Änderungen *Rechtlich relevante Software und Messdaten müssen vor zufälligen oder unbeabsichtigten Veränderungen geschützt werden.*		
Erläuterungen Mögliche Gründe für versehentliche Änderungen und Fehler sind unvorhersehbare physikalische Einflüsse, Einflüsse durch Benutzertätigkeit (Bedienungsfehler) und unerkannte Fehler der Software, obwohl modernste Entwicklungsmethoden beachtet wurden. Diese Anforderung umfasst: a) Physikalische Einflüsse: Gespeicherte Messdaten müssen vor Veränderung oder Löschen aufgrund eines auftretenden Fehlers geschützt oder alternativ muss der Fehler erkennbar sein.		

b) Benutzertätigkeit: Vor dem Löschen oder Ändern von Daten muss eine Bestätigung verlangt werden.
c) Softwaremängel: Es müssen geeignete Maßnahmen getroffen werden, um Daten vor unbeabsichtigten Änderungen zu schützen, die durch fehlerhaften Programmentwurf oder Programmierfehler auftreten könnten, z.B. mittels Plausibilitätsprüfungen.

Erforderliche Dokumentation

Die Dokumentation muss die Maßnahmen aufzeigen, die zum Schutz von Software und Daten gegen unbeabsichtigte Änderungen getroffen wurden.

Validierungsanleitung

Auf Basis der Dokumentation ist zu überprüfen

- ob eine Prüfsumme über den Programmcode und die relevanten Parameter automatisch erzeugt und überprüft wird.
- ob das Überschreiben von Daten nicht vor Ende der Datenspeicherungsdauer eintreten kann, das durch den Hersteller vorgesehen und dokumentiert ist.
- ob eine Warnung an den Benutzer ausgegeben wird, wenn er im Begriff ist, Messwertdateien zu löschen.

Funktionsprüfungen:

- Durch geeignete Stichproben überprüfen, ob vor dem Löschen von Messdaten eine Warnung erfolgt, sofern Löschen überhaupt möglich ist.

Beispiel einer akzeptablen Lösung

- Eine zufällige Veränderung von Software und Messdaten kann durch die Berechnung einer Prüfsumme über die relevanten Teile und Vergleich mit dem Sollwert erkannt werden. Bei einer erkannten Abweichung erfolgt eine Fehlerreaktion, wie z.B. das Beenden der Software.
- Messdaten werden nicht ohne vorherige Genehmigung gelöscht, z.B. Dialoganweisung oder -Fenster mit der Bitte um Löschbestätigung.
- Zur Fehlererkennung siehe auch Anhang I.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Zusätzliche Dokumentation zu denen von Risikoklasse B und C):

Quellcode des Gerätes.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D):

Auf Basis des Quellcodes ist zu überprüfen

- ob die getroffenen Maßnahmen zum Erkennen von Veränderungen (Störungen) angemessen sind.
- ob bei der Bildung einer Prüfsumme alle Teile der rechtlich relevanten Software durch sie abgedeckt sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D

P6: Schutz vor vorsätzlichen Änderungen

Rechtlich relevante Software muss vor unzulässigen Veränderungen, Laden oder Austausch von Hardwarespeichern geschützt werden.

Erläuterungen

1. Gerät ohne Schnittstelle: Manipulation von Programmcode wäre durch die Manipulation des technischen Speichers möglich, d.h. der Speicher wird entfernt und durch einen Speicher mit betrügerischer Software oder Daten ersetzt. Um dies zu verhindern, muss das Gehäuse des Gerätes oder der technische Speicher selbst gegen unbefugte Entnahme gesichert sein.
2. Gerät mit Schnittstelle: Die Schnittstelle darf nur Funktionen umfassen, die Prüfgegenstand sind. Alle Funktionen der Schnittstelle müssen geprüft werden (siehe P4). Wenn eine Schnittstelle zum Softwaredownload verwendet wird, muss Anhang D eingehalten werden.
3. Daten werden als ausreichend geschützt betrachtet, wenn nur rechtlich relevante Software sie verarbeitet. Wenn rechtlich nicht relevante Software nach der Zulassung verändert werden soll, sind die Anforderungen von Anhang S zu beachten.

Erforderliche Dokumentation Die Dokumentation muss darlegen, wie sichergestellt ist, dass rechtlich relevante Software nicht unzulässig verändert werden kann.	**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die Maßnahmen zum Schutz vor vorsätzlichen Änderungen sind anzugeben.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob die dokumentierten Maßnahmen zur Sicherung der Programm-Speicher gegen unbefugten Austausch ausreichend sind. • ob der Programmier-Modus elektrisch abgeschaltet werden und die Mittel zum Abschalten gesichert/versiegelt werden können, wenn der Speicher (ohne Demontage) direkt programmiert werden kann. (Zur Überprüfung von Downloadeinrichtungen siehe Anhang D). *Funktionsprüfungen*: • Geeignetes Testen des Programmiermodus und Prüfen, ob das Abschalten funktioniert.	**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) Auf Basis der Dokumentation ist zu überprüfen • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.
Beispiel einer akzeptablen Lösung Das Gerät ist versiegelt und die Schnittstellen genügen den Anforderungen P3 und P4.	

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Zusätzliche Dokumentation zu denen von Risikoklasse B und C): Quellcode des Gerätes.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): *Auf Basis des Quellcodes ist zu überprüfen* • ob die Maßnahmen für den Nachweis von vorsätzlichen Änderungen angemessen sind.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
P7: Parameterschutz *Parameter, die rechtlich relevante Eigenschaften des Messgerätes festlegen, müssen gegen unbefugte Änderung gesichert werden.*		
Erläuterungen 1. Bauartspezifische Parameter sind für jedes Exemplar der Bauart identisch und sind im allgemeinen Teil des Programmcodes. Daher gilt für sie Anforderung P6. 2. Gerätespezifische gesicherte Parameter dürfen mit Hilfe von Gerätetastatur oder Schaltern oder über Schnittstellen geändert werden, aber nur bevor sie gesichert wurden. 3. Frei setzbare gerätespezifische Parameter dürfen nach dem Sichern geändert werden.		
Erforderliche Dokumentation Die Dokumentation muss alle rechtlich relevanten Parameter beschreiben, ihre Wertebereiche und Sollwerte, wo sie gespeichert sind, wie sie inspiziert werden können und wie und wann sie gesichert werden (d.h. vor oder nach der Eichung) angeben.		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die für die Parameter getroffenen Schutzmaßnahmen sind anzugeben.
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, nach den (in Anhang I angegebenen) Listen als gesichert klassifiziert wurden.		**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen

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.	Schutzniveau entsprechen.
Beispiel einer akzeptablen Lösung a) Die Parameter sind durch Versiegelung des Instruments oder Speichergehäuses und Sperren des Schaltkreiseingangs, der Schreiben aktiviert/sperrt, durch einen dazugehörigen, versiegelten Jumper oder Schalter gesichert.	
Änderungsprotokoll (audit trail) b) Ein Ereigniszähler registriert jede Änderung eines Parameterwertes. Der aktuelle Zählerstand kann angezeigt und mit dem ursprünglichen Zählerstand verglichen werden, der bei der letzten Eichung aufgezeichnet wurde und unlöschbar auf dem Gerät registriert ist. c) Parameteränderungen 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: • die Identifikation des Parameters (z.B. der Name), • den Parameterwert (der aktuelle oder der vorherige Wert), • den Zeitstempel der Änderung. Das Ereignislogbuch kann nicht ohne Zerstörung eines Siegels gelöscht oder geändert werden.	

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Zusätzliche Dokumentation zu denen von Risikoklasse B und C): Quellcode, der die Art und Weise der Sicherung und Anzeige der rechtlich relevanten Parameter aufzeigt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): *Auf Basis des Quellcodes ist zu überprüfen* • ob die Maßnahmen für den Schutz der Parameter angemessen sind (z.B. Justiermodus nach dem Sichern gesperrt).

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

5.1 Technische Beschreibung

Die Softwareanforderungen in diesem Kapitel treffen für Messgeräte zu, die auf einem Universalrechner basieren. Die technische Beschreibung des Typ-U-Messsystems ist im Folgenden zusammengefasst. Grundsätzlich muss ein Typ-U-System angenommen werden, wenn die Voraussetzungen für ein Typ-P-Gerät (siehe Kapitel 4.1) nicht erfüllt werden.

Hardwarekonfiguration

a) Das modulare System basiert auf einem Universalrechner. Das Computersystem kann ein Stand-alone-System, Teil eines geschlossenen Netzes (z.B. Ethernet, Token-Ring-LAN) oder Teil einer 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 geschlossene Kommunikationsverbindung angekoppelt. Die Kommunikationsverbindung kann aber auch offen sein (z.B. ein Netzwerk, womit mehrere Messfühler angeschlossen werden können).

c) Die Benutzeroberfläche kann wechselweise umgeschaltet werden von einer Betriebsart, die nicht unter rechtlicher Kontrolle steht, in eine, die unter rechtlicher Kontrolle steht.

d) Speichermedien können fest installiert (z.B. Festplatte) oder entfernbar (z.B. Disketten, CD-RW) sein

Softwarekonfiguration

e) Es kann jedes Betriebssystem verwendet werden, soweit die nachfolgenden Anforderungen erfüllt werden. Neben der Anwendung des Messgeräts können sich gleichzeitig auch andere Softwareanwendungen auf dem System befinden. Teile der Software, z.B. die Messgerätanwendung, unterliegen der rechtlichen Kontrolle und dürfen nach der Zulassung nicht unzulässig verändert werden. Nicht der rechtlichen Kontrolle unterliegende Teile dürfen u.U. verändert werden.

f) Das Betriebssystem und die Low-Level-Treiber, z.B. Video-Treiber, Druckertreiber, Disk-Treiber usw., sind rechtlich nicht relevant, soweit sie nicht speziell für eine bestimmte Messaufgabe programmiert sind.

5.2 Spezifische Anforderungen an Typ U

Risikoklassen B bis E
U1: Dokumentation Zusätzlich zur spezifischen Dokumentation, die in jeder der folgenden Anforderungen erforderlich ist, muss die Dokumentation folgendes grundsätzlich umfassen: a. Eine Beschreibung der rechtlich relevanten Software, der Bedeutung der Daten usw.. b. Eine Beschreibung der Genauigkeit der Messalgorithmen (z.B. Preisberechnungs- und Rundungsalgorithmen). c. Eine Beschreibung der Benutzerschnittstelle, der Menüs und der Dialoge. d. Die Softwareidentifikation. e. Einen Überblick über die Systemhardware, z.B. Block-Schaltbild, Computerart, Art des Netzwerkes, usw., wenn sie nicht im Betriebshandbuch beschrieben sind. f. Einen Überblick über die Teile des verwendeten Betriebssystems, die genutzten Sicherungsmaßnahmen des Betriebssystems (z.B. Schutz, Benutzerkonten, Zugriffsrechte) usw. g. Das Betriebshandbuch.

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">U2: Softwareidentifikation
Die rechtlich relevante Software muss eindeutig gekennzeichnet sein. Die Softwareidentifikation muss untrennbar mit der Software verbunden sein. Sie muss auf Befehl oder während des Betriebs laufend dargestellt werden.</td></tr>
<tr><td>Erläuterungen
1. Die Softwareidentifikation umfasst nicht Low-Level-Treiber wie Video-Treiber, Druckertreiber, Disk-Treiber usw., aber sie umfasst Treiber, die speziell für eine bestimmte rechtlich relevante Aufgabe programmiert wurden.
2. Änderungen der rechtlich relevanten Software erfordern eine Information der Benannten Stelle. Die Benannte Stelle entscheidet, ob eine neue eindeutige Softwareidentifikation notwendig ist oder nicht. Eine neue Softwareidentifikation ist nur erforderlich, wenn die Softwareänderungen zu Änderungen der zugelassenen Funktionen oder Charakteristika führen.</td><td colspan="2">Erläuterungen
1. Einschränkung von 1, Risikoklasse B: (Low-Level)-Treiber, die bei der Konformitätsbewertung/Baumusterprüfung als relevant definiert wurden, müssen gekennzeichnet sein.
2. Zusätzlich zu 2 Risikoklasse B: Jede Änderung des rechtlich relevanten Programmcodes, der bei Konformitätsbewertung/Baumusterprüfung als fest definiert wurde, oder Änderungen der typspezifischen Parameter erfordert eine neue Softwareidentifikation.
Wenn nicht die gesamte rechtlich relevante Software als fest definiert ist, kann es einen zusätzlichen Teil geben, der auch bei Risikoklasse C entsprechend Risikoklasse B behandelt wird. Wenn es jedoch technisch nicht möglich ist, eine Softwareidentifikation nur für den festen Teil zu realisieren (z.B. eine ausschließlich über dem festen Teil des ausführbaren Codes erzeugte CRC-Prüfsumme) und eine für den Rest (z.B. eine Versionsnummer) muss die gesamte Software als fest definiert werden und durch eine Prüfsumme identifizierbar sein.</td></tr>
<tr><td colspan="3">3. Wenn die rechtlich relevanten Funktionen und der Account mit den Messfunktionen durch eine spezielle Betriebssystemkonfiguration geschützt sind, müssen die relevanten Konfigurationsdateien eine zusätzliche Identifikation besitzen.
4. Die Softwareidentifikation muss für Eich- und Inspektionszwecke einfach anzeigbar sein (einfach bedeutet über die Standardbenutzerschnittstelle, ohne zusätzliche Werkzeuge).</td></tr>
</table>

5. Die Softwareidentifikation muss eine Struktur haben, aus der zweifelsfrei hervorgeht, welcher Teil die Software kennzeichnet, deren Änderung eine Konformitätsbewertung/Baumusterprüfung erfordert, und welche nicht.
6. Identifikationen können auf verschiedene Ebenen angewendet werden, z.B. auf vollständige Programme, Module, Funktionen, usw.
7. Wenn zwischen verschiedenen Funktionen der Software durch bauartspezifische Parameter umgeschaltet werden kann, muss jede Funktion oder Variante separat bzw. das komplette Paket als Ganzes identifiziert werden.

Erforderliche Dokumentation Die Dokumentation muss die Softwareidentifikationen auflisten und beschreiben, wie die Softwareidentifikation erzeugt wird, wie sie untrennbar mit der Software verbunden ist, wie sie zur Ansicht abgerufen werden kann und wie sie strukturiert ist, um bei Versionsänderungen unterscheiden zu können, ob sie eine Konformitätsbewertung/Baumusterprüfung erfordern oder nicht.	**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die Dokumentation muss die Maßnahmen aufzeigen, die ergriffen werden, um die Softwareidentifikation vor Fälschung zu schützen.
Validierungsanleitung *Auf Basis der Dokumentation ist folgendes zu überprüfen* • die Beschreibung der Erzeugung und Darstellung der Softwareidentifikation, • ob alle Programme, die rechtlich relevante Aufgaben ausführen, deutlich gekennzeichnet und beschrieben sind, so dass sowohl der Benannten Stelle als auch dem Hersteller klar ist, welche Softwarefunktionen durch die Softwareidentifikation abgedeckt werden und welche nicht, • ob ein Sollwert der Identifikation (Versionsnummer oder Prüfsumme) vom Hersteller bereitgestellt wird. Dieser Sollwert muss im Prüfzertifikat aufgeführt sein. *Funktionsprüfungen:* • wird die Softwareidentifikation so dargestellt, wie in der Dokumentation beschrieben. • ist die dargestellte Identifikation korrekt.	**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die Maßnahmen, die zum Schutz vor Fälschung ergriffen werden, geeignet sind.

Beispiel einer akzeptablen Lösung

- Die Identifikation der rechtlich relevanten Software umfasst zwei Teile. Teil (A) muss geändert werden, wenn Änderungen an der Software eine neue Prüfung erfordern. Teil (B) zeigt nur geringfügige Änderungen der Software, z.B. Fehlerbeseitigungen, die keine neue Prüfung erfordern.
- Die Identifikation wird auf Befehl erzeugt und angezeigt.

• Teil (A) der Identifikation. besteht aus einer Versionsnummer oder der TEC-Nummer. Um zu verhindern, dass diese durch einfache Softwaretools geändert wird, wird sie in Binärformat im ausführbaren Programm gespeichert.	• Teil (A) der Identifikation besteht aus einer automatisch erzeugten Prüfsumme über den Teil der rechtlich relevanten Software, der bei der Konformitätsbewertung/Baumusterprüfung als fest erklärt wurde. Für die verbleibende rechtlich relevante Software darf Teil (A) eine Versionsnummer oder TEC-Nummer sein. Um zu verhindern, dass diese durch einfache Softwaretools geändert wird, wird sie in Binärformat im ausführbaren Programm gespeichert.	
	• Eine akzeptable Lösung für die Ausführung der Prüfsumme ist der CRC-16-Algorithmus.	• Akzeptable Algorithmen für die Ausführung der Prüfsumme sind CRC-32 oder Hash-Algorithmen wie SHA-1, SHA-2, MD5, RipeMD160 usw.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Quellcode, der die Erzeugung der Identifikation enthält.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): *Auf Basis des Quellcodes ist zu überprüfen* • ob alle relevanten Softwareteile durch den Algorithmus für die Erzeugung der Identifikation abgedeckt sind, • ob der Algorithmus korrekt implementiert ist.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
U3: Einflussnahme über die Benutzerschnittstelle *Die über die Benutzerschnittstelle eingegebenen Befehle dürfen die rechtlich relevante Software und die Messdaten nicht unzulässig beeinflussen.*		
Erläuterungen 1. Es muss eine eindeutige Zuordnung jedes Befehls zu einer angestoßenen Funktion oder Datenänderung geben. 2. Schalter- oder Tastenbetätigungen, die nicht als Befehle deklariert und dokumentiert sind, dürfen keine Wirkung auf die Funktionen des Gerätes und die Messdaten haben. 3. Befehle können einzelne oder eine Folge von Schalter- oder Tastenbetätigungen sein, die vom Bediener ausgeführt werden. Der Verwender muss erkennen können, welche Befehle erlaubt sind. 4. Funktionen zum Ändern der rechtlich relevanten Konfiguration des Betriebssystems dürfen dem Benutzer weder lokal noch im Fernzugriff angeboten werden. Die Konfiguration muss gegen unzulässige Änderungen gesichert sein.		
		5. Die Benutzer-Schnittstelle muss abgeschlossen sein, d.h. der Benutzer darf nicht in der Lage sein, Programme zu laden, Programme zu schreiben oder Befehle an das Betriebssystem auszuführen.
Erforderliche Dokumentation Die Dokumentation muss enthalten: • Eine vollständige Liste aller Befehle zusammen mit einer Erklärung des Herstellers zur Vollständigkeit. • Eine Kurzbeschreibung ihrer Bedeutung und ihrer Wirkungen auf die Funktionen und die Daten des Messgerätes. • Eine Beschreibung, wie eine sichere Konfiguration des Betriebssystems erreicht wird, eine Festlegung von Accounts für das Betriebssystem (z.B. "Administrator", "Benutzer", "Messaufgabe") sowie eine Festlegung der diesen Accounts gewährten Zugriffsrechte. Eine Dokumentation der Fernbedienung von Betriebssystemfunktionen (z.B. der gestarteten Dienste) und der Schutzmittel (z.B. Firewall-Konfiguration).		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die Dokumentation muss die Maßnahmen aufzeigen, die zum Vollständigkeitsnachweis der Befehlsdokumentation ergriffen wurden. Die Dokumentation muss ein Protokoll enthalten, das die Tests aller Befehle anzeigt.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob alle dokumentierten Befehle zulässig sind, d.h. ob sie eine erlaubte oder überhaupt keine Auswirkung auf die Messfunktionen (und die relevanten Daten) haben, • ob der Hersteller eine ausdrückliche Erklärung zur Vollständigkeit der Befehlsdokumentation beigefügt hat, • die Umsetzung der Maßnahmen zur Sicherung des Betriebssystems.		**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen und die Testprotokolle dem hohen Schutzniveau entspre-

Funktionsprüfungen: • Ausführen praktischer Tests (Stichproben) mit den dokumentierten und nicht dokumentierten Befehlen. Prüfen aller Menüpunkte, soweit vorhanden.	chen.

Beispiel einer akzeptablen Lösung

- Ein Modul in der rechtlich relevanten Software filtert unzulässig Befehle heraus. Nur dieses Modul empfängt die Befehle, und es kann nicht umgangen werden. Jede falsche Eingabe ist gesperrt. Der Benutzer wird bei der Befehlseingabe mittels eines speziellen Softwaremoduls geführt und seine Eingaben werden kontrolliert. Dieses Modul ist untrennbar mit dem Modul verbunden, das unzulässige Befehle herausfiltert.
- 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 (Dokumentation, die zusätzlich für die Risikoklassen B und C erforderlich ist):
Quellcode der rechtlich relevanten Software.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C):
Auf Basis des Quellcodes ist zu überprüfen

- ob der die Befehle betreffende Datenfluss 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 interpretiert werden und keine nicht dokumentierten Befehle existieren. Das Überprüfen kann mit Tools oder manuell erfolgen.

Risikoklasse B	Risikoklasse C	Risikoklasse D

U4: Einflussnahme über die Kommunikationsschnittstelle

Die über eine unversiegelte Kommunikationsschnittstelle empfangenen Befehle dürfen keinen unzulässigen Einfluss auf die rechtlich relevante Software und die Messdaten haben.

Erläuterungen

1. Es muss eine eindeutige Zuordnung jedes Befehls zu einer initiierten Funktion oder zu Datenänderungen geben.
2. Signale oder Codes, die nicht als Befehle erklärt und dokumentiert sind, dürfen keine Wirkung auf die Funktionen und die Daten des Gerätes haben.
3. Befehle können eine Folge von elektrischen (optischen, elektromagnetischen usw.) Signalen am Eingangskanal sein oder Codes in Datenübertragungsprotokollen.
4. Die Einschränkungen dieser Anforderung gelten nicht, wenn ein Softwaredownload entsprechend Anhang D durchgeführt wird.

5. Die jeweiligen Softwareteile, die die rechtlich relevanten Befehle interpretieren, müssen als rechtlich relevante Software betrachtet werden. 6. Andere Softwareteile können die Schnittstelle benutzen, sofern sie nicht den Empfang oder die Übertragung von rechtlich relevanten Befehlen oder Daten stören oder verfälschen.	5. (Statt 5, Risikoklasse B / C) Alle Programme und Programmteile, die an der Übertragung und dem Empfang von rechtlich relevanten Befehle oder Daten beteiligt sind, müssen durch die rechtlich relevante Software überwacht werden. 6. (Statt 6, Risikoklasse B / C) Die Schnittstelle, die die rechtlich relevanten Befehle oder Daten überträgt oder empfängt, muss

	für diese Funktion reserviert sein und darf nur von rechtlich relevanter Software verwendet werden. Standardschnittstellen sind jedoch nicht ausgeschlossen, wenn Softwareschutzmaßnahmen entsprechend Anhang T umgesetzt werden.
7. Wenn das Betriebssystem Fernsteuerung oder –zugriff gestattet, beziehen sich die Anforderungen U3 auf die Kommunikationsschnittstelle bzw. die angeschlossenen Fernzugriffsterminals. Zusätzlich muss Teil T für die Übertragung zwischen Computer und Terminal berücksichtigt werden.	
Erforderliche Dokumentation Die Dokumentation muss umfassen: • Eine vollständige Liste aller Befehle zusammen mit einer Erklärung der Vollständigkeit. • Eine Kurzbeschreibung ihrer Bedeutung und ihrer Wirkung auf die Funktionen und die Daten des Messgerätes. • Eine Beschreibung, wie eine sichere Konfiguration des Betriebssystems erreicht wird, eine Festlegung von Accounts für das Betriebssystem (z.B. "Administrator" und "Benutzer") sowie eine Festlegung, der diesen Accounts gewährten Zugriffsrechte. • Eine Dokumentation der Fernbedienung von Betriebssystemsfunktionen (z.B. der gestarteten Dienste) und der Schutzmittel (z.B. Firewall-Konfiguration).	**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) • Die Dokumentation muss die Maßnahmen aufzeigen, die zum Vollständigkeitsnachweis der Befehlsdokumentation ergriffen wurden. • Die Dokumentation muss ein Protokoll enthalten, das die Tests der Befehle oder alternativ andere geeignete Maßnahmen zum Korrektheitsnachweis belegt.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob alle dokumentierten Befehle zulässig sind, d.h. ob sie eine erlaubte oder keine Auswirkung auf die Messfunktionen (und die relevanten Daten) haben. • ob der Hersteller eine ausdrückliche Erklärung zur Vollständigkeit der Befehlsdokumentation beigefügt hat. • die Umsetzung der Maßnahmen zur Sicherung des Betriebssystems. *Funktionsprüfungen:* • Ausführen praktischer Tests (Stichproben), falls verfügbar mit Zusatzausstattungen.	**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen und Testprotokolle dem hohen Schutzniveau entsprechen.
Beispiel einer akzeptablen Lösung Ein Softwaremodul empfängt und interpretiert Daten von der Schnittstelle. Dieses Modul ist Teil der rechtlich relevanten Software. Er leitet nur erlaubte Befehle zu den anderen rechtlich relevanten Softwaremodulen. Alle unbekannten oder nicht erlaubten Signal- oder Codefolgen werden zurückgewiesen und haben keine Auswirkung auf die rechtlich relevante Software oder Messdaten. Der Zugriff auf das Betriebssystem über die Schnittstellen ist eingeschränkt (siehe U3/U6).	

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Zusätzliche Dokumentation zu denen von Risikoklasse B und C):

Quellcode des Gerätes.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): *Auf Basis des Quellcodes ist zu überprüfen* • ob der die Befehle betreffende Datenfluss eindeutig in der rechtlich relevanten Software definiert ist und nachvollzogen werden kann. • dass kein unzulässiger Datenfluss von der Schnittstelle zu den zu schützenden Bereichen erfolgt. • ob die Befehle richtig interpretiert werden und keine nicht dokumentierten Befehle existieren. Das Überprüfen kann mit Tools oder manuell erfolgen.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
U5: Schutz vor zufälligen oder unbeabsichtigten Änderungen *Rechtlich relevante Software und Messdaten müssen vor zufälligen oder unbeabsichtigten Veränderungen geschützt werden.*		
Erläuterungen Unbeabsichtigte Änderungen können auftreten durch: a. falschen Programmentwurf, z.B. falsche Loop-Operation, Verändern globaler Variablen in einer Funktion usw.; um dies zu vermeiden, müssen so viele Tests wie möglich durchgeführt werden. b. Missbrauch des Betriebssystems; um dies zu vermeiden, müssen die Programmierer mit dem verwendeten Betriebssystem hinreichend vertraut sein. c. versehentliches Überschreiben oder Löschen von gespeicherten Daten und Programmen (siehe auch Anhang L); d. falsche Zuordnung von übertragenen Messdaten. Messwerte und Daten, die zu einem Verarbeitungsvorgang gehören, dürfen nicht wegen fehlerhafter Programmierung oder Speicherung mit denen eines anderen Verarbeitungsvorgangs verwechselt werden; um dies zu vermeiden, müssen so viele Tests wie möglich durchgeführt und wann immer sinnvoll, zusätzliche Bestätigungsaufforderungen dafür angefordert werden. e. physikalische Effekte (elektromagnetische Störungen, Temperatur, Vibration usw.); das kann durch Selbsttests der Software vermieden werden.		
Erforderliche Dokumentation Die Dokumentation muss die Maßnahmen aufzeigen, die zum Schutz von Software und Daten gegen unbeabsichtigte Änderungen getroffen wurden.		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) • Die Dokumentation muss die Maßnahmen aufzeigen, die zur Validierung der Wirksamkeit des Schutzes ergriffen wurden.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob eine Prüfsumme des Programmcodes und der relevanten Parameter automatisch erzeugt und überprüft wird. • ob das Überschreiben von Daten nicht vor Ende der Datenspeicherungsdauer, die vom Hersteller vorgesehen und dokumentiert ist, eintreten kann. • ob eine Warnung an den Benutzer ausgegeben wird, wenn er im Begriff ist, Messwertdateien zu löschen. *Funktionsprüfungen:* • Durch geeignete Stichproben überprüfen, ob vor dem Löschen von Messdaten eine Warnung erfolgt, sofern Löschen überhaupt möglich ist.		**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.
Beispiel einer akzeptablen Lösung		

- Vermeiden eines falschen Programmdesigns - dies wird nicht im Rahmen dieser Risikoklassen betrachtet.
- Missbrauch des Betriebssystems, Überschreiben oder Löschen der gespeicherten Daten und Programme - Der Hersteller sollte in vollem Umfang die Schutz- und Vertraulichkeitsrechte nutzen, die durch das Betriebssystem oder die Programmiersprache zur Verfügung stehen.
- Die versehentliche Änderung von Programmen und Dateien kann dadurch überprüft werden, dass eine Prüfsumme über dem entsprechenden Code berechnet wird , diese mit dem Sollwert verglichen und das System gestoppt wird, wenn der Code geändert wurde; es muss eine entsprechende Reaktionen eingeleitet werden, wenn Parameter oder Daten betroffen sind.
- Falls das Betriebssystem es gestattet, ist es empfehlenswert, dass die Rechte zum Löschen, Verschieben oder Ändern der rechtlich relevanten Software für alle Benutzer entfernt werden und der Zugriff nur über Hilfsprogramme erlaubt wird. Zugriffskontrolle auf Programme und Daten durch die Verwendung von Passwörtern ist ebenso zu empfehlen, wie der Einsatz von Read-Only-Mechanismen. Der Systemsupervisor darf Rechte nur bei Bedarf wiederherstellen.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Dokumentation, die zusätzlich für die Risikoklassen B und C erforderlich ist):
Quellcode des Gerätes.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D):
Auf Basis des Quellcodes ist zu überprüfen

- ob die getroffenen Maßnahmen zum Erkennen von Veränderungen (Störungen) geeignet sind.
- ob bei der Bildung einer Prüfsumme alle Teile der rechtlich relevanten Software durch sie abgedeckt sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
U6: Schutz vor vorsätzlichen Änderungen *Rechtlich relevante Software muss vor unzulässigen Veränderungen geschützt werden.*		
Erläuterungen 1. Änderungen in Betrugsabsicht können versucht werden durch: a. Ändern des Programmcodes einschließlich der enthaltenen Daten. Wenn der Programmcode in ausführbarem Format (.exe) vorliegt, ist er für die Risikoklassen B und C ausreichend dagegen geschützt. b. Ändern der gespeicherten Messdaten - siehe Anhang L. 2a Die Mittel des Betriebssystems müssen eingesetzt werden, um zu verhindern, dass genehmigte Software durch nicht genehmigte Software mithilfe des Betriebssystems ersetzt wird (siehe auch U3). Für autorisierten Softwaredownload siehe Anhang D. 2b Der Massenspeicher, in dem die relevanten Daten, Konfigurationsdateien, Programme und Parameter aufbewahrt werden, muss vor Austausch geschützt sein. 3. Es müssen Maßnahmen ergriffen werden, um rechtlich relevante Software vor Änderungen mithilfe des Betriebssystems oder anderer einfach verfügbarer und handhabbarer gebräuchlicher Tools zu schützen (siehe auch U3). 4. Die Teile und Funktionen des Betriebssystems, die den		**Erläuterungen** 1. Das Schutzniveau sollte demjenigen des elektronischen Zahlungsverkehrs entsprechen. Generell ist ein Universalcomputer nur mit zusätzlicher Sicherungshardware für diese Risikoklasse geeignet.

Schutz des Messsystems realisieren, müssen als rechtlich relevante Software betrachtet und als solche geschützt werden.	
Erforderliche Dokumentation Die Dokumentation muss darlegen, wie sichergestellt ist, dass rechtlich relevante Software nicht unzulässig verändert wird.	**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die getroffenen Schutzmaßnahmen sind anzugeben.
Validierungsanleitung Fall 1: Geschlossene Benutzeroberfläche der rechtlich relevanten Software. *Auf Basis der Dokumentation ist zu überprüfen* • ob die Softwaremodule automatisch booten, • ob der Benutzer keinen Zugriff auf das PC-Betriebssystem hat, • ob der Benutzer keinen Zugriff auf andere Software als die zugelassene hat, • ob eine schriftliche Erklärung vorliegt, dass es keine versteckten Funktionen zum Umgehen der geschlossenen Benutzeroberfläche gibt. Fall 2: Betriebssystem und / oder Software mit Benutzerzugang. *Auf Basis der Dokumentation ist zu überprüfen* • ob die Prüfsumme über den Maschinencode der Softwaremodule erzeugt wird. Rechtlich relevante Software darf nicht gestartet werden können, wenn der Code verfälscht wurde.	**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.
Beispiel einer akzeptablen Lösung • Programmcode und Daten können mittels Prüfsummen geschützt werden. 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. • Für den Algorithmus muss eine Schlüssellänge von mindestens 2 Byte verwendet werden; eine CRC-16-Prüfsumme mit einem geheimen Startvektor (im ausführbaren Code verborgen) ist ausreichend (siehe auch Anhänge L und T). • Eine unerlaubte Veränderung der rechtlich relevanten Software kann über die Zugriffskontrolle oder die Datenschutzattribute des Betriebssystems verhindert werden. Die Administrierungsebene dieser Systeme muss durch Versiegelung oder ein gleichwertiges Mittel gesichert werden. • Der Zugang als Administrator wird a) für alle gesperrt oder b) nur nach den Regelungen der nationalen Marktüberwachungsgesetze autorisierten Personen gewährt. Lösung a) automatisches Generieren eines unbekannten, zufälligen Passwortes. Änderung der rechtlich relevanten Konfiguration nur möglich mittels Durchführung eines Betriebssystem-Setups. Lösung b) Passwort durch eine autorisierte Person ausgewählt und in einem Umschlag oder in / an dem Gehäuse verborgen und versiegelt. • Ein Umgehen der Schutzmaßnahmen des Betriebssys-	**Beispiel einer akzeptablen Lösung** • Programmcode kann durch die Speicherung der rechtlich relevanten Software in einer geeigneten Einsteckeinheit gesichert werden, die versiegelt ist. Die Einsteckeinheit kann z.B. ein Read-Only-Speicher oder ein Mikrocontroller sein.

tems durch direktes Schreiben auf den Massenspeicher oder dessen Austausch wird durch Versiegelung verhindert.	

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich für die Risikoklassen B und C erforderlich ist): Quellcode des Gerätes.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): *Auf Basis des Quellcodes ist zu überprüfen* • die Kommunikation mit der zusätzlichen Sicherungshardware, • ob Programm- oder Datenänderungen erkannt werden und in diesem Fall die Programmausführung stoppt.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
U7: Parameterschutz *Rechtlich relevante Parameter müssen gegen unbefugte Änderung gesichert werden.*		
Erläuterungen 1. Bauartspezifische Parameter sind für jedes Exemplar der Bauart identisch und sind im allgemeinen Teil des Programmcodes, d.h. Teil der rechtlich relevanten Software. Daher gilt für sie Anforderung U6. 2. Gerätespezifische Parameter: • "gesicherte" Parameter dürfen jederzeit mittels einer On-Board-Tastatur oder eines Schalters oder über Schnittstellen geändert werden, jedoch nur *vor* der Sicherungsaktion. Da gerätespezifische Parameter auf Universalcomputer unter Benutzung einfacher Werkzeuge manipuliert werden können, dürfen die Parameter nicht in Standardspeichern eines Universalcomputers gehalten werden. Das Speichern dieser Parameter ist nur in zusätzlicher Hardware erlaubt. • Frei setzbare gerätespezifische Parameter dürfen nach dem Sichern geändert werden.		
Erforderliche Dokumentation Die Dokumentation muss alle rechtlich relevanten Parameter beschreiben, ihre Wertebereiche und Sollwerte, wo sie gespeichert sind, wie sie inspiziert werden können und wie und wann sie gesichert werden (d.h. vor oder nach der Eichung).		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die für die Parameter getroffenen Schutzmaßnahmen sind anzugeben.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob die Schutzmethode für gerätespezifische Parameter angemessen ist, • ob kein gerätespezifischer Parameter in den Standardspeichern des Universalcomputers gespeichert ist, sondern alle Parameter auf separater Hardware, die versiegelt und schreibgeschützt werden kann, gespeichert sind. *Funktionsprüfungen:* • Überprüfen des Justierungs-/(Konfigurations-)Modus und Prüfen, ob das Sperren nach der Sicherung funktioniert. • Prüfen der Klassifizierung und des Zustands der Parameter (gesichert/setzbar) am Display des Messgerätes, wenn ein entsprechender Menüpunkt verfügbar ist. Die Konformitäts- oder Baumusterprüfbescheinigung muss auflisten, welche Parameter setzbar und wo sie zu finden sind.		**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.
Beispiel einer akzeptablen Lösung • 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 Schreibschutzschalters im Schutzzustand unterbunden. Änderungsprotokolle sind in Kombination mit Sicherungshardware möglich (siehe P7).
- Setzbare Parameter sind auf einem Standardspeicher des Universalcomputers gespeichert.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich für die Risikoklassen B und C erforderlich ist): Quellcode des Gerätes
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): *Auf Basis des Quellcodes ist zu überprüfen* • ob die Maßnahmen für den Schutz der Parameter korrekt implementiert und angemessen sind.

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">U8: Softwareauthentizität und Darstellung der Ergebnisse
Es müssen Mittel zur Gewährleistung der Authentizität der rechtlich relevanten Software eingesetzt werden. Die Authentizität der dargestellten Ergebnisse muss garantiert werden.</td></tr>
<tr><td colspan="2">Erläuterungen
1. Es darf nicht möglich sein, zugelassene rechtlich relevante Software mit den Funktionen des Betriebssystems oder anderer einfach erreichbarer und gebräuchlicher Werkzeuge betrügerisch nachzuahmen (vorzutäuschen).
2. Dargestellte Ergebnisse können als authentisch akzeptiert werden, wenn die Darstellung von der rechtlich relevanten Software generiert wird.</td><td>Erläuterungen
1. Einschränkung hinsichtlich BC 1 und 2: Es sind Mittel zum Schutz vor vorsätzlichem Missbrauch einschließlich auf Zusatzhardware basierender Simulation. erforderlich</td></tr>
<tr><td colspan="3">3. Dargestellte Messwerte müssen nachvollziehbar sein und von allen notwendigen Informationen begleitet werden, um Verwechslungen mit anderen (rechtlich nicht relevanten) Informationen zu vermeiden.
4. Unter Berücksichtigung der Mittel des Betriebssystems muss durch technische Maßnahmen sichergestellt werden, dass auf dem Universalcomputer nur die für den rechtlich relevanten Zweck zugelassene Software ausgeführt werden kann (z.B. darf ein Sensor nur gemeinsam mit dem zugelassenen Programm arbeiten).
5. Durch technische Mittel muss sichergestellt werden, dass die rechtlich relevante Software ihre Integrität und Authentizität in regelmäßigen Abständen (Zeitintervallen) während ihrer Ausführung überprüft.</td></tr>
<tr><td colspan="2">Erforderliche Dokumentation
Die Dokumentation muss beschreiben, wie die Authentizität der Software gewährleistet wird.</td><td>Erforderliche Dokumentation (Zusätzliche Dokumentation zu denen von Risikoklasse B und C)
Die getroffenen Schutzmaßnahmen sind anzugeben.</td></tr>
<tr><td colspan="2">Validierungsanleitung
Auf Basis der Dokumentation ist zu überprüfen
• ob die Darstellung von der rechtlich relevanten Software erzeugt wird und wie eine Manipulation von rechtlich nicht relevanten Programmen verhindert werden kann,
• ob die rechtlich relevanten Aufgaben nur durch die zugelassene rechtlich relevante Software realisiert werden.
Funktionsprüfungen:
• Überprüfen durch Sichtkontrolle, ob die Ergebnisdarstellung leicht unterscheidbar von anderen, möglicherweise auch dargestellten Informationen ist.</td><td>Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C)
Auf Basis der Dokumentation ist zu überprüfen
• ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.</td></tr>
</table>

• Überprüfen der Vollständigkeit der dargestellten Informationen gemäß Dokumentation.	

Beispiel einer akzeptablen Lösung

Formale Mittel:

1. Der von der Software angezeigte Softwareidentifikationsteil A (Prüfsumme, Versionsnummer oder TEC-Nummer, siehe U2) wird mit dem gewünschten Wert in der Baumusterprüfbescheinigung verglichen.

Technische Mittel:

1. Das Fenster, das die Messwerte anzeigt, wird von der rechtlich relevanten Software erzeugt. Die für das Fenster nötigen technischen Maßnahmen sind:
   - Die rechtlich nicht relevanten Programme erhalten keinen Zugriff auf die Messwerte, bis die diese angezeigt wurden.
   - Das Fenster wird periodisch aktualisiert. Das zugehörige Programm überprüft, ob es das oberste angezeigte Fenster ist und es dem Benutzer unmöglich ist, das Fenster zu schließen oder es aus dem Sichtbereich zu schieben, solange die Messung nicht abgeschlossen ist.
   - Die Messwertverarbeitung hält an, wenn dieses Fenster geschlossen wird oder nicht vollständig sichtbar ist.

Die Bedienungsanleitung (und TEC) muss zu Referenzzwecken eine Abbildung der Fenster enthalten.

2a Die Sensoreinheit verschlüsselt die Messwerte mit einem Schlüssel, der auf dem Universalcomputer nur der zugelassenen Software bekannt ist (z.B. ihre Versions- oder Identifikationsnummer). 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 kann gewählt sowie der Sensoreinheit und der Software auf dem Universalcomputer ohne Zerstörung eines Siegels übergeben werden.	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, muss der neue Schlüssel in die Sensoreinheit eingegeben und diese versiegelt werden.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Dokumentation, die zusätzlich für die Risikoklassen B und C erforderlich ist):

Quellcode der rechtlich relevanten Software.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C):

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 Authentizität der Software zu gewährleisten (z.B. dass rechtlich relevante Aufgaben nur von der zugelassenen, rechtlich relevanten Software ausgeführt werden).

Risikoklasse B	Risikoklasse C	Risikoklasse D
U9: Einfluss anderer Software		
Die rechtlich relevante Software muss so aufgebaut sein, dass andere Software sie nicht unzulässig beeinflusst.		
Erläuterungen		

1. Die Softwaretrennung zwischen der rechtlich relevanten und der rechtlich nicht relevante 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. 2. Moderne Betriebssysteme erlauben es, einen Softwareteil sehr effizient von anderen abzuschotten. Das Betriebssystem muss so restriktiv wie möglich für den beabsichtigten Messzweck konfiguriert werden. Nicht benötigte Funktionen müssen deaktiviert oder deinstalliert werden. Die Konfigurationsdateien und -skripte des Betriebssystems, welche die Trennung realisieren, müssen vor Änderung geschützt werden.
Erforderliche Dokumentation Siehe Anhang S
Validierungsanleitung Siehe Anhang S
Beispiel einer akzeptablen Lösung Siehe Anhang S

6 Anhang L: Langzeitspeicherung von Messdaten

Dies ist ein 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 Universalrechner (Typ-U-Anforderungen). Er beschreibt die Anforderungen an die Speicherung von Messdaten von dem Zeitpunkt an, an dem eine Messung physisch abgeschlossen ist, bis zu dem Zeitpunkt, an dem alle durch die rechtlich relevante Software zu erledigenden Prozesse beendet sind. Er kann ebenso auf die Datenlangzeitspeicherung danach angewendet werden.

6.1 Technische Beschreibung

Der Satz von Anforderungen dieses Anhangs wird nur dann angewendet, wenn eine Langzeitspeicherung von Messdaten durchgeführt wird. Er betrifft nur rechtlich relevante Messdaten. 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, wie 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 Universalrechner 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.

Integrierte Speicher Einfaches Gerät, zweckgebunden, keine von außen anwendbare Werkzeuge oder Mittel für Bearbeitung oder Ändern von Daten verfügbar, integrierter Speicher für Messdaten oder Parameter, z.B. RAM, Flash-Speicher, Festplatte.
Speicher des Universalcomputers Universalcomputer, grafische Benutzeroberfläche, Multitasking-Betriebssystem, Aufgaben unter rechtlicher Kontrolle und nicht unter rechtlicher Kontrolle bestehen parallel; der Speicher kann aus dem Gerät entfernt werden oder Inhalte können überall innerhalb oder außerhalb des Computers kopiert werden.
Wechseldatenträger oder entfernte (externe) Speicherung Freies Grundgerät (zweckgebundenes Gerät oder Universalcomputer); der Speicher kann aus dem Gerät genommen werden. Dies können beispielsweise Disketten, Flash-Karten oder entfernte, über das Netzwerk angeschlossene Datenbanken sein.

Tabelle 6-1: Technische Beschreibung der Langzeitspeicherung

6.2 Spezifische Softwareanforderungen an die Langzeitspeicherung

Die Anforderungen in diesem Kapitel gelten zusätzlich zum Anforderungssatz entweder für Messgeräte mit zweckgebundener Hard- und Software oder für Messgeräte mit Universalrechner.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
L1: Vollständigkeit der gespeichert Messdaten *Die gespeicherten Messdaten müssen alle relevanten Informationen enthalten, die zur Rekonstruktion einer früheren Messung nötig sind.*		
Erläuterungen 1. Die gespeicherten Messdaten können zu einem späteren Zeitpunkt zum Nachweis erforderlich sein, z.B. zum Überprüfen von Rechnungen. Alle aus rechtlichen und messtechnischen Gründen notwendigen Daten müssen zusammen mit dem Messwert gespeichert werden.		
Erforderliche Dokumentation Beschreibung aller Felder der Datensätze.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob alle für die relevanten rechtlichen und messtechnischen 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 - rechtlich korrekte Maßeinheit - Preis je Einheit oder zu zahlender Preis (falls zutreffend) - Ort und Zeitpunkt der Messung (falls zutreffend) - Identifikation des Gerätes, falls zutreffend (externe Speicherung) • 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 (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode, der die Datensätze zu Speicherung erzeugt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): *Auf Basis des Quellcodes ist zu überprüfen* • ob die Datensätze korrekt aufgebaut sind.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
L2: Schutz vor zufälliger oder unbeabsichtigter Änderung *Die gespeicherten Messdaten müssen vor zufälliger oder unbeabsichtigter Änderung geschützt sein.*		
Erläuterungen 1. Zufällige Datenänderung kann durch physikalische Effekte verursacht werden. 2. Unbeabsichtigte Änderungen werden durch den Benutzer des Gerätes verursacht. Im Rahmen der Bereinigung von Daten kann es erforderlich sein, dass Daten von Zeit zu Zeit gelöscht werden, die zu bezahlten oder abgelaufenen Rechnungen gehören. Automatische oder halbautomatische Mittel müssen zur Absicherung eingesetzt werden, dass nur bestimmte Daten gelöscht werden, und dass das versehentliche Löschen von noch gültigen Daten verhindert wird. Dies ist besonders bei vernetzten Systemen und abgesetzten Speichern oder Wechseldatenträgern wichtig, wo der Verwender die Bedeutung		

der Daten evtl. nicht erkennt.

3. Vom Empfänger muss eine Prüfsumme berechnet und mit dem beigefügten Sollwert verglichen werden. Wenn die Werte übereinstimmen, ist der Datensatz gültig und kann verwendet werden, andernfalls muss er gelöscht oder als ungültig markiert werden.

Erforderliche Dokumentation Beschreibung der Schutzmittel (z.B. der Prüfsummenalgorithmus einschließlich der Länge des Erzeugungspolynoms).	**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die Dokumentation muss die Maßnahmen aufzeigen, die zur Validierung der Schutzwirksamkeit getroffen wurden.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob eine Prüfsumme über die Daten erzeugt wird, • ob die rechtlich relevante Software, die die Daten liest und eine Prüfsumme berechnet, wirklich den berechneten Wert mit dem Sollwert vergleicht, • ob die Daten nicht vor Ende des Datenspeicherungszeitraumes, der vom Hersteller vorgesehen und dokumentiert ist, überschrieben werden können • ob eine Warnung an den Benutzer ausgegeben wird, wenn er im Begriff ist, Messwertdateien zu löschen. *Funktionsprüfungen:* • Überprüfen durch geeignete Stichproben, ob vor dem Löschen von Messdaten – sofern das Löschen überhaupt möglich ist - eine Warnung erfolgt.	**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen

Beispiel einer akzeptablen Lösung

- 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.

  Hinweis: Der Algorithmus ist nicht geheim, im Gegensatz zu Anforderung L3 ist weder der Startvektor des CRC-Registers noch das Erzeugungspolynom, d.h. der Divisor im Algorithmus, geheim. Startvektor und Erzeugungspolynom sind sowohl dem Programm bekannt, das die Prüfsummen erzeugt als auch dem, das sie überprüft.
- Messdaten bzw. Rechnungsdateien können durch das Anbringen eines automatischen Zeitstempels bei der Erzeugung und eines Kennzeichens, ob die Rechnung bezahlt oder unbezahlt ist, geschützt werden. Ein Dienstprogramm löscht oder verschiebt Dateien nur, wenn die Rechnung bezahlt oder die Aufbewahrungsfrist abgelaufen sind.
- Messdaten werden nicht ohne vorherige Bestätigung gelöscht, z.B. eine Dialoganweisung oder ein Fenster mit der Bitte um Löschbestätigung.
- Messdaten dürfen automatisch überschrieben werden, wenn ein angemessener Schutz der aufzubewahrenden Aufzeichnungen vorhanden ist. Über einen Parameter wird die Anzahl der Tage festlegt, ehe die Messdaten entsprechend der Nutzungsbedingungen und der Datenspeichergröße gelöscht werden können; dieser Parameter wird beim In-Verkehr-bringen gesichert. Das Gerät muss anhalten, wenn der Speicher voll ist und keine Datensätze vorhanden sind, die alt genug zum Überschreiben sind. In diesem Fall kann manuelle Löschen (mit vorheriger Genehmigung) durchgeführt werden. In Fällen, in denen die Messung nicht unterbrechbar ist (z.B. Zähler), muss der Speicher so groß sein, dass eine Unterbrechung wegen mangelndem Speicherplatz vermieden wird.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist)

Quellcode, der den Schutz der gespeicherten Daten umsetzt.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): *Auf Basis des Quellcodes ist zu überprüfen* • ob die zum Schutz der gespeicherten Daten getroffenen Maßnahmen angemessen und korrekt umgesetzt wurden.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
L3: Datenintegrität *Die gespeicherten Messdaten müssen vor vorsätzlicher Änderung geschützt sein.*		
Erläuterungen 1. Diese Anforderung gilt für alle Speichertypen außer integrierten Speichern.		
2. Der Schutz muss gegen vorsätzliche Änderungen wirksam sein, die durch einfache gebräuchliche Softwaretools ausgeführt werden. 3. Einfache gebräuchliche Softwaretools sind Werkzeuge, die leicht verfügbar und handhabbar sind, wie z.B. Office-Pakete.		2. Der Schutz muss gegen vorsätzliche Änderungen wirksam sein, die durch spezielle, anspruchsvolle Softwaretools ausgeführt werden. 3. "Anspruchsvolle Softwaretools" sind z.B. Debugger, Recompiler, Softwareentwicklungstools usw. 4. Das Schutzniveau muss dem im elektronischen Zahlungsverkehr äquivalent sein. 5. Der Schutz wird durch eine elektronische Signatur mit einem Algorithmus umgesetzt, der garantiert, dass bei verschiedenen Datensätzen keine identische Signatur auftritt. <u>Hinweis:</u> Auch wenn Algorithmus und Schlüssel das hohe Niveau erfüllen, erreicht eine technische Lösung mit einem Standard-PC das Schutzniveau **nicht**, sofern es nicht geeignete Schutzmaßnahmen für die Programme gibt, die einen Datensatz signieren oder überprüfen (siehe Basisleitfaden U, Kommentar auf Anforderung U6-Risikoklasse D).
Erforderliche Dokumentation Die Umsetzungsmethode des Schutzes muss dokumentiert werden.		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die getroffenen Schutzmaßnahmen müssen aufgezeigt werden.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen*		**Validierungsanleitung** (zusätzlich zur Anleitung für Ri-

• ob bei Verwendung einer Prüfsumme oder einer Signatur: - die Prüfsumme oder Signatur über den gesamten Datensatz erzeugt wird, - die rechtlich relevante Software, welche die Daten liest und eine Prüfsumme berechnet oder eine Signatur entschlüsselt, wirklich den berechneten Wert mit dem Sollwerte vergleicht. • ob geheime Daten (z.B. Schlüsselinitialwert, falls verwendet) gegen das Ausspähen mit einfachen Werkzeugen geheim gehalten werden. *Funktionsprüfungen:* • Überprüfen, ob ein gefälschter Datensatz durch das Verifikationsprogramm abgelehnt wird.	sikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.
Beispiel einer akzeptablen Lösung Vor Wiederverwendung der Daten wird der Prüfsummenwert neu berechnet und mit dem gespeicherten Sollwert verglichen. 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. Hinweis: Der Algorithmus ist nicht geheim, aber im Gegensatz zu Anforderung **L2** muss es der Startvektor des CRC-Registers oder das Erzeugungspolynom (d.h. der Divisor im Algorithmus) sein. Der Startvektor oder das Erzeugungspolynom sind nur den Programmen bekannt, welche die Prüfsummen erzeugen und überprüfen. Sie müssen wie Schlüssel behandelt werden (siehe **L5**).	**Beispiel einer akzeptablen Lösung** Anstelle des CRC wird eine Signatur berechnet. Ein geeigneter Signaturalgorithmus wäre ein Hashalgorithmus, wie z.B. SHA-1 oder RipeMD160, in Verbindung mit einem Verschlüsselungsalgorithmus wie RSA oder Elliptischen Kurven. Die minimale Schlüssellänge ist 768 Bit (RSA) oder 128-160 Bits (EK).

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode, der die Integrität der gespeicherten Daten umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): *Auf Basis des Quellcodes ist zu überprüfen* • ob die zur Integritätsgarantie getroffenen Maßnahmen angemessen und korrekt implementiert sind.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
L4: Authentizität der gespeicherten Messdaten *Die gespeicherten Messdaten müssen authentisch auf die Messung rückführbar sein, bei der sie erzeugt wurden.*		
Erläuterungen 1. Die Authentizität der Messdaten kann zu einem späteren Zeitpunkt als Referenz benötigt werden, z.B. zur Rechnungsüberprüfung. 2. Authentizität erfordert die korrekte Zuordnung (Verknüpfung) von Messdaten zu der Messung, bei der die Daten erzeugt wurden. 3. Authentizität setzt eine Datensatzidentifikation voraus. 4. Eine Verschlüsselung der Messdaten ist zur Sicherstellung der Authentizität nicht unbedingt erforderlich.		
Erforderliche Dokumentation Beschreibung des zur Gewährleistung der Authentizität verwendeten Verfahrens.		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die getroffenen Schutzmaßnahmen müssen aufgezeigt

	werden.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • 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 und auf dem Beleg oder der Rechnung gedruckten Daten identisch sind.	**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.
Beispiel einer akzeptablen Lösung Ein gespeicherter Datensatz enthält die folgenden Datenfelder (zusätzlich zu den in L3 definierten Feldern): • Eine eindeutige (fortlaufende) Identifikationsnummer. Die Identifikationsnummer wird auch auf den Lieferschein übertragen. • Zeitpunkt, an dem die Messung durchgeführt wurde (Zeitstempel). Der Zeitstempel wird auch auf den Lieferschein übertragen. • Eine Identifikation des Messgerätes, das den Wert erzeugt hat. • Eine Signatur, die für die Gewährleistung der Datenintegrität verwendet wird und gleichzeitig für die Gewährleistung der Authentizität verwendet werden kann. Die Signatur umfasst alle Datensatzfelder. Siehe Anforderung L2, L3. • 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, bewiesen.	

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

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
L5: Geheimhaltung der Schlüssel *Schlüssel und zugehörige Informationen müssen wie rechtlich relevante Daten behandelt, geheim gehalten und vor Gefährdung durch Softwaretools geschützt werden*		
Erläuterungen 1. Diese Anforderung gilt nur, wenn ein geheimer Schlüssel verwendet wird. 2. Diese Anforderung gilt für die Messdatenspeicher, die sich außerhalb des Messgerätes befinden oder auf Universalcomputern umgesetzt sind. 3. Der Schutz muss gegen vorsätzliche Änderungen wirksam sein, die durch einfache gebräuchliche Softwaretools ausgeführt werden. 4. Wenn der Zugang zu dem geheimen Schlüssel verhindert wird, z.B. durch Versiegeln des Gehäuses eines Messge-		**Erläuterungen** 1. Diese Anforderung gilt für Speicher in Universalcomputern und für externe Speicher. 2. Der Schutz muss gegen vorsätzliche Änderungen wirksam sein, die durch spezielle, anspruchsvolle Softwaretools ausgeführt werden.

rätes mit zweckgebundener Hard- und Software, sind keine zusätzlichen Softwareschutzmaßnahmen erforderlich	3. Geeignete, dem elektronischen Zahlungsverkehr gleichwertige Methoden müssen verwendet werden. Der Benutzer muss in der Lage sein, die Authentizität des öffentlichen Schlüssels überprüfen zu können.
Erforderliche Dokumentation Beschreibung des Schlüsselmanagements und der Maßnahmen zur Geheimhaltung der Schlüssel und der zugehörige Informationen	**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die getroffenen Schutzmaßnahmen müssen aufgezeigt werden.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob die geheimen Informationen nicht gefährdet werden können.	**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau 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 Daten. Wenn der CRC-Algorithmus an Stelle einer Signatur verwendet wird, spielen der Startvektor oder das Erzeugungspolynom 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. <u>Hinweis:</u> 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). 1) *Public-Key*-Infrastruktur: Der öffentliche Schlüssel des unter gesetzlicher Kontrolle stehenden Speichers wurde von einem akkreditierten Trust Center zertifiziert. 2) *Direct Trust*: Es ist nicht notwendig, ein Trust-Center einzubeziehen, wenn nach vorheriger Vereinbarung beide Parteien in der

	Lage sind, den öffentlichen Schlüssel des Messgerätes direkt an dem unter gesetzlicher Kontrolle stehenden Gerät abzulesen, das den betreffenden Datensatz erzeugt.[3]

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode, der das Schlüsselmanagement umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): *Auf Basis des Quellcodes ist zu überprüfen* • ob die für das Schlüsselmanagement getroffenen Maßnahmen angemessen sind.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
L6: Abrufen von gespeicherten Daten *Die Software zum Nachprüfung der gespeicherten Messdatensätze muss die Daten anzeigen oder ausdrucken, die Daten auf Veränderungen überprüfen und warnen, wenn eine Änderung stattgefunden hat. Daten, die als beschädigt erkannt wurden, dürfen nicht verwendet werden.*		
Erläuterungen 1. Die gespeicherten Messdaten können zu einem späteren Zeitpunkt benötigt werden, z.B. bei Überprüfung von Transaktionen. Wenn es Zweifel an der Richtigkeit eines Lieferscheines / Beleges gibt, muss es möglich sein, die gespeicherten Messdaten der fraglichen Messung eindeutig zu identifizieren (siehe auch L1, L3, L4 und L5). 2. Die Identifikationsnummer (siehe L1) muss zusammen mit einer Erklärung und einem Verweis auf die Speicherung, die der gesetzlichen Kontrolle unterliegt, für den Kunden auf den Lieferschein oder Beleg gedruckt werden. 3. Verifikation bedeutet die Überprüfung der Integrität, Authentizität und richtigen Zuordnung der gespeicherten Messdaten. 4. Die Verifikationssoftware für Anzeige oder Druck der gespeicherten Daten unterliegt der gesetzlichen Kontrolle. 5. Zu gerätespezifischen Anforderungen siehe Anhang I.		
Erforderliche Dokumentation • Beschreibung der Funktionen des Abfrageprogramms, • Beschreibung der Aufdeckung von Datenverfälschungen, • Betriebsanleitung für dieses Programm.		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die getroffenen Schutzmaßnahmen müssen aufgezeigt werden.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob Verifikationssoftware wirklich die berechneten mit den Sollwerten vergleicht. • ob die Verifikationssoftware Teil der rechtlich relevanten Software ist. *Funktionsprüfungen:* • Überprüfen, ob das Programm verfälschte Datensätze erkennt.		**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.

[3] Fehler im Original, hier korrigiert: Der öffentliche Schlüssel muss nicht am empfangenden Gerät, sondern am signierenden angezeigt werden können.

• Durchführung von Stichprobenüberprüfungen um zu prüfen, ob das Verifikationsprogramm alle erforderlichen Informationen liefert.	

Beispiel einer akzeptablen Lösung
Der Datensatz wird durch das Überprüfungsprogramm aus dem Speicher gelesen und die Signatur über alle Datenfelder wird neu berechnet und mit dem gespeicherten Sollwert verglichen. Wenn beide Werte übereinstimmen, ist der Datensatz korrekt, sonst werden die Daten nicht verwendet und durch das Programm gelöscht oder als ungültig markiert.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist)
Quellcode des Abfrageprogramms.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D):
Auf Basis des Quellcodes ist zu überprüfen

- ob getroffene Maßnahmen für Abfrage, Signaturüberprüfung usw. angemessen und richtig umgesetzt sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D

L7: Automatisches Speichern

Die Messdaten müssen automatisch gespeichert werden, wenn die Messung abgeschlossen ist.

Erläuterungen

1. Diese Anforderung gilt für alle Speichertypen.
2. Diese Anforderung bedeutet, dass die Speicherungsfunktion nicht von einer Bedienerentscheidung abhängt. Trotzdem ist bei einigen Gerätearten, z.B. Waagen, eine Entscheidung oder ein Befehl des Bedieners erforderlich, ob das Ergebnis anzunehmen ist oder nicht. Mit anderen Worten, es kann einige Zwischenmessungen geben, die nicht gespeichert werden (z.B. beim Laden oder ehe die verlangte Warenmenge auf dem Lastträger ist). Doch selbst in diesem Fall, wird das Ergebnis automatisch gespeichert, wenn der Bediener das Ergebnis annimmt.
3. Für den Fall der vollständigen Speicherung siehe Anforderung L8.

Erforderliche Dokumentation
Bestätigung, dass das Speichern automatisch ausgeführt wird. Beschreibung der graphischen Benutzeroberfläche.

Validierungsanleitung
Funktionsprüfungen:
Stichprobenkontrollen, ob die Messwerte nach der Messung oder nach Akzeptieren des Messungsabschlusses automatisch gespeichert werden. Überprüfen, ob es keine Tasten oder Menüpunkte zum Unterbrechen oder Deaktivieren der automatischen Speicherung gibt.

Beispiel einer akzeptablen Lösung
In der grafischen Benutzeroberfläche (GUI) gibt es keinen Menüpunkt oder Button, der ein manuelles Speichern 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 Billigung der Messung gespeichert.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist)
Quellcode des Gerätes

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D):
Auf Basis des Quellcodes ist zu überprüfen

- ob die für die automatische Speicherung getroffenen Maßnahmen angemessen und korrekt umgesetzt sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D

L8: Speicherkapazität und -dauer

Der Langzeitspeicher muss eine Kapazität besitzen, die für den beabsichtigten Zweck ausreichend ist.

Erläuterungen

1. Wenn ein Speicher voll oder vom Gerät getrennt wird, muss eine Warnung an den Bediener gegeben werden. Eine Warnung ist nicht erforderlich, wenn durch die Konstruktion gewährleistet ist, dass nur abgelaufene Daten überschrieben werden können. Für weitere notwendige Maßnahmen siehe messgerätespezifische Anforderungen (Anhang I).
2. Die Regelung hinsichtlich des Mindestzeitraumes für die Speicherung von Messdaten liegt außerhalb des Anwendungsbereiches dieser Anforderung und ist nationalen Regelungen überlassen. Es liegt in der Verantwortung des Eigentümers, ein Instrument mit genügend Speicherkapazität zu verwenden, um die für seine Arbeit zutreffenden Anforderungen zu erfüllen. Die benannte Stelle für die EC-Konformitätsbewertung/Baumusterprüfung prüft nur, ob die Daten korrekt gespeichert und abgerufen werden und ob neue Vorgänge verhindert werden, wenn der Speicher voll ist.
3. Ebenso liegt es außerhalb des Anwendungsbereiches dieser Anforderung, bestimmte Beschriftungen auf dem Gerät hinsichtlich Speicherkapazität oder anderer begleitender Informationen zu fordern, die das Berechnen der Kapazität gestatten. Jedoch muss der Hersteller Informationen über die Kapazität zur Verfügung stellen.

Erforderliche Dokumentation

Beschreibung zum Umgang mit Ausnahmefällen bei der Messwertspeicherung.

Validierungsanleitung

Auf Basis der Dokumentation ist zu überprüfen

- ob die Speicherkapazität oder eine Berechnungsformel vom Hersteller angegeben wird.
- ob das Überschreiben von Daten nicht vor Ende des Datenspeicherungszeitraumes eintreten kann, der durch den Hersteller vorgesehen und dokumentiert ist.

Funktionsprüfungen:

- ob eine Warnung an den Benutzer ausgegeben wird, wenn er im Begriff ist, Messwertdateien zu löschen (sofern das Löschen überhaupt möglich ist),
- ob eine Warnung ausgegeben wird, wenn der Speicher voll ist oder entfernt wurde.

Beispiel einer akzeptablen Lösung

- Für unterbrechbare Messungen, die einfach und schnell unterbrochen werden können, wie z.B. Wägen, Kraftstoffmessung usw., kann die Messung abgeschlossen werden, auch wenn der Speicher nicht mehr verfügbar ist. Das Messgerät oder das Teilgerät muss einen Puffer besitzen, der groß genug zur Speicherung des aktuellen Vorgangs ist. Danach kann ein neuer Messvorgang begonnen werden und die gepufferten Werte werden zur späteren Übertragung in einen neu eingesetzten Speicher aufbewahrt.
- Messungen, die nicht unterbrechbar sind, wie z.B. Messung von Energie, Volumen usw., benötigen keine besonderen Zwischenpuffer, da diese Messungen immer kumulativ sind. Die kumulativen Register können zu einem späteren Zeitpunkt, wenn der Speicher wieder verfügbar ist, ausgelesen und übertragen werden.
- Messdaten können von einem Dienstprogramm automatisch überschrieben werden, das überprüft, ob die Messdaten abgelaufen sind (entsprechend den nationalen Regelungen für den relevanten Zeitraum) oder die Rechnung bezahlt wurde. Das Dienstprogramm muss die Löscherlaubnis vom Benutzer fordern, und die Daten werden in der Reihenfolge „älteste zuerst“ gelöscht.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist)

Quellcode, der die Datenspeicherung umsetzt.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D):

Auf Basis des Quellcodes ist zu überprüfen

- ob die für die automatische Speicherung getroffenen Maßnahmen angemessen und korrekt umgesetzt sind.

7 Anhang T: Messdatenübertragung über Kommunikationsnetze

Dieser Anhang ist eine Erweiterung der Grundleitfäden P und U. Er muss nur benutzt werden, wenn Messdaten über Kommunikationsnetze zu einem entfernten Gerät übertragen werden, wo sie für rechtlich geregelte Zwecke weiter verarbeitet und/oder verwendet werden. Dieser Anhang gilt nicht, wenn es keine nachträgliche Verarbeitung rechtlich relevanter Daten gibt. Wenn Software auf ein Gerät heruntergeladen wird, das der gesetzlichen Kontrolle unterliegt, gelten die Anforderungen des Anhangs D.

7.1 Technische Beschreibung

Der Satz von Anforderungen dieses Anhangs wird nur dann angewendet, wenn das betrachtete Gerät mit einem Netz verbunden ist und rechtlich relevante Messdaten sendet oder empfängt. In der folgenden Tabelle sind drei Netzkonfigurationen aufgezeigt. Die einfachste besteht aus einer Anzahl von Geräten, die alle der gesetzlichen Kontrolle unterliegen. Die Teilnehmer werden bei der Verifikation beim In-Verkehr-bringen festgeschrieben. Eine Variante davon (geschlossenes Netz, teilweise unter gesetzliche Kontrolle), ist ein Netz mit Teilnehmern, die nicht alle der gesetzlichen Kontrolle unterliegen, aber alle bekannt sind und sich während des Betriebes nicht ändern. Ein offenes Netz hat keine Einschränkung hinsichtlich Identität, Funktionsweise, Anwesenheit und Standort der Teilnehmer.

Beschreibung von Konfigurationen
Geschlossenes Netz, vollständig unter gesetzlicher Kontrolle Nur eine feste Anzahl von Teilnehmern mit eindeutiger Identität, Funktionsweise und Standort sind verbunden. Alle Geräte unterliegen der gesetzlichen Kontrolle. Im Netz gibt es keine Geräte, die nicht der gesetzlichen Kontrolle unterliegen.
Geschlossenes Netz, zum Teil unter gesetzlicher Kontrolle Eine feste Anzahl von Teilnehmern mit eindeutiger Identität und Standort sind an das Netz angeschlossen. Nicht alle Geräte unterliegen der gesetzlichen Kontrolle und daher ist ihre Funktionsweise unbekannt.
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 IR- oder Funknetzwerkkommunikationsschnittstellen 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 *Die übertragenen Daten müssen alle relevanten Informationen enthalten, die zur Darstellung oder Weiterverarbeitung der Messergebnisse in der Empfangseinheit nötig sind.*		
Erläuterungen 1. Der messtechnische Teil eines übertragenen Datensatzes besteht aus einem oder mehreren Messwerten mit der richtigen Auflösung, der rechtlich korrekten Maßeinheit, abhängig von der Geräteanwendung dem Preis pro Einheit oder dem zu zahlenden Preis und dem Ort der Messung.		
Erforderliche Dokumentation Beschreibung aller Felder des Datensatzes		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • 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 pro Einheit oder zu zahlender Preis (falls zutreffend) • Datum und Uhrzeit der Messung (falls zutreffend) • Identifikation des Gerätes, falls zutreffend (Datenübertragung) • Ort der Messung (falls zutreffend)		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode, der die Datensätze zur Übertragung erzeugt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): *Auf Basis des Quellcodes ist zu überprüfen* • ob die Datensätze korrekt aufgebaut sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
T2: Schutz vor zufälliger oder unbeabsichtigter Änderung *Die übertragenen Daten müssen vor zufälliger oder unbeabsichtigter Änderung geschützt sein.*		
Erläuterungen 1. Zufällige Datenänderung kann durch physikalische Effekte verursacht werden. 2. Unbeabsichtigte Änderungen werden durch den Benutzer des Gerätes verursacht. 3. Es müssen Mittel zum Erkennen von Übertragungsfehlern vorhanden sein.		
Erforderliche Dokumentation Beschreibung des Prüfsummenalgorithmus, falls verwendet, einschließlich der Länge des Erzeugungspolynoms. Beschreibung eines alternativen Verfahrens, falls verwendet.		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die Dokumentation muss die Maßnahmen aufzeigen, die zur Validierung der Schutzwirksamkeit getroffen wurden.
Validierungsanleitung		**Validierungsanleitung** (zu-

Auf Basis der Dokumentation ist zu überprüfen • ob eine Prüfsumme über die Daten erzeugt wird, • ob die rechtlich relevante Software, welche die Daten empfängt, die Prüfsumme neu berechnet und sie mit dem im Datensatz enthaltenen Sollwert vergleicht.	sätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.
Beispiel einer akzeptablen Lösung • Zum Aufdecken von Datenänderungen wird mit dem CRC-16-Algorithmus eine Prüfsumme über 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. Hinweis: Der Algorithmus ist nicht geheim, und im Gegensatz zu Anforderung T3, sind es auch nicht der Startvektor des CRC-Registers und das Erzeugungspolynom, d.h. der Divisor im Algorithmus. Startvektor und Erzeugungspolynom sind gleichermaßen den Programmen bekannt, welche die Prüfsummen erzeugen und sie überprüfen. • Nutzung von Mitteln, die von den Übertragungsprotokollen, z.B. TCP/IP, IFSF, bereitgestellt werden.	

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode, der den Schutz der übertragenen Daten umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): *Auf Basis des Quellcodes ist zu überprüfen* • ob die zum Schutz der übertragenen Daten getroffenen Maßnahmen angemessen sind.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
T3: Datenintegrität *Die übertragenen rechtlich relevanten Daten müssen vor vorsätzlicher Änderung durch Softwaretools geschützt sein.*		
Erläuterungen 1. Diese Anforderung gilt nur für Netze, die offen sind oder zum Teil unter gesetzlicher Kontrolle stehen, nicht für geschlossene Netze. 2. Der Schutz muss gegen vorsätzliche Änderungen wirksam sein, die durch einfache gebräuchliche Softwaretools ausgeführt werden. 3. Einfache gebräuchliche Softwaretools sind Werkzeuge, die leicht verfügbar und handhabbar sind, wie z.B. Office-Pakete.		**Erläuterungen** 1. Diese Anforderung gilt für Netze, die offen sind oder zum Teil unter gesetzlicher Kontrolle stehen. 2. Der Schutz wird durch eine elektronische Signatur mit einem Algorithmus umgesetzt, der garantiert, dass keine gleichen Signaturen aus verschiedenen Datensätzen resultieren. 3. Der Schutz muss gegen vorsätzliche Änderungen wirken, die durch spezielle, anspruchsvolle Softwaretools ausgeführt werden. 4. "Anspruchsvolle Softwaretools" sind z.B. Debugger, Recompiler, Softwareentwicklungstools usw.

	5. Das Schutzniveau muss dem im elektronischen Zahlungsverkehr äquivalent sein. Hinweis: Auch wenn Algorithmus und Schlüssel das hohe Niveau erfüllen, setzt eine technische Lösung mit einem Standard-PC das Schutzniveau **nicht** um, sofern es nicht geeignete Schutzmaßnahmen für die Programme gibt, die den Datensatz signieren oder überprüfen (siehe Basisleitfaden U, Kommentar auf Anforderung U6-Risikoklasse D).
Erforderliche Dokumentation Beschreibung der Schutzmethode	**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die getroffenen Schutzmaßnahmen müssen aufgezeigt werden.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob bei Verwendung einer Prüfsumme oder einer Signatur: - die Prüfsumme oder Signatur über den gesamten Datensatz erzeugt wird, - die rechtlich relevante Software, welche die Daten empfängt, neu die Prüfsumme berechnet bzw. die Signatur entschlüsselt und sie mit dem im Datensatz enthaltenen Sollwerte 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) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.
Beispiel einer akzeptablen Lösung • Eine Prüfsumme von dem zu übertragenden Datensatz wird erzeugt. Vor der Wiederverwendung der Daten wird der Wert der Prüfsumme vom Empfänger neu berechnet und mit dem Sollwert, der im empfangenen Datensatz enthalten ist, verglichen. 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. Hinweis: Der Algorithmus ist nicht geheim, aber im Gegensatz zu Anforderung **T2** müssen der Startvektor des CRC-Registers oder das Erzeugungspolynom (d.h. der Divisor im Algorithmus) geheim sein. Der Startvektor und das Erzeugungspolynom sind nur den Programmen bekannt, welche die Prüfsummen erzeugen und überprüfen. Sie müssen wie Schlüssel behandelt werden (siehe **T5**).	**Beispiel einer akzeptablen Lösung** • Anstelle des CRC wird eine Signatur berechnet. Ein geeigneter Signaturalgorithmus wäre z.B. einer der Hashalgorithmen SHA-1 oder RipeMD160, in Verbindung mit einem Verschlüsselungsalgorithmus wie RSA oder Elliptischen Kurven. Die minimale Schlüssellänge ist 768 Bit (RSA) oder 128-160 Bit (EK). • Schutz ist durch einige Übertragungsprotokolle wie z.B. HTTPS gegeben.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode, der die Integrität der übertragenen Daten umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C): *Auf Basis des Quellcodes ist zu überprüfen* • ob die Maßnahmen angemessen sind, die zur Integritätsgarantie der übertragenen Daten getroffenen wurden.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
T4: Authentizität der übertragenen Daten *Dem die übertragenen Daten empfangenden Programm muss es möglich sein, die Authentizität und die Zuordnung der Messwerte zu einer bestimmten Messung zu überprüfen.*		
Erläuterungen 1a In einem Netzwerk mit unbekannten Teilnehmern ist es notwendig, die Herkunft der übertragenen Messdaten eindeutig zu identifizieren. (Die Authentizität beruht auf der Identifikationsnummer des Datensatzes und der Netzwerkadresse). 1b In einem geschlossenen Netz sind alle Teilnehmer bekannt. Keine zusätzlichen IT-Mittel sind notwendig, aber die Topologie des Netzes (die Anzahl der Teilnehmer) sollte durch Versiegelung festgeschrieben werden. 2. Unvorhergesehene Verzögerungen während der Übertragung sind möglich. Für eine korrekte Zuordnung eines empfangenen Messwertes zu einer bestimmten Messung muss der Zeitpunkt der Messung registriert werden. 3. Eine Verschlüsselung der Messdaten ist zur Sicherstellung der Authentizität nicht unbedingt erforderlich.		
Erforderliche Dokumentation *Netz mit unbekannten Teilnehmern:* Beschreibung der IT-Mittel für die korrekte Zuordnung des Messwertes zur Messung. *Geschlossenes Netz*: Beschreibung der Hardwaremittel zur Speicherung der Teilnehmeranzahl im Netz. Beschreibung der initialen Identifikation der Teilnehmer.		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die getroffenen Schutzmaßnahmen müssen aufgezeigt werden.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob es eine korrekte Verknüpfung zwischen den einzelnen Messwerten und der zugehörigen Messung gibt. • ob die Daten digital signiert sind, um ihre ordnungsgemäße Identifizierung und Authentifizierung sicherzustellen.		**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.
Beispiel einer akzeptablen Lösung • Jeder Datensatz hat eine eindeutige (fortlaufende) Identifikationszahl, welche den Zeitpunkt der Durchführung der Messung (Zeitstempel) enthalten kann. • Jeder Datensatz enthält Informationen über die Herkunft der Messdaten, d.h. die Seriennummer oder ein anderes Identitätsmerkmal des Messgerätes, das den Wert erzeugt hat. • In einem Netz mit unbekannten Teilnehmern ist Authentizität gewährleistet, wenn der Datensatz eine eindeutige Signatur trägt. Die Signatur deckt alle Felder des Datensatzes ab. • Der Empfänger des Datensatzes überprüft alle Daten auf Plausibilität.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode des sendenden und des empfangenden Gerätes.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D):

Auf Basis des Quellcodes ist zu überprüfen • 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 *Schlüssel und zugehörige Daten müssen als rechtlich relevante Daten behandelt, geheim gehalten und vor Kompromittierung geschützt werden.*		
Erläuterungen 1. Diese Anforderung gilt nur, wenn im System ein geheimer Schlüssel vorhanden ist. (Normalerweise nicht in geschlossenen Netzen.) 2. Der Schutz muss gegen vorsätzliche Änderungen wirksam sein, die durch einfache gebräuchliche Softwaretools ausgeführt werden. 3. Wenn der Zugang zu dem geheimen Schlüssel verhindert wird, z.B. durch Versiegeln des Gehäuses eines Messgerätes mit zweckgebundener Hard- und Software, sind keine zusätzlichen Softwareschutzmaßnahmen erforderlich		**Erläuterungen** 1. Diese Anforderung gilt nur, wenn im System ein geheimer Schlüssel vorhanden ist. (Normalerweise nicht in geschlossenen Netzen.) 2. Der Schutz muss gegen vorsätzliche Änderungen wirksam sein, die durch spezielle, anspruchsvolle Softwaretools ausgeführt werden. 3. Die empfangenen Messwerte werden aus dem Datensatz gelesen und ihre Signatur mit Hilfe des öffentlichen Schlüssels des sendenden Messgerätes (oder des Gerätes, das den relevanten Datensatz erzeugt hat) überprüft. Mit dieser Überprüfung kann der Empfänger nachweisen, dass Wert und Signatur zusammengehören. 4. Geeignete, dem elektronischen Zahlungsverkehr gleichwertige Methoden müssen verwendet werden.
Erforderliche Dokumentation Beschreibung des Schlüsselmanagements und der Maßnahmen zur Geheimhaltung der Schlüssel und der zugehörige Informationen		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die getroffenen Schutzmaßnahmen müssen aufgezeigt werden.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob die geheimen Informationen nicht gefährdet werden können.		**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau 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 zum Signieren verwendet wird, spielen der Startvektor oder das Erzeugungspolynom 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 dieses Schlüssels. Hinweis: Eine technische Lösung mit einem Standard-PC reicht nicht aus, um das hohe Schutzniveau sicherzustellen, wenn es keinen entsprechenden Hardwareschutzmaßnahmen für den Schlüssel und andere geheime Daten gibt (siehe Basisleitfaden für den Universalcomputer U6). 1) *Public-Key*-Infrastruktur: Der öffentliche Schlüssel des unter gesetzlicher Kontrolle stehenden Gerätes wurde von einem akkreditierten Trust Center zertifiziert worden. 2) *Direct Trust*: Es ist nicht notwendig, ein Trust-Center einzubeziehen, wenn nach vorheriger Vereinbarung beide Parteien in der Lage sind, den öffentlichen Schlüssel des Messgerätes direkt an dem unter gesetzlicher Kontrolle stehenden Gerät abzulesen, das den betreffenden Datensatz erzeugt. [4]

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode, der das Schlüsselmanagement umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): *Auf Basis des Quellcodes ist zu überprüfen* • ob die für das Schlüsselmanagement getroffenen Maßnahmen angemessen sind.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
T6: Handhabung von beschädigten Daten *Daten, die als beschädigt erkannt wurden, dürfen nicht verwendet werden.*		
Erläuterungen		

[4] Fehler im Original, hier korrigiert: Der öffentliche Schlüssel muss nicht am empfangenden Gerät, sondern am signierenden angezeigt werden können.

1. Obwohl Kommunikationsprotokolle normalerweise die Übertragung wiederholen, bis sie gelingt, ist es trotzdem möglich, dass ein beschädigter Datensatz empfangen wird.

Erforderliche Dokumentation Beschreibung der Ermittlung von Übertragungsfehlern oder vorsätzliche Änderungen	**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die getroffenen Maßnahmen für die korrekte Handhabung von beschädigten Daten müssen aufgezeigt werden.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob die beschädigten Daten nach dem angegebenen Konzept nicht verwendet werden.	**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.

Beispiel einer akzeptablen Lösung

Wenn das Programm, das Datensätze empfängt, eine Diskrepanz zwischen dem Datensatzwert und dem Sollwert der Signatur erkennt, 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 (Status-Feld) ein Flag mit der Bedeutung "nicht gültig"
  ODER
- löscht den beschädigten Datensatz.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist)

Quellcode des empfangenden Gerätes.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D):

Auf Basis des Quellcodes ist zu überprüfen

- ob getroffenen Maßnahmen für die Handhabung mit beschädigten Daten angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D

T7: Übertragungsverzögerung

Die Messung darf durch eine Übertragungsverzögerung nicht in unzulässiger Weise beeinflusst werden.

Erläuterungen

Der Hersteller muss das Zeitverhalten der Datenübertragung untersuchen und gewährleisten, 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 (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode, der die Datenübertragung umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): *Auf Basis des Quellcodes ist zu überprüfen* • ob die für die Handhabung von Übertragungsverzögerungen getroffenen Maßnahmen angemessen sind.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
T8: Verfügbarkeit von Übertragungsdienste *Wenn Netzwerkdienste nicht verfügbar sind, dürfen keine Messdaten verloren gehen.*		
Erläuterungen 1. Der Benutzer des Messsystems darf nicht in der Lage sein, Messdaten durch Unterdrückung der Übertragung zu korrumpieren. 2. Übertragungsstörungen geschehen zufällig und können nicht ausgeschlossen werden. Das sendende Gerät muss in der Lage sein, mit dieser Situation umzugehen. 3. Die Reaktion des Gerätes, wenn die Übertragungsdienste nicht verfügbar sind, hängt vom Messprinzip ab (siehe Anhang I).		
Erforderliche Dokumentation Beschreibung der Schutzmaßnahmen bei Übertragungsunterbrechung oder anderen Fehlern.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • welche Maßnahmen angewendet werden, um vor Datenverlust zu schützen. • welche Maßnahmen für den Fall von Übertragungsfehlern vorgesehen sind. *Funktionsprüfungen:* • Stichprobenüberprüfungen, ob keine relevanten Daten aufgrund von Übertragungsunterbrechung verloren gehen.		
Beispiel einer akzeptablen Lösung 1) Für unterbrechbare Messungen, die leicht und schnell unterbrochen werden können, z.B. Wägen, Kraftstoffmessung usw., kann die Messung abgeschlossen werden, 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 Transaktion ist. Danach kann eine neue Transaktion gestartet werden und die gepufferten Werte müssen für die spätere Übertragung aufbewahrt werden. Für weitere Beispiele siehe Anhang I. 2) Messungen, die nicht unterbrochen werden können, z.B. die Messung von Energie, Volumen usw., benötigen keine besonderen Zwischenpuffer, da diese Messungen immer kumulativ sind. Das kumulative Register kann zu einem späteren Zeitpunkt ausgelesen und übertragen werden, wenn die Verbindung wieder besteht.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode, der die Übertragung umsetzt.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): *Auf Basis des Quellcodes ist zu überprüfen* • ob die Maßnahmen für die Reaktion auf unterbrochenen Übertragungsdienst angemessen sind.

8 Anhang S: Softwaretrennung

Softwaretrennung ist eine optionale Entwurfsmethodik, die dem Hersteller eine einfache Modifikation der rechtlich nicht relevanten Software gestattet. Wenn Softwaretrennung realisiert wird, dann muss dieser Anhang zusätzlich zu den Basisanforderungen für die Typen P und U berücksichtigt werden.

8.1 Technische Beschreibung

Softwaregesteuerte Messgeräte und -systeme haben im Allgemeinen komplexe Funktionen und enthalten Module, die rechtlich relevant sind, und Module, die es nicht sind. Es ist ein Vorteil für den Hersteller und Prüfer - obwohl es nicht vorgeschrieben ist -, diese Softwaremodule des Messsystems zu trennen.
In der folgenden Tabelle sind zwei Varianten der Softwaretrennung beschrieben. Beide Varianten sind durch den Anforderungssatz abgedeckt.

Beschreibung
Die Softwaretrennung wird unabhängig vom Betriebssystem als eigener Code- und Datenbereich eines Programms umgesetzt, d.h. auf dem Niveau der Programmiersprache **(Low-Level-Softwaretrennung).** Hinweis: Dieses Feature ist sowohl in Typ-P- als auch in Typ-U-Messgeräten umsetzbar.
Die zu trennenden Softwaremodule werden als eigenständige Objekte in Bezug auf das Betriebssystem umgesetzt **(High-Level-Softwaretrennung)**. Hinweis: Diese Art der Trennung ist in der Regel nur mit Universalcomputern möglich. Beispiellösungen sind unabhängig ausführbare Programme, dynamisch gelinkte Bibliotheken usw.

Tabelle 8-1: Technische Beschreibung der Softwaretrennung

Der Schutz vor unzulässigen Veränderungen der Messwerte und Parameter wird nur indirekt angesprochen, da der Programmierer von Softwareteilen, die nicht der gesetzlichen Kontrolle unterliegen, nicht dem Benutzer des Messsystems die Gelegenheit zur Beeinträchtigung geben soll. Aber dies muss in jedem Fall durch den Programmierer (mit oder ohne Trennung) berücksichtigt werden und die entsprechenden Anforderungen sind in den Basisteilen P und U des Leitfadens (Kapitel 4 und 5) gegeben.

8.2 Spezifische Softwareanforderungen an die Softwaretrennung

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">S1: Umsetzung der Softwaretrennung
Ein Teil der Software, der eindeutig von anderen Softwareteilen getrennt ist, muss alle rechtlich relevanten Software und Parameter enthalten.</td></tr>
<tr><td colspan="3">Erläuterungen
1. Zur rechtlich relevanten Software gehören im Falle von Low-Level-Softwaretrennung alle Programmeinheiten (Unterprogramme, Prozeduren, Funktionen, Klassen usw.) und im Falle von High-Level-Softwaretrennung alle Programme und Bibliotheken[5],
- die zur Berechnung von Messwerten beitragen oder einen Einfluss darauf haben,
- die zu Zusatzfunktionen wie Datenanzeige, Datensicherung, Datenspeicherung, Softwareidentifikation, Ausführung von Softwaredownload, Datenübertragung, Überprüfung empfangener oder gespeicherter Daten usw. beitragen.
2. Alle Variablen, temporären Dateien und Parameter, die Einfluss auf den Messwert oder auf rechtlich relevante Funktionen oder Daten haben, gehören zur rechtlich relevanten Software.
3. Die rückwirkungsfreie Softwareschnittstelle (siehe S3) ist Teil der rechtlich relevanten Software.
4. Die rechtlich nicht relevante Software umfasst die restlichen Programmeinheiten, Daten oder Parameter, die oben nicht aufgeführt wurden. Änderungen an diesem Teil sind ohne Unterrichtung der benannten Stelle zulässig, sofern die nachfolgenden Anforderungen an die Softwaretrennung beachtet sind.</td></tr>
<tr><td colspan="2">Erforderliche Dokumentation
Beschreibung der in den obigen Erläuterungen erwähnten, rückwirkungsfreien Softwareschnittstelle.</td><td>Erforderliche Dokumentation (Zusätzliche Dokumentation zu denen von Risikoklasse B und C)
Die korrekte Umsetzung der Softwaretrennung muss durch die Dokumentation aufgezeigt werden.</td></tr>
<tr><td colspan="2">Validierungsanleitung
Auf Basis der Dokumentation ist zu überprüfen
• ob alle rechtlich relevanten Teile, die in den obigen Erläuterungen 1 bis 3 genannte sind, in der rechtlich relevanter Software enthalten sind</td><td>Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C)
Auf Basis der Dokumentation ist zu überprüfen
• ob die Umsetzung der Softwaretrennung korrekt ist.</td></tr>
<tr><td colspan="3">Beispiel einer akzeptablen Lösung
Wie durch die Anforderung beschrieben.</td></tr>
</table>

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist)

5 Hinweis:
Low-Level-Softwaretrennung: Zusammenfassen von Softwareeinheiten auf der Ebene der Programmiersprache oder Zusammenfassen von Programmteilen (d.h. Unterprogramme, Prozeduren, Funktionen, Klassen) zur Bildung des rechtlich relevanten Programmteils. Der Rest der Programme ist der nicht rechtlich relevante Teil.
High-Level Softwaretrennung: Zusammenfassen aller Softwareteile zu einem einzigen Objekt (ein Programm, eine DLL usw.), das durch das Betriebssystem erkennbar ist. Der Rest der Software ist der rechtlich nicht relevante Teil.

Quellcode der rechtlich relevanten Software
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): *Auf Basis des Quellcodes ist zu überprüfen* • ob im Softwareentwurf der Datenfluss bzgl. rechtlich relevanter Daten in der rechtlich relevanten Software eindeutig festgelegt ist und überprüft werden kann. • 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 von Hand), • ob unzulässiger Datenfluss von Teilen, die nicht der gesetzlichen Kontrolle unterliegen, zu geschützten Bereichen gefunden werden kann.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
S2: Gemischte Anzeige *Zusatzinformationen, die von rechtlich nicht relevanter Software erzeugt werden, dürfen nur auf einer Anzeige oder einem Ausdruck angezeigt werden, wenn sie nicht mit den Informationen verwechselt werden können, die aus dem rechtlich relevanten Teil stammen.*		
Erläuterungen Da die Programmierer der rechtlich nicht relevanten Software vielleicht die Zulässigkeit der Anzeigen nicht kennen, liegt es in der Verantwortung der Hersteller, dass die Anforderungen bei allen angezeigten Informationen erfüllt werden.		
Erforderliche Dokumentation Beschreibung der Software, welche die Anzeige umsetzt. Beschreibung, wie die Anzeige der rechtlich relevanten Informationen vor irreführenden Anzeigen geschützt ist, die durch rechtlich nicht relevante Software erzeugt werden.		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die Umsetzung von gemischter Anzeige muss in der Dokumentation aufgezeigt werden.
Validierungsanleitung *Funktionsprüfungen:* • 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.		**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die durchgeführte Umsetzung der gemischten Anzeige korrekt ist.
Beispiel einer akzeptablen Lösung • Die durch die rechtlich nicht relevante Software angezeigten Informationen werden über die rückwirkungsfreie Softwareschnittstelle (siehe S3) zur rechtlich relevanten Software übertragen. Hinter der Schnittstelle durchlaufen sie ein Filter, das unzulässige Informationen erkennt. Die zulässigen Informationen werden dann, gesteuert durch die rechtlich relevante Software, in die Anzeige eingefügt. • Auf einer Anzeige im Fensterstil (Universalcomputer) überprüft die rechtlich relevante Software in kurzen Zeitabständen, ob das Fenster mit den rechtlich relevanten Informationen immer sichtbar und im Fensterstapel oben ist. Wenn es ausgeblendet, minimiert oder außerhalb der Begrenzung ist, erzeugt die Software eine Warnung oder hält die Ausgabe und Verarbeitung von Messwerten an. Wenn die Messung abgeschlossen ist, kann das für rechtliche Zwecke vorgesehene Fenster geschlossen werden.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode der rechtlich relevanten Software
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): *Auf Basis des Quellcodes ist zu überprüfen*

- ob die rechtlich relevante Software die Anzeige der Messwerte erzeugt,
- ob diese Anzeige von rechtlich nicht relevanten Programmen nicht geändert oder unterdrückt werden kann.

Risikoklasse B	Risikoklasse C	Risikoklasse D

S3: Die rückwirkungsfreie Softwareschnittstelle

Der Datenaustausch zwischen der rechtlich relevanten und der rechtlich nicht relevanten Software muss über eine rückwirkungsfreie Softwareschnittstelle durchgeführt werden, welche die Interaktionen und den Datenfluss umfasst.

Erläuterungen

1. Alle Interaktionen und Datenflüsse dürfen die rechtlich relevante Software einschließlich des dynamischen Verhaltens eines Messvorgangs nicht unzulässig beeinflussen.
2. Es muss eine eindeutige Zuordnung von jedem Befehl geben, der über die Softwareschnittstelle zum Initiieren einer Funktion oder zur Datenänderung in die rechtlich relevante Software geschickt wird.
3. Code und Daten, die nicht deklariert und als Befehle dokumentiert sind, dürfen keine Auswirkungen auf die rechtlich relevante Software haben.
4. Die Schnittstelle muss vollständig dokumentiert sein, und weder vom Programmierer der rechtlich relevanten Software noch vom Programmier der rechtlich nicht relevanten Software darf irgendeine nicht dokumentierte Interaktion oder ein Datenfluss unter Umgehung der Schnittstelle umgesetzt werden.

Hinweis: Die Programmierer sind verantwortlich für die Einhaltung dieser Einschränkungen. Technische Mittel, um ein Umgehen der Softwareschnittstelle zu verhindern, sind nicht möglich. Der Programmierer der rückwirkungsfreien Schnittstelle sollte mit dieser Anforderung vertraut sein.

Erforderliche Dokumentation

- Beschreibung der Softwareschnittstelle, besonders in welchem Datenbereich die Schnittstelle umgesetzt ist,
- Eine vollständige Liste aller Befehle zusammen mit einer Erklärung der Vollständigkeit.
- Eine kurze Beschreibung der Bedeutung der Befehle und ihrer Wirkung auf die Funktionen und Daten des Messgerätes.

Erforderliche Dokumentation (Zusätzliche Dokumentation zu denen von Risikoklasse B und C)
Die Umsetzung der Softwareschnittstelle muss durch die Dokumentation aufgezeigt werden.

Validierungsanleitung

Auf Basis der Dokumentation ist zu überprüfen

- ob die Funktionen der rechtlich relevanten Software, die über die rückwirkungsfreie Softwareschnittstelle ausgelöst werden können, definiert und beschrieben sind,
- ob die Parameter, die über die Schnittstelle ausgetauscht werden können, definiert und beschrieben sind,
- ob die Beschreibung der Funktionen und Parameter schlüssig und vollständig ist.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C)

Auf Basis der Dokumentation ist zu überprüfen

- ob die Umsetzung der Softwareschnittstelle korrekt 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 dem Unterprogramm als Parameter übergeben.
- Die rechtlich relevante Software filtert unzulässige Schnittstellenbefehle heraus.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist)
Quellcode der rechtlich relevanten Software

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D):
Auf Basis des Quellcodes ist zu überprüfen

- ob im Softwareentwurf der Datenfluss in der rechtlich relevanten Software eindeutig definiert ist und überprüft werden kann,
- der Datenfluss über die Softwareschnittstelle mit Softwaretools oder manuell. Es ist zu überprüfen, ob der gesamte Datenfluss zwischen den Teilen dokumentiert wurde (keine Umgehung der angegebenen Softwareschnittstelle),
- ob unzulässiger Datenfluss aus dem nicht kontrolliertem Teil zu geschützten Bereichen gefunden werden kann,
- ob die Befehle, so vorhanden, richtig übersetzt sind und ob es keine undokumentierten Befehle gibt.

9 Anhang D: Download von rechtlich relevanter Software

Dieser Anhang muss für den Download von rechtlich relevanter Software verwendet werden, solange die messtechnischen Merkmale unverändert bleiben und die Konformitätserklärung noch gültig ist, z.B. bei Fehlerbehebungen. Diese Anforderungen sind zusätzlich zu den Basisanforderungen für die Typen P und U zu berücksichtigen, die in den Kapiteln 4 und 5 dieses Leitfadens beschrieben sind.

9.1 Technische Beschreibung

Software kann nur auf die Messgeräte heruntergeladen werden, die durch folgende Eigenschaften gekennzeichnet sind:

Hardwarekonfiguration Das Zielgerät unterliegt der gesetzlichen Kontrolle. Es kann ein Messgerät mit zweckgebundener Hard- und Software (Typ P) oder ein Messgeräte mit Universalrechner (Typ U) sein. Die Kommunikationsanschlüsse für den Download können direkt (z.B. RS 232, USB), über ein geschlossenes Netz, das teilweise oder vollständig gesetzlicher Kontrolle unterliegt (z.B. Ethernet, Token-Ring-LAN), oder über ein offenes Netz (z.B. Internet) erfolgen.
Softwarekonfiguration Die gesamte Software auf dem Zielgerät kann unter gesetzlicher Kontrolle stehen oder es kann Softwaretrennung vorliegen. Der Download der rechtlich relevanten Software muss die im Folgenden aufgeführten Anforderungen erfüllen. Wenn es keine Softwaretrennung im Messgerät gibt, dann gelten alle folgenden Anforderungen für alle Downloads.

Tabelle 9 1: Technische Beschreibung der Konfigurationen für das Softwaredownload

9.2 Spezifische Softwareanforderungen

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">D1: Download-Mechanismus
Der Download und die anschließende Installation der Software erfolgen automatisch und stellen sicher, dass nach dem Download das Schutzniveau der Software wieder auf dem zugelassenen Niveau ist.</td></tr>
<tr><td colspan="3">Erläuterungen
1. Der Download muss automatisch erfolgen, um sicherzustellen, dass das bestehende Schutzniveau nicht beeinträchtigt wird.
2. Das Zielgerät hat eine feste rechtlich relevante Software, die alle notwendigen Funktionen für die Überprüfung der Erfüllung der Voraussetzungen D2 bis D4 enthält.
3. Das Instrument muss in der Lage sein zu erkennen, wenn Download oder Installation fehlschlagen. Es muss eine Warnung ausgegeben werden. Wenn Download 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 die Fehlerursache behoben ist.
4. Bei erfolgreichem Abschluss der Installation müssen alle Schutzmaßnahmen wieder in ihren Ursprungszustand gebracht werden, es sei denn die Benannte Stelle hat für die heruntergeladene Software in der Baumusterprüfbescheinigung erlaubt, die Schutzmaßnahmen abzuändern.
5. Während des Downloads und der anschließenden Installation der heruntergeladenen Software muss die Messung durch das Gerät gesperrt werden oder es muss sichergestellt sein, dass die Messung korrekt abläuft.
6. Die in Anhang I beschriebenen Fehlerbehandlungsanforderungen können umgesetzt werden, wenn beim Download Fehler auftreten. Die Anzahl der Neuinstallationsversuche muss begrenzt sein.
7. Können die Anforderungen D2 bis D4 nicht erfüllt werden, ist es noch möglich, den Teil der rechtlich nicht relevanten Software herunterzuladen. In diesem Fall müssen folgende Anforderungen erfüllt werden:
- Es gibt eine klare Trennung zwischen der rechtlich relevanten und der rechtlich nicht relevanten Software nach Anhang S.
- Der gesamte rechtlich relevante Softwareteil ist festgeschrieben, d.h. er kann nicht ohne Brechen eines Siegels heruntergeladen oder geändert werden.
- In der Baumusterprüfbescheinigung ist festgelegt, dass das Download des rechtlich nicht relevanten Teiles zulässig ist.
8. Es muss möglich sein, in Mitgliedstaaten, in denen Softwaredownload für Geräte im Einsatz nicht erlaubt ist, den Software-Download-Mechanismus mittels einer versiegelbaren Einrichtung (Schalter, gesichert Parameter) zu deaktivieren. In diesem Fall darf es nicht möglich sein, rechtlich relevante Software ohne Beschädigung des Siegels herunterzuladen.</td></tr>
<tr><td colspan="2">Erforderliche Dokumentation
Die Dokumentation muss kurz beschreiben, wie der Download automatisch abläuft, wie die herunter zu ladende Software überprüft und installiert wird, wie das Schutzniveau nach Abschluss garantiert wird und was im Fehlerfall geschieht.</td><td>Erforderliche Dokumentation (Zusätzliche Dokumentation zu denen von Risikoklasse B und C)
Die Umsetzung des Download-Mechanismus muss durch die Dokumentation aufgezeigt werden.</td></tr>
<tr><td colspan="2">Validierungsanleitung
Auf Basis der Dokumentation ist zu überprüfen
• wie der Download-Vorgang ausgeführt wird,
• ob der Download und die Installation automatisch durchgeführt werden, ob das Messgerät gesperrt wird (falls zu-</td><td>Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C)
Auf Basis der Dokumentation ist zu überprüfen</td></tr>
</table>

treffend) und ob der Softwareschutz nach dem Download unbeeinträchtigt ist. • ob es eine nicht herunterladbare, feste, rechtlich relevante Software zur Authentizitäts- und Integritätsüberprüfung gibt, • ob während des Softwaredownloads keine Messung möglich oder eine korrekte Messung gewährleistet ist. *Funktionsprüfungen:* • Durchführen von mindestens einem Softwaredownload zur Überprüfung, dass die Software korrekt heruntergeladen wird.	• ob die Umsetzung des Download-Mechanismus korrekt ist.
Beispiel einer akzeptablen Lösung Ein im festen, nicht ladbaren[6] Teil der Software angesiedeltes Hilfsprogramm, das: a. sich mit dem Sender synchronisiert und die Genehmigung überprüft, b. automatisch das Messen sperrt, sofern nicht eine korrekte Messung gewährleistet werden kann, c. automatisch die rechtlich relevante Software auf 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 Unterstützung von Download und Installation entfernt wurde, nach Abschluss automatisch auf dem zugelassenen Niveau erneuert wird, h. die entsprechende Fehlerbehandlungsprozeduren einleitet, wenn ein Fehler auftritt.	

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode des festen Softwareteils, der für die Ausführung des Downloadprozesses verantwortlich ist.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und 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 heruntergeladenen Software *Es müssen Maßnahmen getroffen werden, die sicherstellen, dass die heruntergeladene Software authentisch ist, und dass angezeigt wird, dass die heruntergeladene Software von einer Benannten Stelle zugelassen wurde.*		
Erläuterungen 1. Bevor die heruntergeladene Software zum ersten Mal verwendet wird, muss das Messgerät automatisch überprüfen, ob: a. die Software authentisch ist (und keine betrügerische Simulation), b. die Software für diese Messgerätebauart zugelassen ist. 2. Die Maßnahmen, mit denen nachgewiesen wird, dass die Software eine Zulassung durch eine Benannte Stelle hat, müssen gesichert werden, um eine Fälschung des Zulassungsstatus zu verhindern. 3. Versagt die heruntergeladene Software bei einer der obigen Kontrollen, siehe D1. 4. Wenn ein Hersteller beabsichtigt, rechtlich relevante Software zu ändern oder zu aktualisieren, muss er die beabsichtigten Änderungen bei der zuständigen Benannten Stelle ankündigen. Die Benannte Stelle entscheidet, ob eine Ergänzung der bestehenden TEC notwendig ist oder nicht. Zum Softwaredownload ist es unerlässlich, dass es eine Soft-		

[6] Ergänzung zum Original

wareidentifikation gibt, die eindeutig der genehmigten Softwareversion zugeordnet ist.

Erforderliche Dokumentation Die Dokumentation muss darstellen: • wie die Authentizität der Softwareidentifikation gewährleistet wird, • wie die Authentizität der Zulassung durch die Benannte Stelle gewährleistet wird, • wie gewährleistet wird, dass die heruntergeladene Software für die Messgerätebauart zugelassen ist, für die sie heruntergeladen wurde.	**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die Umsetzung der Authentifizierung muss durch die Dokumentation aufgezeigt werden.
Validierungsanleitung *Dokumentation- und mit funktionsabhängige Überprüfungen:* • Überprüfung der Dokumentation, wie Downloaden von betrügerischer Software verhindert wird, • Funktionsüberprüfungen, dass Downloaden von betrügerischer Software verhindert wird. Die Authentifizierungsüberprüfung der Software ist anhand der Dokumentation und mit Hilfe von Funktionsüberprüfungen sicherzustellen.	**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.
Beispiel einer akzeptablen Lösung 1. **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 festen Softwareteil des Geräts gespeichert ist, die Herkunft der Signatur vom Hersteller bestätigt. Die Überprüfung mit Hilfe des Schlüssels muss automatisch erfolgen. 2. **Benannte Stelle**: Der Schlüssel wird vor dem In-Verkehr-bringen im festen Softwareteil gespeichert. 3. **Richtige Messgerätebauart**: Die Überprüfung des Gerätebauart erfordert den automatischen Abgleich der Gerätebauartidentifikation, die im festen Softwareteil des Gerätes gespeichert ist, mit einer Kompatibilitätsliste, die der Software beigefügt ist.	
4. **Zulassung durch die Benannte Stelle** Wenn die Authentizität durch die Verwendung des Herstellerschlüssels gewährleistet ist, kann die Zulassung durch die Benannte Stelle angenommen werden.	4. **Zulassung durch die Benannte Stelle** Eine Lösung, um die tatsächliche Zulassung der Software zu überprüfen, besteht darin, dass die gesamte heruntergeladene Software die Signatur der zuständigen Benannten Stelle enthält. Der öffentliche Schlüssel der zuständigen Benannten Stelle ist im Messgerät gespeichert und wird zur automatischen Überprüfung der der Software beigefügten Signatur verwendet. Er kann zum Vergleich mit dem von der zuständigen Benannten Stelle veröffentlichten Schlüssel auf dem Gerät sichtbar gemacht werden.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist)

Quellcode des festen Softwareteils, der für die Authentizitätsüberprüfung der heruntergela-

denen Software zuständig ist
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): *Auf Basis des Quellcodes ist zu überprüfen* • ob die zur Authentizitätsüberprüfung getroffenen Maßnahmen angemessen sind.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
D3: Integrität der heruntergeladenen Software *Es müssen Maßnahmen getroffen werden, die sicherstellen, dass die heruntergeladene Software während des Downloads nicht unzulässig verändert wurde.*		
Erläuterungen 1. Vor der ersten Nutzung der heruntergeladenen Software muss das Messgerät automatisch überprüfen, ob die heruntergeladene Software nicht unzulässig verändert wurde. 2. Besteht die heruntergeladene Software diese Prüfung nicht, siehe D1.		
Erforderliche Dokumentation Die Dokumentation muss darstellen, wie die Integrität der Software gewährleistet wird.		**Erforderliche Dokumentation** (Zusätzliche Dokumentation zu denen von Risikoklasse B und C) Die Maßnahmen zur Integritätssicherung müssen durch die Dokumentation aufgezeigt werden.
Validierungsanleitung • Sicherstellung der Integritätsüberprüfung der Software nach dem Download gemäß der Dokumentation und mittels Funktionsprüfungen		**Validierungsanleitung** (zusätzlich zur Anleitung für Risikoklassen B und C) *Auf Basis der Dokumentation ist zu überprüfen* • ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.
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 beigefügt ist (siehe auch U2 als Beispiel für eine akzeptable Lösung). • Akzeptabler Algorithmus: CRC, geheimer Startvektor, Länge 32 Bit. Der Startvektor ist im festen Softwareteil gespeichert.		**Beispiel einer akzeptablen Lösung** • Es wird ein Hash-Wert der herunterzuladenden Software (Algorithmen wie z.B. SHA-1, RipeMD-160) erzeugt und mit einer geeigneten Schlüssellänge verschlüsselt (RSA, Elliptische Kurven). • Der Schlüssel für die Entschlüsselung ist im festen Softwareteil gespeichert.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist) Quellcode des festen Softwareteils, der für die Integritätsüberprüfung der heruntergeladenen Software zuständig ist.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D): *Auf Basis des Quellcodes ist zu überprüfen* • ob die zur Integritätsüberprüfung ergriffenen Maßnahmen angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D

D4: Rückverfolgbarkeit des Downloads rechtlich relevanter Software

Mit Hilfe geeigneter technischer Hilfsmittel muss gewährleistet werden, dass Downloads rechtlich relevanter Software für spätere Kontrollen im Gerät in geeigneter Form zurückverfolgt werden können.

Erläuterungen

1. Diese Anforderung gestattet Prüfstellen, die für die messtechnische Überwachung gesetzlich kontrollierter Geräte verantwortlich sind, die Rückverfolgung von Downloads rechtlich relevanter Software über einen angemessenen Zeitraum(dieser hängt von der nationalen Gesetzgebung ab).
2. Die Maßnahmen zur und Aufzeichnungen der Rückverfolgung (Logbuch) sind Teil der rechtlich relevanten Software und müssen als solche geschützt werden.

Erforderliche Dokumentation

Die Dokumentation muss

- kurz darstellen, wie die Maßnahmen zur Rückverfolgbarkeit umgesetzt und geschützt werden,
- erklären, wie die heruntergeladene Software zurückverfolgt werden kann.

Erforderliche Dokumentation (Zusätzliche Dokumentation zu denen von Risikoklasse B und C)

Die Sicherungsmaßnahmen für die Rückverfolgbarkeit müssen durch die Dokumentation aufgezeigt werden.

Validierungsanleitung

Auf Basis der Dokumentation ist zu überprüfen

- ob die Mittel zur Rückverfolgbarkeit umgesetzt und geschützt sind.

Funktionsprüfungen:

- Überprüfung der Funktionsfähigkeit dieser Maßnahmen durch Stichproben

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C)

Auf Basis der Dokumentation ist zu überprüfen

- ob die getroffenen Maßnahmen dem hohen Schutzniveau entsprechen.

Beispiel einer akzeptablen Lösung

- Protokollierung der Ladevorgänge. Das Messgerät kann mit einem Logbuch ausgestattet sein, das automatisch zumindest das Datum und den Zeitpunkt des Downloads, die Identifikation der heruntergeladenen rechtlich relevanten Software, die Identifikation der herunterladenden Stelle und einen Erfolgseintrag aufzeichnet. Für jeden Downloadversuch, unabhängig davon, ob dieser erfolgreich war oder nicht, wird ein Eintrag erzeugt.
- Ist die Kapazität des Logbuches erschöpft, muss durch technische Mittel sichergestellt sein, dass keine weiteren Downloads erfolgen können. Das Logbuch kann nur durch Aufbrechen physikalischer oder elektronischer Siegel gelöscht werden. Die Versiegelung darf nur von den Prüfstellen neu angebracht werden.

Zusätze für Risikoklasse E

Erforderliche Dokumentation (Dokumentation, die zusätzlich zu Risikoklassen B, C und D erforderlich ist)

Quellcode des festen Softwareteils, der für die Rückverfolgung der Downloadprozesse und die Verwaltung des Änderungsprotokolls zuständig ist.

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B, C und D):

Auf Basis des Quellcodes ist zu überprüfen

- ob die für die Rückverfolgung der Downloadprozesse ergriffenen Maßnahmen angemessen sind,
- ob die zum Schutz des Änderungsprotokolls ergriffenen Maßnahmen angemessen sind.

Zustimmung zum Download

Es wird davon ausgegangen, dass der Hersteller des Messgeräts seine Kunden bezüglich Updates der Software – insbesondere des rechtlich relevanten Teils - gut informiert und dass

der Kunde ein Softwareupdate nicht ablehnt. Weiterhin wird davon ausgegangen, dass der Hersteller und der Kunde, Nutzer oder Eigentümer des Gerätes sich auf ein - je nach Verwendungszweck und Verwendungsort – geeignetes Verfahren zur Durchführung eines Downloads einigen.

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 3). 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 Abschnitte 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 vorangegangen 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

vorgegeben 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 vorangegangen Kapiteln kommentiert werden.

10.x.4 Beispiele für rechtlich relevante 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 den Bestimmungen der MID unterliegen. Die spezifischen Anforderungen des vorliegenden Kapitels beruhen ausschließlich auf Anhang MI-001.

Empfehlungen und Normen der OIML wurden nicht berücksichtigt.

10.1.2 Technische Beschreibung

10.1.2.1 Hardwarekonfiguration

Wasserzähler sind normalerweise als Messgeräte mit zweckgebundener Hard- und Software umgesetzt (in diesem Dokument Typ P).

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 Mengenmessung kann nicht wiederholt werden.

10.1.2.4 Fehlererkennung und -reaktion

Die Anforderung MI-001, 7.1.2 behandelt elektromagnetische Störungen. Es ist notwendig, diese Anforderung für softwaregesteuerte Geräte zu interpretieren, da die Entdeckung 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.

10.1.3 Spezielle Softwareanforderungen (Wasserzähler)

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-1: Fehlerbehebung *Die Software muss nach einer Störung wieder zur normalen Verarbeitung zurückkehren.*		
Erläuterungen Datumstempel–Flags zur Unterstützung der Protokollierung von Zeiträumen im Fehlbetrieb müssen eingerichtet werden.		
Erforderliche Dokumentation Kurze Beschreibung des Fehlerbehebungsmechanismus und wann er aktiviert wird.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob die Umsetzung der Fehlerbehebung geeignet ist. *Funktionsprüfungen:* • Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.		
Beispiel einer akzeptablen Lösung Ein 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: Backup-Einrichtungen *Es muss eine Einrichtung vorhanden sein, die für ein regelmäßiges Backup rechtlich relevanter Daten (wie z. B. Messwerte und der aktuelle Prozessstatus) im Falle einer Störung sorgt. Diese Daten müssen in einem Permanentspeicher gehalten werden.*		
Erläuterungen Die Speicherintervalle müssen kurz genug sein, damit die Diskrepanz zwischen den aktuellen und den gespeicherten kumulierten Werten gering ist.		
Erforderliche Dokumentation Kurze Beschreibung, für welche Daten ein Backup ausgeführt wird und wann dies geschieht. Berechnung des maximalen Fehlers, der bei kumulierten Werten auftreten kann.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob alle rechtlich relevanten Daten in Dauerspeicher gerettet werden und wiederhergestellt werden können. *Funktionsprüfungen:* • Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.		
Beispiel einer akzeptablen Lösung Für die rechtlich relevanten Daten wird ein Backup wie gefordert ausgeführt (z.B. alle 60 Minuten).		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-3: MID-Anhang I, 8.5 (Rücksetzen kumulierter Messwerte verhindern) *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.*		
Erläuterungen Kumulative Register eines Messgeräts dürfen vor der Inbetriebnahme zurückgesetzt werden.		
Erforderliche Dokumentation Dokumentation der Schutzmaßnahmen vor dem Rücksetzen der Mengenregister.		

Validierungsanleitung

Auf Basis der Dokumentation ist zu überprüfen

- ob kumulative, rechtlich relevante Messdaten nicht ohne das Hinterlassen einer Spur zurückgesetzt werden können.

Funktionsprüfungen:

- Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.

Beispiel einer akzeptablen Lösung

Die Mengenregister sind gegen Verändern und Rücksetzen mit denselben Mitteln wie die Parameter (siehe P7) gesichert.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I1-4: Dynamisches Verhalten

Die rechtlich nicht relevante Software muss das dynamische Verhalten eines Messprozesses nicht nachteilig beeinflussen.

Erläuterungen

- Diese Anforderung gilt zusätzlich zu S-1, S-2 und S-3, wenn eine Softwaretrennung gemäß Anhang S durchgeführt wurde.
- Die zusätzliche Anforderung stellt sicher, dass das dynamische Verhalten der rechtlich relevanter Software bei Echtzeitanwendungen von Zählern nicht in unzulässiger Weise von der rechtlich nicht relevanter Software beeinflusst wird, d.h. dass die Ressourcen der rechtlich relevanten Software nicht in unzulässiger Weise durch den rechtlich nicht relevanten Teil gemindert werden.

Erforderliche Dokumentation

- Beschreibung der Unterbrechungshierarchie.
- Zeitdiagramm der Softwareaufgaben. Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben.

Validierungsanleitung

Auf Basis der Dokumentation ist zu überprüfen

- ob die Dokumentation der Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben dem Programmierer des rechtlich nicht relevanten Softwareteils zur Verfügung steht.

Funktionsprüfungen:

- Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.

Beispiel einer akzeptablen Lösung

Die Unterbrechungshierarchie ist so entworfen, dass nachteilige Einflüsse vermieden werden.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I1-5: Aufgeprägte Softwareidentifikation

Die Softwareidentifikation wird normalerweise auf einem Display angezeigt. Für Wasserzähler wäre als Ausnahme ein Aufprägen der Softwareidentifikation 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 eine Anzeige der Softwareidentifikation auf dem Display zu aktivieren, oder das Display gestattet die Anzeige der Softwareidentifikation aus technischen Gründen nicht (mechanischen Zähler).

b. Das Messgerät hat keine Schnittstelle, um die Softwareidentifikation 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.

Erläuterungen

- Der Hersteller der Hardware bzw. der betroffenen Hardware ist dafür verantwortlich, dass die Softwareidentifikation ordnungsgemäß auf der betroffenen Hardware angegeben ist.
- Es gelten alle Erläuterungen von P2/U2.

Erforderliche Dokumentation

- gemäß P2/U2.

Validierungsanleitung *Prüfung auf Basis der Dokumentation:* • gemäß P2/U2. *Funktionsprüfungen:* • gemäß P2/U2.
Beispiel einer akzeptablen Lösung Aufprägen der Softwareidentifikation auf das Typenschild des Messgeräts

10.1.4 Beispiele für rechtlich relevante Parameter

Wasserzähler haben Parameter wie Konstanten für Berechnungen, für Konfigurationen usw., aber auch für das Festlegen der Gerätefunktionalität. Bezüglich der Identifikation und des Schutzes von Parametern und Parametersätzen siehe Anforderungen unter P2 und P7, Leitfaden P.

Nachstehend werden einige typische Parameter für Wasserzähler genannt. (Diese Tabelle wird aktualisiert, sobald die WELMEC-Arbeitsgruppe 11 den endgültigen Inhalt beschlossen hat.)

Parameter	geschützt	einstellbar	Anmerkung
Kalibrierfaktor	x		
Linearisierungsfaktor	x		

10.1.5 Weitere Aspekte

Bei Anwendungen im Haushalt geht man davon aus, dass ein Softwaredownload (Anhang D, Kapitel 9) im Allgemeinen nicht notwendig ist.

Die kumulierte Energie oder das Mengenregister von Geräten im Haushalt ist keine Langzeitspeicherung im Sinne von Anhang L (Kapitel 6). Für ein Gerät, das nur kumulierte Energie / Menge misst, ist deshalb die Anwendung von Anhang L nicht erforderlich.

10.1.6 Einstufung in Risikoklassen

Gemäß der Beschlüsse der zuständigen WELMEC-Arbeitsgruppe 11 (2. Sitzung, 3./4. März 2005) wird derzeit die folgende Risikoklasse als angemessen befunden und sollte angewendet werden, wenn Softwareprüfungen für (softwaregesteuerte) Wasserzähler auf Grundlage dieses Leitfadens durchgeführt werden:

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

Eine endgültige Entscheidung wurde jedoch bis jetzt noch nicht getroffen, und die Arbeitsgruppe 11 wird diesen Punkt in Verbindung mit der Diskussion der geeigneten Risikoklasse(n) für Typ-U-Geräte berücksichtigen.

10.2 Gaszähler und Mengenkonverter

10.2.1 Spezifische Vorschriften, Normen und andere normative Dokumente

Die Mitgliedstaaten können – gemäß Artikel 2 der MID – festlegen, dass Gaszähler und Mengenumwerter für Privathaushalte, Gewerbe und Leichtindustrie den Bestimmungen der MID unterliegen. Die spezifischen Anforderungen des vorliegenden Kapitels beruhen ausschließlich auf Anhang MI-002.

Empfehlungen und Normen der OIML wurden nicht berücksichtigt.

10.2.2 Technische Beschreibung

10.2.2.1 Hardwarekonfiguration

Gaszähler und Mengenumwerter sind normalerweise als Messgeräte mit zweckgebundener Hard- und Software umgesetzt (in diesem Dokument Typ P). Sie können einen oder mehrere Eingänge für externe Sensoreinheiten haben und Zähler und Konverter können unterschiedliche Hardwareeinheiten sein.

10.2.2.2 Softwarekonfiguration

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

10.2.2.3 Messprinzip

Gaszähler kumulieren kontinuierlich die verbrauchte Menge. Die kumulierte Menge wird auf dem Messgerät angezeigt. Es werden verschiedene Prinzipien angewendet. Ein Mengenumwerter wird verwendet, um die Menge im Grundzustand zu berechnen. Der Konverter kann integraler Bestandteil des Zählers sein.

Die Mengenmessung kann nicht wiederholt werden.

10.2.2.4 Fehlererkennung und –reaktion

Die Anforderung MI-002, 4.3.1 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.

10.2.3 Spezielle Softwareanforderungen (Gaszähler und Mengenumwerter)

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-1: Fehlerbehebung *Die Software muss nach einer Störung wieder zur normalen Verarbeitung zurückkehren.*		
Erläuterungen Datumstempel–Flags zur Unterstützung der Protokollierung von Zeiträumen im Fehlbetrieb müssen eingerichtet werden.		
Erforderliche Dokumentation Kurze Beschreibung des Fehlerbehebungsmechanismus und wann er aktiviert wird.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob die Umsetzung der Fehlerbehebung geeignet ist. *Funktionsprüfungen:* • Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.		
Beispiel einer akzeptablen Lösung Ein 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
I2-2: Backup-Einrichtungen *Es muss eine Einrichtung vorhanden sein, die für ein regelmäßiges Backup rechtlich relevanter Daten (wie z. B. Messwerte und der aktuelle Prozessstatus) im Falle einer Störung sorgt. Diese Daten müssen in einem Permanentspeicher gehalten werden.*		
Erläuterungen Die Speicherintervalle müssen kurz genug sein, damit die Diskrepanz zwischen den aktuellen und den gespeicherten kumulierten Werten gering ist.		
Erforderliche Dokumentation Kurze Beschreibung, für welche Daten ein Backup ausgeführt wird und wann dies geschieht. Berechnung des maximalen Fehlers, der bei kumulierten Werten auftreten kann.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob alle rechtlich relevanten Daten in Dauerspeicher gerettet werden und wiederhergestellt werden können. *Funktionsprüfungen:* • Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.		
Beispiel einer akzeptablen Lösung Für die rechtlich relevanten Daten wird ein Backup wie gefordert ausgeführt (z.B. alle 60 Minuten).		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-3: MI-002, 5.3[7] (Tauglichkeit der Anzeige) *Die Anzeige der gesamten unkorrigierten Menge muss über eine ausreichende Stellenanzahl verfügen, um sicherzustellen, dass sie bei 8000 Stunden Zählerbetrieb bei Q_{max} nicht auf ihren Ursprungswert zurückkehrt.*		
Erläuterungen		
Erforderliche Dokumentation		

[7] Abweichung vom englischen Original, hier Fehler korrigiert

Dokumentation der internen Darstellung des Mengenregisters.
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob die Speicherkapazität ausreichend ist.
Beispiel einer akzeptablen Lösung Typische Werte für Haushaltsgaszähler sind: Q_{max} = 6 m^3/h. Der erforderliche Bereich beträgt 48.000 m^3 (derzeit zeigen elektronische Gaszähler bis zu 99.999 m^3 an).

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
I2-4: MID-Anhang I, 8.5 (Rücksetzen kumulierter Messwerte verhindern) *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.*		
Erläuterungen Kumulative Register eines Messgeräts dürfen vor der Inbetriebnahme zurückgesetzt werden.		
Erforderliche Dokumentation Dokumentation der Schutzmaßnahmen vor dem Rücksetzen der Mengenregister.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob kumulative, rechtlich relevante Messdaten nicht ohne das Hinterlassen einer Spur zurückgesetzt werden können. *Funktionsprüfungen:* • Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.		
Beispiel einer akzeptablen Lösung Die Mengenregister sind gegen Verändern und Rücksetzen mit denselben Mitteln wie die Parameter (siehe P7) gesichert.		

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
I2-5: MI-002, 5.3 (Lebensdauer der Energiequelle) *Eine dedizierte Energiequelle muss eine Lebensdauer von mindestens fünf Jahren haben. Nach Ablauf von 90% ihrer Lebensdauer muss eine geeignete Warnung angezeigt werden.*		
Erläuterungen Lebensdauer wird hier im Sinne von verfügbarer Energiekapazität verwendet. Wenn die Energiequelle vor Ort ausgetauscht werden kann, dürfen die Parameter und die rechtlich relevanten Daten während des Wechsels nicht verfälscht werden.		
Erforderliche Dokumentation Dokumentation der Kapazität der Energiequelle, der Höchstlebensdauer (unabhängig vom Energieverbrauch), von Messungen zur Bestimmung der verbrauchten oder verfügbare Energie, Beschreibung der Maßnahmen zur Warnung bei wenig verfügbarer Energie.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob die ergriffenen Maßnahmen zur Überwachung der verfügbaren Energie geeignet sind.		
Beispiel einer akzeptablen Lösung Die Betriebsstunden oder die Weckereignisse des Geräts werden gezählt, in einem Permanentspeicher 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.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-6: MI-002, 9.1 (Elektronischer Mengenumwerter) *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 Konverter die Integration der umgewandelten Menge beenden und kann die umgewandelte Menge separat summieren, solange er außerhalb des Betriebsbereiches arbeitet.*		
Erläuterungen Der Fehlerzustand muss angezeigt werden.		
Erforderliche Dokumentation Dokumentation der verschiedenen Register für umgewandelte Menge und Ausfallmenge.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob die ergriffenen Maßnahmen für den Umgang mit ungewöhnlichen Betriebszuständen geeignet sind.		
Beispiel einer akzeptablen 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
I2-7: MI-002, 5.5 (Prüfelement) *Der Gaszähler muss über ein Prüfelement verfügen, das das Ausführen von Prüfungen innerhalb eines vernünftigen Zeitraums gestattet.*		
Erläuterungen Das Prüfelement zur Beschleunigung zeitaufwendiger Prüfverfahren wird normalerweise für die Prüfung vor Installierung 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 *Auf Basis der Dokumentation ist zu überprüfen* • ob alle zeitaufwendigen Prüfverfahren des Gaszählers mit Hilfe des Prüfelements ausgeführt werden können.		
Beispiel einer akzeptablen Lösung 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.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-8: Dynamisches Verhalten *Die rechtlich nicht relevante Software darf das dynamische Verhalten eines Messprozesses nicht nachteilig beeinflussen.*		
Erläuterungen • Diese Anforderung gilt zusätzlich zu S-1, S-2 und S-3, wenn eine Softwaretrennung gemäß Anhang S durchgeführt wurde. • Die zusätzliche Anforderung stellt sicher, dass das dynamische Verhalten der rechtlich relevanter Software bei Echtzeitanwendungen von Zählern nicht in unzulässiger Weise		

durch die rechtlich nicht relevante Software beeinflusst wird, d.h. dass die Ressourcen der rechtlich relevanten Software nicht in unzulässiger Weise durch den rechtlich nicht relevanten Teil gemindert werden.

Erforderliche Dokumentation

- Beschreibung der Unterbrechungshierarchie.
- Zeitdiagramm der Softwareaufgaben. Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben.

Validierungsanleitung

Auf Basis der Dokumentation ist zu überprüfen

- ob die Dokumentation der Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben dem Programmierer des rechtlich nicht relevanten Softwareteils zur Verfügung steht.

Funktionsprüfungen:

- Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.

Beispiel einer akzeptablen Lösung

Die Unterbrechungshierarchie ist so entworfen, dass nachteilige Einflüsse vermieden werden.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I2-9: Aufgeprägte Softwareidentifikation

Die Softwareidentifikation wird normalerweise auf einem Display angezeigt. Für Gaszähler und Mengenumwerter wäre als Ausnahme ein Aufprägen der Softwareidentifikation auf dem 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 der Softwareidentifikation auf dem Display zu aktivieren, oder das Display gestattet die Anzeige der Softwareidentifikation aus technischen Gründen nicht (mechanischen Zähler).

B. Das Messgerät hat keine Schnittstelle, um die Softwareidentifikation 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.

Erläuterungen

- Der Hersteller der Hardware bzw. der betroffenen Hardware ist dafür verantwortlich, dass die Softwareidentifikation ordnungsgemäß auf der betroffenen Hardware angegeben wird.
- Es gelten alle Detaillierenden Anmerkungen von P2/U2.

Erforderliche Dokumentation

- gemäß P2/U2.

Validierungsanleitung

Prüfung auf Basis der Dokumentation:

- gemäß P2/U2.

Funktionsprüfungen:

- gemäß P2/U2.

Beispiel einer akzeptablen Lösung

Aufprägen der Softwareidentifikation auf das Typenschild des Messgeräts

10.2.4 Beispiele für rechtlich relevante Parameter

Gaszähler und Mengenumwerter haben häufig viele Parameter. Sie werden als Konstanten für Berechnungen, als Konfigurationsparameter usw., aber auch für das Festlegen der Gerätefunktionalität verwendet. Bezüglich der Identifikation und des Schutzes von Parametern und Parametersätzen siehe die Anforderungen unter P2 und P7, Leitfaden P.

Nachstehend werden einige typische Parameter für Gaszähler und Mengenumwerter genannt. (Diese Tabelle wird aktualisiert, sobald die WELMEC-Arbeitsgruppe 11 den endgültigen Inhalt beschlossen hat.)

Parameter	geschützt	einstellbar	Anmerkung
Kalibrierfaktor	x		
Linearisierungsfaktor	x		

10.2.5 Weitere Aspekte

Bei Anwendungen im Haushalt geht man davon aus, dass ein Softwaredownload (Anhang D, Kapitel 9) im Allgemeinen nicht notwendig ist.

Die kumulierte Energie oder das Mengenregister von Geräten im Haushalt ist keine Langzeitspeicherung im Sinne von Anhang L (Kapitel 6). Für ein Gerät, das nur kumulierte Energie / Menge misst, ist deshalb die Anwendung von Anhang L nicht erforderlich.

10.2.6 Einstufung in Risikoklassen

Gemäß den Beschlüssen der zuständigen WELMEC-Arbeitsgruppe 11 (2. Sitzung, 3./4. März 2005) wird derzeit die folgende Risikoklasse als angemessen befunden und sollte angewendet werden, wenn Softwareprüfungen für (softwaregesteuerte) Gaszähler und Mengenumwerter auf Grundlage dieses Leitfadens durchgeführt werden:

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

Eine endgültige Entscheidung wurde jedoch bis jetzt noch nicht getroffen, und die Arbeitsgruppe 11 wird diesen Punkt in Verbindung mit der Diskussion der geeigneten Risikoklasse(n) für Typ-U-Geräte berücksichtigen.

Die Arbeitsgruppe 11 ist der Ansicht, dass Vorauszahlung und Intervallmessungsfunktionalität zu den in der MID, Anhang MI-002, angegebenen wesentlichen Funktionen zugefügt werden müssen. Aus diesem Grund werden diese Varianten in keine höhere Risikokategorie eingestuft als die Grundmessgeräte, die bereits von diesem Softwareleitfaden abgedeckt sind. Für die Grundmessfunktion sollte jedoch eine Bewertung erfolgen, und zwar - so wie für alle anderen Geräte vom Typ P - zusammen mit einer eventuellen weiteren, erforderlichen Bewertung zum Nachweis, dass die Software mit diesen Funktionen keinen unzulässigen Einfluss auf das Grundmessgerät hat.

10.3 Aktive elektrische Energiezähler

10.3.1 Spezifische Vorschriften, Normen und andere normative Dokumente

Die Mitgliedstaaten können – gemäß Artikel 2 der MID – festlegen, dass Wirkverbrauchszähler für Privathaushalte, Gewerbe und Leichtindustrie den Bestimmungen der MID unterliegen. Die spezifischen Anforderungen des vorliegenden Kapitels beruhen ausschließlich auf Anhang MI-003.

Empfehlungen und Normen der OIML wurden nicht berücksichtigt.

10.3.2 Technische Beschreibung

Wirkverbrauchszähler verwenden Spannung und Strom als Eingangsmessgrößen, leiten von ihnen die aktive elektrische Leistung ab und integrieren diese über der Zeit, um die Wirkverbrauch anzugeben.

10.3.2.1 Hardwarekonfiguration

Wirkverbrauchszähler sind normalerweise als Messgeräte mit zweckgebundener Hard- und Software umgesetzt (in diesem Dokument Typ P). Sie können einen oder mehrere Eingänge haben und können in Kombination mit externen Messwandlern verwendet werden.

10.3.2.2 Softwarekonfiguration

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

10.3.2.3 Messprinzip

Wirkverbrauchszähler kumulieren kontinuierlich die in einem Stromkreis verbrauchte Energie. Der kumulierte Energiewert wird auf dem Gerät angezeigt. Es werden verschiedene Prinzipien für Messumformer und Multiplikatoren angewendet.

Die Energiemessung kann nicht wiederholt werden.

10.3.2.4 Fehlererkennung und –reaktion

Die Anforderung MI-003, 4.3.1 behandelt elektromagnetische Störungen. Es ist notwendig, diese Anforderung für softwaregesteuerte Geräte zu interpretieren, da die Entdeckung 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.

10.3.3 Spezielle Softwareanforderungen (Elektrizitätszähler für den Wirkverbrauch)

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-1: Fehlerbehebung *Die Software muss nach einer Störung wieder zur normalen Verarbeitung zurückkehren.*		
Erläuterungen		
Erforderliche Dokumentation Kurze Beschreibung des Fehlerbehebungsmechanismus und wann er aktiviert wird. Kurze Beschreibung der diesbezüglichen, vom Hersteller durchgeführten Tests.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob die Umsetzung der Fehlerbehebung geeignet ist. *Funktionsprüfungen:* • Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.		
Beispiel einer akzeptablen Lösung Ein 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: Backup-Einrichtungen *Es muss eine Einrichtung vorhanden sein, die für ein regelmäßiges Backup rechtlich relevanter Daten (wie z. B. Messwerte und der aktuelle Prozessstatus) im Falle einer Störung sorgt. Diese Daten müssen in einem Permanentspeicher gehalten werden.*		
Erläuterungen Wird die Sicherungsmöglichkeit für die Fehlerbehebung verwendet, muss der Mindestabstand berechnet werden, um sicherzustellen, dass der kritische Wechselwert nicht überschritten wird.		
Erforderliche Dokumentation Kurze Beschreibung, für welche Daten ein Backup ausgeführt wird und wann dies geschieht.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob alle rechtlich relevanten Daten in Dauerspeicher gerettet werden und wiederhergestellt werden können. *Funktionsprüfungen:* • Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.		
Beispiel einer akzeptablen Lösung Für die rechtlich relevanten Daten wird ein Backup wie gefordert ausgeführt (z.B. alle 60 Minuten).		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-3: MI-003, 5.2 (Anzeigetauglichkeit) *Die Anzeige der Gesamtenergie 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 $PF = 1$).*		
Erläuterungen		
Erforderliche Dokumentation Dokumentation der internen Darstellung der elektrischen Energieregistrierung und der Hilfs-		

größen.

Validierungsanleitung

Auf Basis der Dokumentation ist zu überprüfen

- ob die Stellenzahl ausreicht.

Beispiel einer akzeptablen Lösung

Typische Werte für Dreiphasen-Stromzähler sind: P_{max} (4000h) = 3*60 A * 230 V * 4000h = 165600 kWh. Dies erfordert eine interne Darstellung von 4 Byte.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I3-4: MID-Anhang I, 8.5 (Rücksetzen kumulierter Messwerte verhindern)

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.

Erläuterungen

Kumulative Register eines Messgeräts dürfen vor der Inbetriebnahme zurückgesetzt werden.

Erforderliche Dokumentation

Dokumentation der Schutzmaßnahmen vor dem Rücksetzen der Mengenregister.

Validierungsanleitung

Auf Basis der Dokumentation ist zu überprüfen

- ob die kumulierten, rechtlich relevanten Messwerte nicht ohne den Nachweis eines Eingriffs zurückgesetzt werden können.

Funktionsprüfungen:

- Funktionsprüfungen in Gegenwart von Störgrößen reichen aus. Siehe P3 und P4.

Beispiel einer akzeptablen Lösung

Die Energieregister sind gegen Verändern und Rücksetzen mit denselben Mitteln wie die Parameter (siehe P7) gesichert.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I3-5: Dynamisches Verhalten

Die rechtlich nicht relevante Software darf das dynamische Verhalten des Messprozesses nicht nachteilig beeinflussen.

Erläuterungen

- Diese Anforderung gilt zusätzlich zu S-1, S-2 und S-3, wenn eine Softwaretrennung gemäß Anhang S durchgeführt wurde.
- Die zusätzliche 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

Auf Basis der Dokumentation ist zu überprüfen

- ob die Dokumentation der Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben dem Programmierer des rechtlich nicht relevanten Softwareteils zur Verfügung steht.

Funktionsprüfungen:

- Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.

Beispiel einer akzeptablen Lösung

Die Unterbrechungshierarchie ist so entworfen, dass nachteilige Einflüsse vermieden werden.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-6: Aufgeprägte Softwareidentifikation *Die Softwareidentifikation wird normalerweise auf einem Display angezeigt. Für Wirkverbrauchszähler wäre als Ausnahme ein Aufprägen der Softwareidentifikation 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 der Softwareidentifikation auf dem Display zu aktivieren, oder das Display gestattet die Anzeige der Softwareidentifikation aus technischen Gründen nicht (mechanischen Zähler).* *B. Das Messgerät hat keine Schnittstelle, um die Softwareidentifikation 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.*		
Erläuterungen • Der Hersteller der Hardware bzw. der betroffenen Hardware ist dafür verantwortlich, dass die Softwareidentifikation ordnungsgemäß auf der betroffenen Hardware angegeben ist. • Es gelten alle Erläuterungen von P2/U2.		
Erforderliche Dokumentation • gemäß P2/U2.		
Validierungsanleitung *Prüfung auf Basis der Dokumentation:* • gemäß P2/U2. *Funktionsprüfungen:* • gemäß P2/U2.		
Beispiel einer akzeptablen Lösung Aufprägen der Softwareidentifikation auf das Typenschild des Messgeräts		

10.3.4 Beispiele für rechtlich relevante Parameter

Elektronische Verbrauchszähler haben häufig viele Parameter. Sie werden als Konstanten für Berechnungen, als Konfigurationsparameter usw., aber auch für das Festlegen der Gerätefunktionalität verwendet. Bezüglich der Identifikation und des Schutzes von Parametern und Parametersätzen siehe die Anforderungen unter P2 und P7, Leitfaden P.

Nachstehend werden einige typische Parameter von Elektrizitätszählern für Wirkverbrauch genannt. (Diese Tabelle wird aktualisiert, sobald die WELMEC-Arbeitsgruppe 11 den endgültigen Inhalt beschlossen hat.)

Parameter	geschützt	einstellbar	Anmerkung
Kalibrierfaktor	x		
Linearisierungsfaktor	x		

10.3.5 Weitere Aspekte

Bei Anwendungen im Haushalt geht man davon aus, dass ein Softwaredownload (Anhang D, Kapitel 9) im Allgemeinen nicht notwendig ist.

Die kumulierte Energie oder das Mengenregister von Geräten im Haushalt ist keine Langzeitspeicherung im Sinne von Anhang L (Kapitel 6). Für ein Gerät, das nur kumulierte Energie / Menge misst, ist deshalb die Anwendung von Anhang L nicht erforderlich.

10.3.6 Einstufung in Risikoklassen

Gemäß den Beschlüssen der zuständigen WELMEC-Arbeitsgruppe 11 (2. Sitzung, 3./4. März 2005) wird derzeit die folgende Risikoklasse als angemessen befunden und sollte angewendet

werden, wenn Softwareprüfungen für (softwaregesteuerte) Elektrizitätszähler für Wirkverbrauch auf Grundlage dieses Leitfadens durchgeführt werden:

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

Eine endgültige Entscheidung wurde jedoch bis jetzt noch nicht getroffen, und die Arbeitsgruppe 11 wird diesen Punkt in Verbindung mit der Diskussion der geeigneten Risikoklasse(n) für Typ-U-Geräte berücksichtigen.

Die Arbeitsgruppe 11 ist der Ansicht, dass Vorauszahlung und Intervallmessungsfunktionalität zu den in der MID, Anhang MI-002, angegebenen wesentlichen Funktionen zugefügt werden müssen. Aus diesem Grund werden diese Varianten in keine höhere Risikokategorie eingestuft als die Grundmessgeräte, die bereits von diesem Softwareleitfaden abgedeckt sind. Für die Grundmessfunktion sollte jedoch eine Bewertung erfolgen, und zwar - so wie für alle anderen Geräte vom Typ P - zusammen mit einer eventuellen weiteren, erforderlichen Bewertung zum Nachweis, dass die Software mit diesen Funktionen keinen unzulässigen Einfluss auf das Grundmessgerät hat.

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 der MID unterliegen. Die spezifischen Anforderungen des vorliegenden Kapitels beruhen ausschließlich auf Anhang MI-004.

Empfehlungen und Normen der OIML wurden nicht berücksichtigt.

10.4.2 Technische Beschreibung

10.4.2.1 Hardwarekonfiguration

Wärmezähler sind normalerweise als Messgeräte mit zweckgebundener Hard- und Software umgesetzt (in diesem Dokument Typ P). Ein Wärmezähler ist entweder ein vollständiges Messgerät oder ein kombiniertes Gerät, das aus den Baugruppen Durchflusssensor, Temperaturfühlerpaar und Rechenwerk - gemäß MID Artikel 4(b) - oder aus einer Kombination derselben besteht.

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 MI-004, 4.1 und 4.2, behandeln elektromagnetische Störungen. Es ist notwendig, diese Anforderung für softwaregesteuerte Geräte zu interpretieren, da die Entdeckung 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.

10.4.3 Spezielle Softwareanforderungen (Wärmezähler)

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-1: Fehlerbehebung *Die Software muss nach einer Störung wieder zur normalen Verarbeitung zurückkehren.*		
Erläuterungen Datumstempel–Flags zur Unterstützung der Protokollierung von Zeiträumen im Fehlbetrieb müssen eingerichtet werden.		
Erforderliche Dokumentation Kurze Beschreibung des Fehlerbehebungsmechanismus und wann er aktiviert wird.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob die Umsetzung der Fehlerbehebung geeignet ist. *Funktionsprüfungen:* • Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.		
Beispiel einer akzeptablen Lösung Ein 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: Backup-Einrichtungen *Es muss eine Einrichtung vorhanden sein, die für ein regelmäßiges Backup rechtlich relevanter Daten (wie z. B. Messwerte und der aktuelle Prozessstatus) im Falle einer Störung sorgt. Diese Daten müssen in einem Permanentspeicher gehalten werden.*		
Erläuterungen Die Speicherintervalle müssen kurz genug sein, damit die Diskrepanz zwischen den aktuellen und den gespeicherten kumulierten Werten gering ist.		
Erforderliche Dokumentation Kurze Beschreibung, für welche Daten ein Backup ausgeführt wird und wann dies geschieht. Berechnung des maximalen Fehlers, der bei kumulierten Werten auftreten kann.		
Validierungsanleitung *Auf Basis der Dokumentation ist zu überprüfen* • ob alle rechtlich relevanten Daten in Dauerspeicher gerettet werden und wiederhergestellt werden können. *Funktionsprüfungen:* • Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.		
Beispiel einer akzeptablen Lösung Für die rechtlich relevanten Daten wird ein Backup wie gefordert ausgeführt (z.B. alle 60 Minuten).		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-3: MID-Anhang I, 8.5 (Rücksetzen kumulierter Messwerte verhindern) *Bei Versorgungsmessgeräten muss 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.*		
Detaillierende Anmerkungen Kumulative Register eines Messgeräts dürfen vor der Inbetriebnahme zurückgesetzt werden.		
Erforderliche Dokumentation Dokumentation der Schutzmaßnahmen vor dem Rücksetzen der Mengenregister.		

Validierungsanleitung

Auf Basis der Dokumentation ist zu überprüfen

- ob kumulative, rechtlich relevante Messdaten nicht ohne das Hinterlassen einer Spur zurückgesetzt werden können.

Funktionsprüfungen:

- Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.

Beispiel einer akzeptablen Lösung

Die Mengenregister sind gegen Verändern und Rücksetzen mit denselben Mitteln wie die Parameter (siehe P7) gesichert.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I4-4: Dynamisches Verhalten

Die rechtlich nicht relevante Software darf das dynamische Verhalten eines Messprozesses nicht nachteilig beeinflussen.

Erläuterungen

- Diese Anforderung gilt zusätzlich zu S-1, S-2 und S-3, wenn eine Softwaretrennung gemäß Anhang S durchgeführt wurde.
- Die zusätzliche Anforderung stellt sicher, dass das dynamische Verhalten von rechtlich relevanter Software bei Echtzeitanwendungen von Zählern nicht in unzulässiger Weise durch die 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

Auf Basis der Dokumentation ist zu überprüfen

- ob die Dokumentation der Grenzen der anteiligen Laufzeit der rechtlich nicht relevanten Aufgaben dem Programmierer des rechtlich nicht relevanten Softwareteils zur Verfügung steht.

Funktionsprüfungen:

- Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.

Beispiel einer akzeptablen Lösung

Die Unterbrechungshierarchie ist so entworfen, dass nachteilige Einflüsse vermieden werden.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I4-5: Aufgeprägte Softwareidentifikation

Die Softwareidentifikation wird normalerweise auf einem Display angezeigt. Für Wärmezähler wäre als Ausnahme ein Aufprägen der Softwareidentifikation 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 der Softwareidentifikation auf dem Display zu aktivieren, oder das Display gestattet die Anzeige der Softwareidentifikation aus technischen Gründen nicht (mechanischen Zähler).

B. Das Messgerät hat keine Schnittstelle, um die Softwareidentifikation 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.

Erläuterungen

- Der Hersteller der Hardware bzw. der betroffenen Hardware ist dafür verantwortlich, dass die Softwareidentifikation ordnungsgemäß auf der betroffenen Hardware angegeben ist.
- Es gelten alle Erläuterungen von P2/U2.

Erforderliche Dokumentation

- gemäß P2/U2.

Validierungsanleitung *Prüfung auf Basis der Dokumentation:* • gemäß P2/U2. *Funktionsprüfungen:* • gemäß P2/U2.
Beispiel einer akzeptablen Lösung Aufprägen der Softwareidentifikation auf das Typenschild des Messgeräts

10.4.4 Beispiele für rechtlich relevante Parameter

Wärmezähler haben Parameter wie Konstanten für Berechnungen, für die Konfiguration usw., aber auch für das Festlegen der Gerätefunktionalität. Bezüglich der Identifikation und des Schutzes von Parametern und Parametersätzen siehe die Anforderungen unter P2 und P7, Leitfaden P.

Nachstehend werden einige typische Parameter für Wärmezähler genannt. (Diese Tabelle wird aktualisiert, sobald die WELMEC-Arbeitsgruppe 11 den endgültigen Inhalt beschlossen hat.)

Parameter	geschützt	einstellbar	Anmerkung
Kalibrierfaktor	x		
Linearisierungsfaktor	x		

10.4.5 Weitere Aspekte

Bei Anwendungen im Haushalt geht man davon aus, dass ein Softwaredownload (Anhang D, Kapitel 9) im Allgemeinen nicht notwendig ist.

Die kumulierte Energie oder das Mengenregister von Geräten im Haushalt ist keine Langzeitspeicherung im Sinne von Anhang L (Kapitel 6). Für ein Gerät, das nur kumulierte Energie / Menge misst, ist deshalb die Anwendung von Anhang L nicht erforderlich.

10.4.6 Einstufung in Risikoklassen

Gemäß den Beschlüssen der zuständigen WELMEC-Arbeitsgruppe 11 (2. Sitzung, 3./4. März 2005) wird derzeit die folgende Risikoklasse als angemessen befunden und sollte angewendet werden, wenn Softwareprüfungen für (softwaregesteuerte) Wärmezähler auf Grundlage dieses Leitfadens durchgeführt werden:

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

Eine endgültige Entscheidung wurde jedoch bis jetzt noch nicht getroffen, und die Arbeitsgruppe 11 wird diesen Punkt in Verbindung mit der Diskussion der geeigneten Risikoklasse(n) für Typ-U-Geräte berücksichtigen.

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 sind in Anhang MI-005 enthalten. Weder diese spezifischen Anforderungen noch sonstige normative Dokumente wurden bisher im vorliegenden Dokument berücksichtigt.

10.6.1 - 10.6.2 werden ausgefüllt, falls dies in Zukunft notwendig erscheint.

10.5.3 Spezielle Softwareanforderungen (Messsysteme für Flüssigkeiten außer Wasser)

Risikoklasse B	Risikoklasse C	Risikoklasse D
I5-1: Aufgeprägte Softwareidentifikation *Die Softwareidentifikation wird normalerweise auf einem Display angezeigt. Für Messsysteme für Flüssigkeiten außer Wasser wäre als Ausnahme ein Aufprägen der Softwareidentifikation 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 der Softwareidentifikation auf dem Display zu aktivieren, oder das Display gestattet die Anzeige der Softwareidentifikation auf dem Display aus technischen Gründen nicht oder es gibt kein Display am Gerät.* *B. Das Messgerät hat keine Schnittstelle, um die Softwareidentifikation zu übermitteln.* *C. Nach der Fertigung eines Gerätes ist eine Änderung der Software nicht mehr möglich oder nur dann möglich, wenn auch die Hardware oder ein Hardwareteil geändert wird.*		
Erläuterungen • Der Aufkleber der die Softwareidentifikation aufweist, darf weder löschbar noch übertragbar sein. • Der Hersteller der Hardware bzw. der betroffenen Hardware ist dafür verantwortlich, dass die Softwareidentifikation ordnungsgemäß auf der betroffenen Hardware angegeben ist. • Es gelten alle Erläuterungen von P2/U2.		
Erforderliche Dokumentation • gemäß P2/U2.		
Validierungsanleitung *Prüfung auf Basis der Dokumentation:* • gemäß P2/U2. *Funktionsprüfungen:* • gemäß P2/U2.		
Beispiel einer akzeptablen Lösung Aufprägen der Softwareidentifikation auf das Typenschild des Geräts		

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 derzeit die folgende Risikoklasse angewendet werden, wenn Softwareprüfungen für (softwaregesteuerte) Messsysteme zur kontinuierlichen und dynamischen Mengenmessung von Flüssigkeiten außer Wasser auf Grundlage dieses Leitfadens durchgeführt werden:

- **Risikoklasse C**

10.6 Waagen

Waagen werden in zwei Hauptkategorien unterteilt:

- nicht selbsttätige Waagen (NSW) und
- selbsttätige Waagen (SW)

Während die meisten selbsttätigen Waagen durch der 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 Straßenfahrzeug 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 Anpassung 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.

10.6.2.5 Fehlererkennung und –reaktion

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 etc.). Die Fehlerbehebungsverfahren sind überall gleich.

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

Risikoklasse B	Risikoklasse C	Risikoklasse D

I6-1: Fehlererkennung

Die Software muss erkennen, dass die normale Verarbeitung gestört ist.

Erläuterungen

Bei Entdeckung eines Fehlers:

a) Die kumulativen Messwerte und andere rechtlich relevante Daten müssen automatisch in einen Permanentspeicher gerettet werden (siehe Anforderung I6-2), und

b) 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

Auf Basis der Dokumentation ist zu überprüfen

- ob die Umsetzung der Fehlererkennung geeignet ist.

Funktionsprüfungen:

- 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 Watchdog wird von einem zyklisch ausgeführten Mikroprozessor-Unterprogramm zurückgesetzt, um das Auslösen des Watchdogs zu verhindern. Vor dem Zurücksetzen überprüft das Unterprogramm das System, z.B. ob alle metrologisch relevanten Unterprogramme innerhalb des letzten Intervalls ausgeführt wurden. 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

I6-2: Backup-Einrichtungen

Es muss eine Einrichtung vorhanden sein, die für das Backup rechtlich relevanter Daten (wie z. B. Messwerte und der aktuelle Prozessstatus) im Falle einer Störung sorgt.

Erläuterungen

- Die Zustandsmerkmale und wichtige Daten müssen in einem Permanentspeicher gespeichert werden.
- 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").
- 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 *Auf Basis der Dokumentation ist zu überprüfen* • ob im Falle einer Störung alle rechtlich relevanten Daten gerettet sind. *Funktionsprüfungen:* • Durch Simulierung einer Störung überprüfen, ob der Backupmechanismus so wie in der Dokumentation beschrieben funktioniert.
Beispiel einer akzeptablen Lösung Eine 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 Permanentspeicher, z.B. in einem EEPROM oder in einem anderen geeigneten Speicher. Hinweis: 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 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 Wagen (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
	TF		X	X				

Umschaltsperre zw. Funktionen z.B. Nullstellung/Tara			X	X	X	X	X	
Betrieb automat./nicht automat. Nullstellung/Totalisieren		X						X
Log für Änderung der dynamischen Justierung	TF (VV)		X	X				
Maximale 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 automatische 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 (ob P oder U).

Jedoch erscheint gemäß dem Ergebnis der WG7-Befragung (2004) die folgende Unterteilung hinsichtlich der Typ-P- und Typ-U-Geräte und "Selbsttätige Waagen zum diskontinuierlichen und zum kontinuierlichen Totalisieren" als geeignet und wird in der WELMEC-Arbeitsgruppe WG2 noch einmal diskutiert (Beschluss 25. WG2-Sitzung vom 14. und 15. Oktober 2004):

- **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 besonderen Anforderungen sind in Anhang MI-007 enthalten. Bisher sind weder diese besonderen Anforderungen noch irgendwelche normativen Dokumente berücksichtigt worden.

10.7.1 Spezifische Vorschriften, Normen und andere normative Dokumente

Die EU-Norm EN50148, die ein normatives Dokument im Sinne der MID werden könnte, ist bisher noch nicht berücksichtigt worden. Als ein Ergebnis des MID-Verfahrensprojekts wurde ein Leitfaden über Taxameter veröffentlicht. In Zukunft wird dieses Dokument als Grundlage für einen WELMEC-Leitfaden dienen. Auch gibt es einen allerersten Entwurf einer OIML-Empfehlung zu Taxametern. Das OIML-Dokument kann jedoch beim derzeitigen Stand nicht als normatives Dokument verwendet werden (Stand: Oktober 2004).

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.

Aktuelle Taxameter verwenden eine eingebettete Architektur, d.h. Taxameter sind Messgeräte mit zweckgebundener Hard- und Software (Typ P) im Sinne dieses Leitfadens. In Zukunft wird erwartet, dass Taxametern auch unter Verwendung von Universalrechnern (Typ U) hergestellt werden.

10.7.3 Spezielle Softwareanforderungen

MID Anhang MI-007, 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.

Das Taxameter benötigt außerdem einen Langzeitspeicher, denn die Daten müssen mindestens ein Jahr lang im Taxameter abrufbar sein, siehe MI-007, 15.2.

Risikoklasse B	**Risikoklasse C**	**Risikoklasse D**
I7-1: Backup-Einrichtungen *Es muss eine Einrichtung vorhanden sein, die automatisch für wichtige Daten ein Backup erzeugt, wie z.B. Messwerte oder den aktuellen Prozessstatus, wenn die Spannung für längere Zeit abfällt.*		
Erläuterungen 1) Diese Daten sollten normalerweise in einem Permanentspeicher 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 die Umsetzung der Fehlerbehebung geeignet ist. *Funktionsprüfungen:*		

• Funktionsprüfungen in Gegenwart von Störgrößen reichen aus.
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 Permanentspeicher, 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.

10.7.4 Beispiele für rechtlich relevante Funktionen und Daten

Nachstehend sind einige typische Taxameter-Parameter aufgelistet.

Parameter	geschützt	einstellbar	Anmerkung
K-Faktor	x		Impulse pro km
Tarife	x	x	Währungseinheit/km, Währungseinheit/h
Schnittstellenparameter		x	Baud-Rate etc.

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 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) 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 Messgeräte betrachtet. Daher gilt der vorliegende Software-Leitfaden derzeit nicht für Maßverkörperungen.

10.9 Längenmessgeräte

Längenmessgeräte unterliegen den Regelungen der MID. Die besonderen Anforderungen sind in Anhang MI-009 enthalten. Bisher sind weder diese besonderen 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 besonderen Anforderungen sind in Anhang MI-010 enthalten. Bisher sind weder diese besonderen 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) Längenmessgeräte durchgeführt werden:

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

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

11 Definition von Risikoklassen

11.1 Allgemeiner Grundsatz

Die Anforderungen des vorliegenden Leitfadens werden nach (Software-) Risikoklassen unterschieden. Die Risiken beziehen sich auf die Software des Messgeräts und nicht auf sonstige Risiken. Der Einfachheit halber wird der kürzere Begriff "Risikoklasse" verwendet. Jedes Messgerät muss in eine bestimmte Risikoklasse eingestuft werden, da die speziellen, anzuwendenden Softwareanforderungen davon abhängen, zu welcher Risikoklasse das Gerät gehört. Eine Risikoklasse ist durch die Verbindung der geeigneten Stufen für Softwareschutz, Softwareprüfung und Softwarekonformität bestimmt. Für jede dieser Kategorien werden drei Stufen - niedrig, mittel und hoch - eingeführt.

11.2 Beschreibung der Stufen für Schutz, Prüfung und Konformität

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 Softwarewerkzeugen (z.B. Texteditoren) vorgenommen werden können.

Hoch: Die Software ist gegen vorsätzliche Veränderungen geschützt, die mit Hilfe von anspruchsvollen Softwarewerkzeugen (z.B. Debugger oder Festplatteneditoren, Softwareentwicklungswerkzeuge etc.) 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 unterzogen 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.

Stufen der Softwarekonformität

Niedrig: Die implementierte Softwarefunktionalität jedes Einzelgerätes stimmt mit der zugelassenen Dokumentation überein.

Mittel: Zusätzlich zu Konformitätsstufe "Niedrig" müssen bei der Konformitätsbewertung/Baumusterprüfung in Abhängigkeit von den technischen Eigenschaften Teile der Software als "fest", d.h. als nur mit Zustimmung der Benannten Stelle veränderbar definiert werden. Der "feste" Teil muss in allen Einzelgeräten gleich sein.

Hoch: Die implementierte Software in den Einzelgeräten ist vollständig identisch mit der zugelassenen Software.

11.3 Ableitung von Risikoklassen

Von den 27 theoretisch möglichen Permutationen der Stufen sind nur 4 oder höchstens 5 von praktischem Interesse (Risikoklassen B, C, D und E, eventuell F). Sie decken alle Messgeräteklassen ab, die unter die Bestimmungen der MID fallen. Darüber hinaus bieten sie genügend Spielraum für den Fall, dass sich Risikobewertungen ändern. Die Klassen werden in der nachstehenden Tabelle definiert.

Risikoklasse	Softwareschutz	Softwareprüfung	Grad der Softwarekonformität
A	*niedrig*	*niedrig*	*niedrig*
B	*mittel*	*mittel*	*niedrig*
C	*mittel*	*mittel*	*mittel*
D	*hoch*	*mittel*	*mittel*
E	*hoch*	*hoch*	*mittel*
F	*hoch*	*hoch*	*hoch*

Tabelle 11-1: Definition der Risikoklassen

11.4 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 Prüfungsstufe auf die mittlere Stufe angehoben. Die Konformität bleibt gegenüber Risikoklasse A unverändert.

Risikoklasse C: Im Vergleich mit Risikoklasse B wird die Konformitätsstufe auf "mittel" angehoben. Dies bedeutet, dass bei der Bauartzulassung Teile der Software als "fest" definiert werden können. Die übrige Software muss auf der Stufe der Funktionalität konform sein. 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 Konformitätsstufe bleibt gegenüber Risikoklasse C unverändert.

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

Risikoklasse F: Die Stufen werden in jeder Hinsicht (Schutz, Prüfung und Konformität) auf "hoch" gesetzt. Wie bei Risikoklasse A ist nicht zu erwarten, dass irgendein Gerät als Gerät der Risikoklasse F eingestuft wird. Durch Einführen dieser Klasse wird jedoch die entsprechende Möglichkeit offen gehalten

12 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.

12.1 Muster für den allgemeinen Teil des Prüfberichts

Prüfbericht Nr. XYZ122344

Durchflussmessgerät Dynaflow Model DF101

Validierung der Software

(*n* Anhänge)

Auftrag

Die Messgeräterichtlinie (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 rechtlich relevanter Daten.

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.

Seite 1 / 3

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, Ausgabe 5 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 Dynaflow 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 für eichpflichtige Daten

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:

- Identifikation der Software
- Vollständigkeit der Dokumentation
- Prüfung des Betriebshandbuchs
- Funktionstestung
- 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
  (Anforderung P4 gilt als nicht anwendbar.)
- L1, L2, L3, L4, L5, L6, L7

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 Dynaflow DF100 V1.2c erfüllt die grundlegenden Anforderungen der Messgeräterichtlinie.

Das Ergebnis bezieht sich nur auf die geprüfte Einheit.

National Testing & Measurement Lab
Softwareabteilung

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

M. S.A.N.S Problème
Technical Officer

Datum: 23. Dezember 2003

Seite 3 / 3

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

Die erste Checkliste unterstützt den Benutzer bei der Entscheidung, welche der Grundkonfigurationen (P oder U) auf das zu prüfende Gerät zutrifft.

Entscheidung zum Gerätetyp				
		(P)		**Anmerkungen**
1	Wurde die gesamte Anwendersoftware für den Messzweck konzipiert?			
		(J)		
2	Wenn allgemein verwendbare Software vorhanden ist, ist sie dann für den Nutzer zugänglich oder sichtbar?			
		(N)		
3	Wird dem Nutzer der Zugang zum Betriebssystem verweigert, wenn es möglich ist, auf eine nicht eichpflichtige Betriebsart umzuschalten?			
		(J)		
4	Sind die implementierten Programme und die Softwareumgebung unveränderlich (mit Ausnahme von Updates)?			
		(J)		
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 Anhängen					
Notwendige r Anhang		**JA**	**NEIN**	**Entfällt**	**Anmerkungen**
L	Ist das Gerät in der Lage, die Messdaten entweder in einen integrierten Speicher oder auf einem Fern- oder Wechsel-speicher zu speichern?				
T	Besitzt das Gerät Schnittstellen für die Übertragung von Daten auf Geräte, die der gesetzlichen Kontrolle unterliegen ODER empfängt das Gerät Daten von einem anderen Gerät, das der gesetzlichen Kontrolle unterliegt?				
S	Gibt es Softwareteile mit Funktionen, die der gesetzlichen Kontrolle unterliegen UND sollen diese Softwareteile nach der Bauartzulassung geändert werden können?				
D	Ist ein Laden von Software möglich oder erwünscht?				
Beachten Sie den notwendigen Anhang für jede mit JA beantwortete Frage!					

12.3 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 geforderte Herstellerdokumentation die Anforderung P1(a-f)?				
P2		Wird die Softwareidentifikation wie in P2 gefordert umgesetzt?				
P3		Wird bei der Befehlseingabe über die Nutzerschnittstelle die unzulässige Beeinflussung der rechtlich relevanten Software und Messdaten verhindert?				
P4		Wird bei der Befehlseingabe über unversiegelte Kommunikationsschnittstellen des Gerätes die unzulässige Beeinflussung der rechtlich relevanten Software und Messdaten verhindert?				
P5		Sind die rechtlich relevante Software und Messdaten vor zufälligen oder unbeabsichtigten Änderungen geschützt?				
P6		Ist die rechtlich relevante Software gegen unzulässige Veränderungen, unzulässiges Laden oder Auslagern des Hardwarespeichers gesichert?				
P7		Sind Parameter, die rechtlich relevante Eigenschaften des Messgeräts festlegen, gegen unbefugte Änderungen 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-h)?				
U2		Wird die Softwareidentifikation wie in U2 gefordert umgesetzt?				
U3		Wird bei der Befehlseingabe über die Nutzerschnittstelle die unzulässige Beeinflussung der rechtlich relevanten Software und Messdaten verhindert?				
U4		Wird verhindert, dass Befehle, die über unversiegelte Kommunikationsschnittstellen des Geräts eingegeben werden, die rechtlich relevante Software und Messdaten unzulässig beeinflussen?				
U5		Sind die rechtlich relevante Software und Messdaten vor zufälligen oder unbeabsichtigten Änderungen geschützt?				
U6		Ist die rechtlich relevante Software gegen unzulässige Veränderungen gesichert?				
U7		Sind eichpflichtige Parameter vor unbefugte Änderungen geschützt?				
U8		Werden Mittel eingesetzt, um die Authentizität der eichpflichtigen Software zu gewährleisten, und wird die Authentizität der dargestellten Ergebnisse garantiert?				
U9		Sind rechtlich relevante Parameter gegen unbefugte Änderungen gesichert?				
** Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.*						

3) Checkliste für besondere Anforderungen aus Anhang L

Checkliste für Anforderungen aus Anhang L						
Anforderung	**Prüfverfahren**		**Bestanden**	**Durchgefallen**	**Entfällt**	**Anmerkungen***
L1		Enthalten die gespeicherten Messdaten alle Informationen, die für die Rekonstruktion einer früheren Messung notwendig sind?				
L2		Sind die gespeicherten Daten vor zufälligen oder unbeabsichtigten Änderungen geschützt?				
L3		Sind die gespeicherten Messdaten vor vorsätzlichen Änderungen durch *einfache gebräuchliche Softwaretools* (für Risikoklassen B und C) oder durch *spezielle, anspruchsvolle Softwaretools* (für Risikoklassen D und E) geschützt?				
L4		Können die gespeicherten Messdaten authentisch auf die Messung, die sie erzeugt hat, zurückgeführt werden?				
L5		B und C) Werden die Schlüssel als rechtlich relevante Daten behandelt und geheim gehalten sowie vor Gefährdung durch *einfache gebräuchliche Softwaretools* geschützt?				
		D und E) Werden die Schlüssel und Begleitdaten als eichpflichtige Daten behandelt, geheim gehalten sowie vor Gefährdung durch *anspruchsvolle Softwaretools* geschützt? Werden geeignete, dem elektronischen Zahlungsverkehr entsprechende Methoden verwendet? Ist der Nutzer in der Lage, die Authentizität des öffentlichen Schlüssels zu überprüfen?				
L6		Zeigt die für die Verifizierung gespeicherter Messdatensätze verwendete Software die Daten an oder druckt sie diese, prüft sie auf Änderungen und gibt im Falle einer Änderung eine Warnung? Gibt es Mittel, um zu vermeiden, dass Daten genutzt werden, die als verfälscht entdeckt wurden?				
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 oder unbeabsichtigten Änderungen geschützt?				
T3		Sind die rechtlich relevanten, übertragenen Daten vor beabsichtigten Änderungen geschützt, die durch *einfache gebräuchliche Softwaretools* (für Risikoklassen B und C) oder durch spezielle, anspruchsvolle Softwaretools (für Risikoklassen D und E) vorgenommen werden?				
T4		Ist es dem Programm, das übertragene relevante Daten empfängt möglich, deren Authentizität zu verifizieren und die Messwerte einer bestimmten Messung zuzuordnen?				
T5		B und C) Werden die Schlüssel als rechtlich relevante Daten behandelt und geheim gehalten sowie vor Gefährdung durch *einfache gebräuchliche Softwaretools* geschützt?				
		D und E) Werden die Schlüssel und Begleitdaten als eichpflichtige Daten behandelt, geheim gehalten sowie vor Gefährdung durch *anspruchsvolle Softwaretools* geschützt? Werden geeignete, dem elektronischen Zahlungsverkehr entsprechende Methoden verwendet? Ist der Nutzer in der Lage, die Authentizität des öffentlichen Schlüssels zu überprüfen?				
T6		Wird verhindert, dass als verfälscht entdeckte Daten genutzt werden?				
T7		Ist sichergestellt, dass die Messung durch eine Übertragungsverzögerung nicht unzulässig beeinflusst wird?				
T8		Ist sichergestellt, dass keine Messdaten verlorengehen, wenn Netzdienste nicht verfügbar sind?				
** Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.*						

5) Checkliste für besondere Anforderungen aus Anhang S

Checkliste für Anforderungen von Anhang S						
Anforderung	**Prüfverfahren**		**Bestanden**	**Durchgefallen**	**Entfällt**	**Anmerkungen***
S1		Enthält die Software, die der gesetzlichen Kontrolle unterliegt, die gesamte rechtlich relevante Software und alle rechtlich relevanten Parameter?				
S2		Ist sichergestellt, dass zusätzliche Informationen, die vom rechtlich nicht relevanten Softwareteil auf einer Anzeige oder einem Ausdruck angezeigt werden, nicht mit den Informationen verwechselt werden können, die vom rechtlich relevanten Teil stammen?				
S3		Erfolgt der Datenaustausch zwischen der rechtlich relevanten und der rechtlich nicht relevanten Software über eine geschützte Softwareschnittstelle, die die Interaktionen und den Datenfluss umfassend kontrolliert?				
** 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**	**Anmerkungen***
D1		Erfolgen der Download und die nachfolgende Installation der Software automatisch? Ist sichergestellt, dass die Softwareschutzumgebung nach Beendigung auf dem zugelassenen Stand ist?				
D2		Werden Mittel eingesetzt, die garantieren, dass die heruntergeladene Software authentisch ist, und die anzeigen, ob die heruntergeladene Software von einer Benannten Stelle zugelassen wurde?				
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.*						

12.4 In die Baumusterprüfbescheinigung einzubeziehende Informationen

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

- Verweis auf die zur Konformitätsbewertung/Baumusterprüfung vorgelegte Dokumentation,
- Identifikation und Beschreibung der elektronischen (Hardware-)Teile (Baugruppen/Module), die für die Software-/IT-Funktion der Messgeräte wichtig sind,
- Überblick über die Softwareumgebung, die für den Softwarebetrieb notwendig ist,
- Überblick über rechtlich relevant SW-Module (einschließlich SW-Trennung, falls implementiert),
- Überblick und Identifikation der Hardware- und (wenn relevant) der Softwareschnittstellen, die für die Software-/IT-Funktionen der Messgeräte wichtig sind (einschließlich Infrarot, Bluetooth, Wireless LAN, …),
- Identifikation und Beschreibung der Speicherorte der Softwareteile im Messgerät (d.h. EPROM, Prozessor, Festplatte, …) deren Versiegelung oder Sichern nötig ist.
- Anweisungen, wie die Softwareidentifikation (zur metrologischen Überwachung) zu prüfen ist,
- im Falle elektronischer Versiegelung: Anweisung wie die Änderungsprotokolle zur Ansicht gebracht werden können.

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

(in Bezug auf MID-Version: Richtlinie 2004/22/EG, 31. März 2004)

13.1 Softwareanforderungen und ihr Bezug zur MID

Anforderung		MID	
Nr.	**Bezeichnung**	**Artikel / Anhang Nr.** (AI = Anhang I)	**Bezeichnung**
	Basisleitfaden P		
P1	Herstellerdokumentation	AI-9.3 AI-12 Artikel 10	Informationen, die auf dem Gerät angegeben oder mit ihm zusammen geliefert werden Konformitätsbewertung Technische Dokumentation
P2	Softwareidentifikation	AI-7.6 AI-8.3	Eignung Schutz vor Verfälschung
P3	Beeinflussung über Benutzerschnittstelle	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[8] Schutz vor Verfälschung
P7	Parameterschutz	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Eignung Schutz vor Verfälschung
	Basisleitfaden U		
U1	Herstellerdokumentation	AI-9.3 AI-12 Artikel 10	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

[8] 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	
Nr.	**Bezeichnung**	**Artikel / Anhang Nr.** (AI = Anhang I)	**Bezeichnung**
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 der Ergebnisse
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 der Ergebnisse
L2	Schutz vor zufälligen oder unbeabsichtigten Änderungen	AI-7.1, AI-7.2 AI-8.4	Eignung Schutz vor Verfälschung
L3	Datenintegrität (Vollständigkeit der Daten	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 der Ergebnisse
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 der Ergebnisse
L7	Automatische Speicherung	AI-7.1 AI-8.4	Eignung Schutz vor Verfälschung
L8	Speicherkapazität und Kontinuität	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 verfälschten Daten	AI-7.1 AI-8.4	Eignung Schutz vor Verfälschung

Anforderung		MID	
Nr.	**Bezeichnung**	**Artikel / Anhang Nr.** (AI = Anhang I)	**Bezeichnung**
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	Durchführung der Softwaretrennung	AI-7.6, AI-10.1	Eignung Ergebnisanzeige
S2	Gemischte Anzeige	AI-7.1, AI-7.2, AI-7.6 AI-10.2	Eignung Ergebnisanzeige
S3	rückwirkungsfreie Softwareschnittstelle	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)[9]		
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
I2-3, I3-3	Tauglichkeit der Anzeige	MI-002-5.3, MI-003-5.2	Besondere Anforderungen für Verbrauchszähler
I1-4, I2-8, I3-5, I4-4	Dynamisches Verhalten	AI-7.6	Eignung Schutz vor unzulässiger Beeinflussung.
I1-3, I2-4, I3-4, I4-3	Rücksetzen kumulierter Messwerte verhindern	AI-8.5	Schutz vor Verfälschung

[9] Mehrere Abweichungen vom englischen Original, hier Fehler korrigiert

Anforderung		MID	
Nr.	**Bezeichnung**	**Artikel / Anhang Nr.** (AI = Anhang I)	**Bezeichnung**
I2-5	Lebensdauer der Energiequelle	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	MI-006-IV, MI-006-V	Selbsttätige Waagen zum diskontinuierlichen und zum kontinuierlichen Totalisieren

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

MID			Softwareleitfaden
Artikel / Anhang Nr. (AI = Anhang I)	**Bezeichnung**	**Anmerkung**	**Anforderung Nr.**
	Artikel-Teil[10]		
1, 2, 3		Keine besondere Softwarerelevanz	
4(b)	Definitionen, Anordnung von Baugruppen	Übertragung eichpflichtiger Daten... Grundleitfäden anwendbar auf Teilgeräte	T. P, U
5 bis 9		Keine besondere Softwarerelevanz	
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		

[10] Mehrere Abweichungen vom englischen Original, hier Fehler korrigiert

MID			Software-leitfaden
Artikel / Anhang Nr. (AI = Anhang I)	**Bezeichnung**	**Anmerkung**	**Anforderung Nr.**
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, I7-1
AI-7	Eignung	Keine Merkmale zum Erleichtern betrügerischer Verwendung; minimale Möglichkeiten für unbeabsichtigte Fehlnutzung; Schutz vor unzulässiger Beeinflussung.	P3 - P7, 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, 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	Mit dem Gerät einhergehende Information		
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
AI-9.4 bis AI-9.8		Keine besondere Softwarerelevanz	
AI-10	Ergebnisanzeige		

MID			Softwareleitfaden
Artikel / Anhang Nr. (AI = Anhang I)	**Bezeichnung**	**Anmerkung**	**Anforderung Nr.**
AI-10.1		Anzeige mittels Display oder Ausdruck.	U8, L6, S2
AI-10.2		Bedeutung des Ergebnisses, keine Verwechslung mit zusätzlichen Anzeigen.	U8, L1, L4, L6, S2
AI-10.3		Abdruck oder Aufzeichnung leicht leserlich und nicht löschbar.	U8, L6, S2
AI-10.4		Für Direktverkäufe: Ergebnisanzeige für beide Parteien.	U8, S2
AI-10.5		Für Verbrauchszähler: Display für den Kunden.	I1-3, I2-3, I2-4, I3-3, I3-4, 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	
	Anhang 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

MID			Software-leitfaden
Artikel / Anhang Nr. (AI = An-hang I)	**Bezeichnung**	**Anmerkung**	**Anforderung Nr.**
MI-002-3.1.3 bis MI-002-5.1		Keine besondere Softwarerelevanz	
MI-002-5.2	Eignung	Lebensdauer der Energiequelle	I2-5
MI-002-5.3	Eignung	Tauglichkeit der Anzeige	I2-3
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	Elektronische Mengenumwerter	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 Auswir-kung 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 elektromagneti-schen 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		

MID			Software-leitfaden
Artikel / Anhang Nr. (AI = Anhang I)	**Bezeichnung**	**Anmerkung**	**Anforderung Nr.**
	Anhang MI-006		
MI-006-IV, MI-006-V	Selbsttätige Waage zum diskontinuierlichen und kontinuierlichen Totalisieren	Fehlererkennung Backup-Einrichtungen	I6-1 bis I6-2
	Anhang MI-007		
MI-007-8	Zulässige Auswirkungen von Störgrößen	Backup-Einrichtungen	I7-1
	Anhang MI-008		
	Anhang MI-009		
	Anhang MI-010		

14 Verweise und Literatur

[1] Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments. Official Journal of the European Union L 135/1, 30.4.2004

[2] Software Requirements and Validation Guide, Version 1.00, 29 October 2004, European Growth Network “MID-Software”, contract number G7RT-CT-2001-05064, 2004

[3] Software Requirements on the Basis of the Measuring Instruments Directive, WEMEC 7.1, Issue 2, 2005

15 Revisionshistorie

Ausgabe	Datum	Wichtige Änderungen
1	Mai 2005	Richtlinie 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. Ergänzen um einer 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	Februar 2011	Überarbeitung des Kapitels 5 (Teil U): Weiterentwicklung in Bezug auf Betriebssysteme Ersetzen des Begriffs "Komponente" in der gesamten Richtlinie 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).

Tabelle 15-1: Revisionshistorie