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

WELMEC Leitfaden 7.2

Softwareleitfaden

(Europäische Messgeräterichtlinie 2014/32/EU)

Version 2023

Zur Information:

Dieser Leitfaden wird der Arbeitsgruppe Messinstrumente (Sachverständigengruppe E01349 der Europäischen Kommission) zur Berücksichtigung für zukünftige Referenzierung auf der Europa-Webseite zur Verfügung gestellt.

WELMEC

European cooperation in legal metrology

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

Herausgeber:
WELMEC Sekretariat

E-Mail: secretary@welmec.org

Website: https://www.welmec.org

Softwareleitfaden

(Europäische Messgeräterichtlinie 2014/32/EU)

Inhaltsverzeichnis

Vorwort

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

Dieser Leitfaden hat rein empfehlenden Charakter und legt keine Beschränkungen oder zusätzlichen technischen 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 des WELMEC e.V. eine gute Praxis dar, der gefolgt werden sollte.

Obwohl sich dieser Leitfaden auf Messgeräte im Geltungsbereich der MID-Bestimmungen bezieht, sind die Ergebnisse allgemeiner Natur und lassen sich darüber hinaus anwenden.

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

Einleitung

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

Wird nach diesem Leitfaden verfahren, ist davon auszugehen, dass die softwarebezogenen Anforderungen der MID eingehalten werden. Des Weiteren ist davon auszugehen, dass alle Benannten Stellen diesen Leitfaden als MID-konforme Auslegung hinsichtlich der Software akzeptieren. Um den Zusammenhang zwischen den in diesem Leitfaden aufgestellten Anforderungen und den entsprechenden MID-Anforderungen aufzuzeigen, wurde dem Leitfaden eine Querverweisliste als Anhang beigefügt (Kapitel 13).

Aktuelle Informationen zu den Leitfäden und zur Arbeit der WELMEC Arbeitsgruppe 7 sind auf der Webseite verfügbar.

1 Begriffe

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

Akzeptable Lösung *(acceptable solution)*: Gestaltung oder Prinzip eines Softwaremoduls, einer Hardwarekomponente oder einer Funktionseinheit, bei der oder dem die zutreffende Anforderung als erfüllt angesehen wird.

Anmerkung: 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.

Audit Trail *(audit trail)*: Zusammenhängende Daten, die zeitgestempelte Nachweise von Ereignissen enthalten, z. B. Änderungen von Parameterwerten eines Messgerätes oder Softwareupdates oder andere Aktivitäten, die rechtlich relevant und für die metrologischen Eigenschaften entscheidend sind.

Anmerkung: Zu Beispielen von Ereignissen, die in einem Audit Trail protokolliert werden, siehe Ereignis.

Authentifizierung *(authentication)*: Der Prozess der Überprüfung der erklärten oder vorgeblichen Identität eines Benutzers, Prozesses, Messgerätes oder einer Software.

Anmerkung: Dies kann notwendig sein, wenn überprüft werden soll, ob heruntergeladene Software vom Eigentümer einer Baumusterprüfbescheinigung stammt.

Authentizität *(authenticity)*: Das Ergebnis einer Authentifizierung (erfolgreich oder nicht erfolgreich).

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

Gerät mit zweckgebundener Hard- und Software (Typ P) *(built-for-purpose device)*: Ein Gerät, das für einen spezifischen Zweck einer metrologischen Aufgabe entwickelt worden ist.

Anmerkung 1: Geräte mit zweckgebundener Hard- und Software können Geräte einschließen, die kein Betriebssystem enthalten.

Anmerkung 2: Falls ein Betriebssystem vorhanden ist, kann nicht direkt darauf zugegriffen werden.

Komponente der Kategorie 1 *(category 1 component)*: Die Komponenten, die Teil des Messprozesses sind, d. h. die mit Messdaten arbeiten, um den endgültig gemessenen quantitativen Wert zu erstellen und gemeinsam mit messergebnisrelevanten Daten anzuzeigen.

Komponente der Kategorie 2 *(category 2 component)*: Die Komponenten, die das Messergebnis weiterverarbeiten, ohne den endgültig gemessenen quantitativen Wert und zugehörige messergebnisrelevante Daten zu verändern.

Zertifizierung von Schlüsseln *(certification of keys)*: Der Prozess der Zuordnung eines öffentlichen Schlüssels zu einer Person, Organisation oder anderen Instanz.

Prüfeinrichtung *(checking facility)*: Eine Einrichtung, die Bestandteil eines Messgeräts oder einer Komponente ist und die die Erkennung und Behandlung signifikanter Defekte ermöglicht.

Anmerkung: Mit „Behandlung“ ist jede adäquate Reaktion eines Messgeräts gemeint (optisches Signal, akustisches Signal, Verhinderung des Messprozesses etc.).

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)*: Ein Teil eines Messgeräts, der es ermöglicht, Informationen automatisch zwischen *Messgeräten,* Komponenten von Messgeräten oder externen Systemen auszutauschen.

Anmerkung 1: Kommunikationsschnittstellen können drahtgebunden, optisch, drahtlos etc. realisiert sein und sind üblicherweise so entworfen, dass sie ein bestimmtes Protokoll nutzen.

Anmerkung 2: Diese Definition deckt nicht die Kommunikation zwischen Softwaremodulen innerhalb des Messgeräts oder derselben Komponente ab.

Komponente *(component)*: Ein identifizierbarer Hardwareteil eines Messgeräts oder Teilgeräts, der eine bestimmte Funktion oder Funktionen ausführt und der separat gemäß metrologischer oder technischer Leistungsanforderungen bewertet werden kann.

Anmerkung: siehe WELMEC-Leitfaden 8.8.

Vertraulichkeit *(confidentiality)*:
Die Eigenschaft, dass eine Information unautorisierten Individuen, Entitäten oder Prozessen weder zugänglich gemacht noch offengelegt wird.

Kryptografisches Zertifikat *(cryptographic certificate)*: Ein Datensatz, der einen öffentlichen Schlüssel enthält, der zu einem Messgerät, einer Komponente oder einer Person gehört, zzgl. einer eindeutigen Identifikation des Subjekts, z. B. einer Seriennummer des Messgeräts oder ein Name oder eine Geheimzahl (PIN) der Person, zzgl. eines Ablaufdatums.

Kryptografisches Mittel *(cryptographic means)*: Ein Mittel wie Verschlüsselung und Entschlüsselung, das dem Ziel dient, Informationen gegenüber nichtautorisierten Personen zu verstecken, oder Hashes und elektronische Signaturen, um Integrität and Authentizität zu gewährleisten.

Datendomäne *(data domain)*: Ein Bereich im Speicher, den jedes Programm benötigt, um Daten zu verarbeiten.

Anmerkung: Datendomänen können zu einem Softwaremodul oder zu mehreren Modulen gehören.

Gerätespezifischer Parameter *(device-specific parameter)*: Ein *rechtlich relevanter* Parameter, dessen Wert vom einzelnen gesetzlich geregelten Gerät, einer Komponente und/oder einem Softwaremodul abhängt.

Anmerkung: Gerätespezifische Parameter umfassen Einstellparameter (z. B. Anpassung des Messbereichsumfangs oder andere Justierungen oder Korrekturen) und Konfigurationsparameter (z. B. Maximalwert, Minimalwert, Maßeinheiten usw.).

Elektronisches Messgerät *(electronic measuring instrument)*: Ein Messgerät, das dazu bestimmt ist, eine elektrische oder nichtelektrische Größe mit elektronischen Mitteln zu messen, und/oder das mit elektronischen Teilen bestückt ist.

Anmerkung: Im Rahmen dieses Leitfadens werden Zusatzeinrichtungen, vorausgesetzt, sie unterliegen der metrologischen Kontrolle, als Teil des Messgerätes angesehen.

Elektronische Signatur *(electronic signature)*: Ein Softwaremittel, welches an Software oder Daten angefügt wird, um den Ursprung der Software oder der Daten zu verifizieren, d. h., um deren Authentizität nachzuweisen, oder um zu prüfen, ob Software oder Daten unverändert sind, d. h. ihre Integrität nachzuweisen.

Anmerkung 1: Für elektronische Signierung wird im Allgemeinen ein Public-Key-System verwendet, also ein Schlüsselpaar, von dem nur ein Schlüssel geheim gehalten werden muss, während der andere öffentlich sein kann.

Anmerkung 2: Der private Schlüssel wird verwendet, wenn Software oder Daten signiert werden. Der öffentliche Schlüssel wird verwendet, wenn Software oder Daten vor Verwendung verifiziert werden.

Anmerkung 3: Die Verifizierungsinstanz kann ggf. ein kryptografisches Zertifikat der signierenden Instanz benötigen, um sich der Authentizität des öffentlichen Schlüssels sicher zu sein.

Ereignis *(event)*: Eine Aktion, die die metrologischen Daten und/oder Charakteristiken des Messgeräts beeinflussen kann.

Anmerkung: Beispiele für solch ein Ereignis sind die Änderung eines rechtlich relevanten Parameters oder eine Modifizierung oder Aktualisierung der rechtlich relevanten Software.

Ausführbarer Code *(executable code)*: Die digitale Information, die in einem Messgerät oder einer Komponente installiert ist (EPROM, Festplatte etc.).

Anmerkung: Dieser Code wird vom Prozessor (CPU) des Messgeräts interpretiert und in bestimmte logische, arithmetische, Entschlüsselungs- oder Datentransportoperationen übersetzt.

Hashfunktion *(hash function)*: Eine (mathematische) Funktion, die Werte aus einem großen (möglicherweise sehr großen) Bereich auf ein kleineres Intervall abbildet.

Anmerkung: Bei einer „guten“ Hashfunktion sind die Ergebnisse nach dem Anwenden auf eine (große) Menge von Werten aus dem Bereich gleichmäßig (und scheinbar zufällig) über das gesamte Intervall verteilt.

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

Integrität *(integrity)*: Die Eigenschaft, dass Software, Messdaten und Parameter nicht geändert wurden.

Schnittstelle *(interface)*: Eine gemeinsame Grenze zwischen zwei funktionalen Einheiten, die durch verschiedene Charakteristiken bzgl. Funktionen, physischen Verbindungen, Signalaustausch oder anderen Charakteristiken der Einheiten (sofern angemessen) definiert ist.

Unterbrechbare kumulierende Messung *(interruptible cumulative measurement)*: Ein Prozess einer kumulierenden Messung eines Mengenwerts einer Messgröße, der während der üblichen Ausführung einfach und schnell unterbrochen werden kann.

Anmerkung 1: Beispiele sind: a) selbsttätige Waagen zum Totalisieren, b) Zapfsäulen.

Anmerkung 2: Siehe auch nichtunterbrechbare Messung.

IT-Konfiguration *(IT configuration)*: Der Aufbau des *Messgerätes* hinsichtlich der IT-Funktionen und -Eigenschaften. In diesem Leitfaden werden vier IT-Konfigurationen betrachtet: *Speicherung von Messdaten, Messdatenübertragung, Software-Download* und *Softwaretrennung* (siehe auch *Basiskonfiguration*). Die Begriffe sind entsprechend auf *Teilgeräte* anwendbar.

Schlüssel *(key)*: Eine geeignete Zahl oder Zeichenfolge, die zum Verschlüsseln und/oder Entschlüsseln von Informationen verwendet wird.

Rechtlich relevant *(legally relevant)*:
Die Eigenschaft, die wesentlichen Anforderungen von Anhang I erfüllen zu müssen und/oder einen Einfluss auf die Einhaltung der wesentlichen Anforderungen von Anhang I und den gerätespezifischen Anforderungen der MID und/oder der Anhänge I und III der NAWID zu haben.
Anmerkung 1: Ein Messgerät, das der gesetzlichen Kontrolle unterliegt, muss den wesentlichen Anforderungen genügen, siehe Artikel 6 der MID und Artikel 4 der NAWID. Daher ist das Messgerät per Definition rechtlich relevant.

Anmerkung 2: Dort, wo gerätespezifische Anhänge der MID wesentliche Anforderungen für Teilgeräte festlegen, sind besagte Teilgeräte, die Teil des Messgeräts sind, ebenfalls rechtlich relevant.

Anmerkung 3: Siehe auch Kapitel 15 für weitere Erklärungen.

Fehlergrenze (eines Messgeräts) *(maximum permissible error (of a measuring instrument))*: Der Maximalwert des Messfehlers bezüglich eines bekannten Referenzmengenwerts, der für eine Messung, ein Messgerät oder ein Messsystem durch Spezifikationen oder Regularien erlaubt ist.

Gemessener Mengenwert *(measured quantity value)*: Der Mengenwert, der ein Messergebnis repräsentiert.

Metadaten des gemessenen Mengenwerts *(measured quantity value metadata)*: Die Metadaten, die zum gemessenen Mengenwert gehören.

Messung *(measurement)*: Der Prozess der experimentellen Bestimmung eines oder mehrerer Mengenwerte, die einer Größe sinnvoll zugeordnet werden können.

Anmerkung 1: Die Messung betrifft nicht Nenneigenschaften.

Anmerkung 2: Eine Messung impliziert einen Vergleich von Mengen oder die Zählung von Einheiten.

Anmerkung 3: Die Messung setzt eine dem Verwendungszweck eines Messergebnisses entsprechende Größenbeschreibung, ein Messverfahren und ein nach dem vorgegebenen Messverfahren arbeitendes kalibriertes Messsystem einschließlich der Messbedingungen voraus.

Anmerkung 4: Kapitel 14 illustriert die Begriffe und Definitionen, die den Messprozess betreffen, und ihre Verwendung in diesem Dokument.

Messdaten *(measurement data)*: Die Daten, die während des Messprozesses verwendet werden.

Anmerkung: Messdaten beinhalten den gemessenen Mengenwert, messergebnisrelevante Daten und Messprozessdaten, siehe Kapitel 14.

Anmerkung: Der gemessene Mengenwert und die messergebnisrelevanten Daten sind beide Bestandteile des Messergebnisses und bilden zusammen mit den Messprozessdaten die Messdaten, siehe Kapitel 14.

Messmetadaten *(measurement metadata)*: Die Metadaten, die sich auf den Messprozess beziehen.

Anmerkung: Messmetadaten beinhalten die Metadaten des gemessenen Mengenwerts, messergebnisrelevante Metadaten und Messprozessmetadaten, siehe Kapitel 14.

Messfehler *(measurement error)*: Der gemessene Mengenwert abzüglich des Referenzmengenwerts.

Anmerkung 1: Der Begriff „Messfehler“ kann sowohl verwendet werden, wenn a) es sich um einen einzelnen Referenzmengenwert handelt, der auftritt, wenn eine Kalibrierung mithilfe eines Messnormals durchgeführt wird, dessen gemessener Mengenwert eine vernachlässigbare Messunsicherheit aufweist oder wenn ein konventioneller Mengenwert angegeben ist. In diesem Fall ist der Messfehler bekannt. Der Begriff kann weiterhin verwendet werden, wenn b) eine Messgröße durch einen eindeutigen wahren Mengenwert oder eine Menge wahrer Mengenwerte im vernachlässigbaren Bereich dargestellt werden soll. In diesem Fall ist der Messfehler nicht bekannt.

Anmerkung 2: Eine Messung impliziert einen Vergleich von Mengen oder die Zählung von Einheiten.

Messprozessdaten *(measurement process data)*: Die Daten, die während eines Messprozesses zur Erzeugung des Messergebnisses verwendet werden.

Anmerkung: Beispiele für Messprozessdaten sind Werte von Messparametern, Werte von Verbindungseinstellungen und Werte von Sitzungsparametern.

Messprozessinformationen *(measurement process information)*: Die Menge von Werten qualitativer oder quantitativer Variablen, die den Messprozess repräsentieren.

Anmerkung: Messprozessinformationen beinhalten Messprozessdaten und Messprozessmetadaten.

Messprozessmetadaten *(measurement process metadata)*: Die Metadaten, die sich auf den Messprozess beziehen.

Anmerkung: Beispiele von Messprozessmetadaten sind das Format der Messparameter, das Format der Verbindungseinstellungen, das Format von Sitzungsparametern.

Messergebnis *(measurement result)*: Der Satz von Mengenwerten, die einer Messgröße zusammen mit allen anderen verfügbaren messergebnisrelevanten Daten zugeordnet werden.

Anmerkung: Beispiele messergebnisrelevanter Daten sind Markierungen und Aufschriften, die benötigt werden, um dem Verwender die Bedeutung des Messergebnisses zu verdeutlichen, siehe Artikel 10.2 des Anhangs I der MID.

Anmerkung: Beispiele für messergebnisrelevante Daten sind Informationen über die Herkunft der Messdaten, die zur Bestimmung eines bestimmten Geschäftsvorgangs erforderlich sind, z. B. die Identifizierung des Sensors, siehe Artikel 11.1 des Anhangs I der MID.

Anmerkung: Messergebnisrelevante Daten sind auch Informationen zur Identifizierung des jeweiligen Geschäftsvorgangs, z. B. Nummer der Messung, Datum und Uhrzeit der Messung, siehe Artikel 11.1 von Anhang I der MID.

Anmerkung: Für den Fall, dass die Preisberechnung Teil der rechtlich relevanten Software ist, sind der Einheitspreis und der zu zahlende Preis Teil der

messergebnisrelevanten Daten, siehe die entsprechenden instrumentenspezifischen Anhänge der MID und Anhang I der NAWID.

Anmerkung: Das Messergebnis (einschließlich des gemessenen Mengenwerts) wird für die rechtlich relevanten Zwecke, z. B. den Abschluss eines Geschäftsvorgangs, verwendet.

Messergebnisrelevante Daten *(measurement result relevant data)*: Die Daten, die während des Messprozesses verwendet werden, um das Messergebnis zu erzeugen.

Anmerkung: Beispiele messgeräterelevanter Daten sind Digital- oder Analogwerte der Sensor- oder Messgeräte-ID in Fällen, in denen sie Teil des Messergebnisses sind, siehe Kapitel 14.

Messergebnisrelevante Informationen *(measurement result relevant information)*: Die Menge von Werten qualitativer oder quantitativer Variablen, die für das Messergebnis relevant sind.

Anmerkung: Messergebnisrelevante Informationen beinhalten messergebnisrelevante Daten und messergebnisrelevante Metadaten.

Messergebnisrelevante Metadaten *(measurement result relevant metadata)*: Die Metadaten, die sich auf die Erzeugung des Messergebnisses beziehen.

Anmerkung: Beispiele messergebnisrelevanter Metadaten sind das Format der Digital- oder Analogwerte vom Sensor, das Format des gemessenen Mengenwertes oder das Format der Messgeräte-ID in Fällen, in denen sie Teil des Messergebnisses ist.

Messgerät *(measuring instrument)*: Ein Gerät zur Durchführung von Messungen, allein oder in Verbindung mit einem oder mehreren Zusatzgeräten.

Metadaten *(metadata)*: Die Daten über Daten oder Datenelemente, ggf. einschließlich deren Datenbeschreibungen, sowie Daten über Dateneigentum, Zugriffspfade, Zugriffsrechte und Datenvolatilität.

Messgeräte mit Universalgerät (Typ U) *(measuring instrument using a universal device)*: *Messgerät*, das einen Universalrechner, 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.

Modul *(module)*: Eine Softwareinstanz, wie bspw. ein Programm, eine Subroutine, eine Bibliothek, ein Parameter oder ein Datensatz oder andere Objekte und deren Datendomänen, die in Verbindung mit anderen Instanzen stehen können.

Anmerkung: Die Software eines Messgeräts besteht aus einem oder mehreren Modulen.

Nichtunterbrechbare kumulierende Messung *(non-interruptible cumulative measurement)*: Eine kumulierende Messung ohne definiertes Ende, die nicht vom Verwender/Bediener unterbrochen und fortgesetzt werden kann, ohne das Ergebnis der Messung ungültig zu machen.

Anmerkung 1: Beispiele umfassen: a) selbsttätige Waagen zum kontinuierlichen Totalisieren, b) Wärmezähler.

Anmerkung 2: Siehe auch unterbrechbare kumulierende Messung.

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*).

Betriebssystem *(operating System)*: Die Software, die die Programmausführung steuert und Dienste wie Ressourcenzuteilung, Auftragssteuerung, I/O-Kontrolle und Datenmanagement zur Verfügung stellt.

Anmerkung 1: Andere Programme (wie Editoren, Office-Programme etc.), die nicht für diese Aufgaben vorgesehen sind, zählen nicht zum Betriebssystem.

Anmerkung 2: Bei Komponenten der Kategorie 1 oder kompletten Messgeräten bestehen die rechtlich relevanten Teile des Betriebssystems in der Regel mindestens aus dem Bootloader, dem Kernel, den Schnittstellen (Hardware und Interprozesskommunikation), den (Hintergrund-)Diensten, der Verwaltung von Benutzerrechten, kryptografischen Bibliotheken sowie den Konfigurationsdateien dieser Teile.

Anmerkung 3: Bei Komponenten der Kategorie 2 bestehen die rechtlich relevanten Teile des Betriebssystems in der Regel mindestens aus den Schnittstellen (Hardware und Interprozesskommunikation), der Verwaltung von Benutzerrechten, kryptografischen Bibliotheken sowie den Konfigurationsdateien dieser Teile.

Rückwirkungsfreie Softwareschnittstelle *(protective interface)*: Ein rechtlich relevantes Softwaremodul, das den gesamten Datenfluss zu rechtlich relevanten Softwaremodulen kontrolliert, um unzulässigen Einfluss zu verhindern.

Schutz *(protection)*: Die Mittel, um Messdaten, Parameter, Messgeräte, Komponenten oder Softwaremodule so zu schützen, dass eine Einflussnahme entweder ausgeschlossen oder nachweisbar ist.

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

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

Risikoklasse *(risk class)*: Eine Klasse von Messgerätebauarten mit fast identischen Risikobewertungen.

Siegel *(sealing)*: Ein Mittel, das dazu eingesetzt wird, Software, Parameter, Messdaten, ein Messgerät, eine Komponente oder ein Softwaremodul gegen Modifizierung, Nachjustierung, Entfernung von Komponenten oder Softwaremodulen etc. zu schützen.

Anmerkung: Dies kann durch Hardwaremaßnahmen, Softwaremaßnahmen oder durch eine Kombination aus beidem erreicht werden.

Sicherung *(securing)*: Ein Mittel, das unautorisierten Zugriff auf Hardware, Software, Parameter oder Messdaten verhindert.

Anmerkung: Dies kann mit Hilfe von Passwörtern erreicht werden.

Signaturalgorithmus *(signature algorithm)*:
Ein kryptografischer Algorithmus, der mit Hilfe eines Signaturschlüssels einen Hashcode verschlüsselt und der es erlaubt, den verschlüsselten Hashcode wieder zu

entschlüsseln, sollte der entsprechende Entschlüsselungs-Signaturschlüssel zur Verfügung stehen.

Signifikanter Defekt *(significant defect)*: Ein Vorfall, der unerwünschte Auswirkungen auf die Konformität des Messgeräts hat, oder ein Fehler.

Anmerkung: Beispiele signifikanter Defekte umfassen a) Löschen des Audit Trails, b) unzulässige Parameteränderungen, c) unautorisierte Updates und d) zufällige Softwareänderungen aufgrund physischer Effekte.

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

Softwareprüfung *(software examination)*: Ein technischer Arbeitsschritt, der daraus besteht, eine oder mehrere Charakteristiken der Software gemäß einer spezifischen Prozedur (z. B. Dokumentenanalyse, Programmausführung unter kontrollierten Bedingungen) zu bestimmen.

Software-Identifikation *(software identification)*: Eine Folge von lesbaren Zeichen (z. B. eine Versionsnummer, Prüfsumme), die die betrachtete Software oder das Softwaremodul repräsentiert.

Anmerkung: Die Software-Identifikation kann während der Verwendung an einem Gerät überprüft werden.

Softwareschnittstelle *(software interface)*: Ein Programmcode und eine dedizierte Datendomäne, die Daten zwischen Softwaremodulen empfangen, filtern oder übertragen.

Anmerkung 1: Eine Softwareschnittstelle ist nicht notwendigerweise rechtlich relevant.

Anmerkung 2: Eine Softwareschnittstelle ist eine Schnittstelle zwischen zwei oder mehr Softwaremodulen, die verwendet wird, um Daten auszutauschen und Befehle zu übertragen.

Softwaretrennung *(software separation)*: Die Trennung von Software in Messgeräten oder Komponenten, die in rechtlich relevante Softwaremodule und nicht rechtlich relevante Softwaremodule unterteilt werden können.

Anmerkung: Diese Module kommunizieren über eine rückwirkungsfreie Softwareschnittstelle, siehe S3.

Quellcode *(source code)*: Ein Computerprogramm, geschrieben in einer Form (Programmiersprache), die lesbar und editierbar ist.

Anmerkung: Quellcode wird in ausführbaren Code kompiliert oder interpretiert.

Speichergerät *(storage device)*:
Ein Gerät zum Speichern von Messdaten, die notwendig sind, um das Messergebnis zu erstellen, und/oder zum Speichern des Messergebnisses, um es für spätere rechtlich relevante Zwecke zur Verfügung stellen zu können.

Teilgerät *(sub-assembly)*: Ein Hardwaregerät (Hardware-Einheit), das als solches in den gerätespezifischen Anhängen genannt wird, das selbstständig funktioniert und zusammen mit anderen Teilgeräten (oder einem Messgerät), mit denen es kompatibel ist, ein Messgerät bildet [MID, Artikel 4 (2)].

TEC *(TEC)*: Baumusterprüfbescheinigung.

Zeitstempel *(time stamp)*: Ein eindeutiger Wert, z. B. in Sekunden, oder eine Datums- und Uhrzeitzeichenfolge, die das Datum und/oder die Uhrzeit angibt, zu der ein bestimmter Vorfall (z. B. eine Messung oder ein Ereignis) aufgetreten ist.

Messdatenübertragung *(transmission of measurement data)*: Der elektronische Transport von Messdaten über Kommunikationspfade oder andere Medien zu einem Empfänger.

Trust Centre *(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.

Bauartspezifischer Parameter *(type-specific parameter)*: Ein rechtlich relevanter Parameter mit einem Wert, der von der Bauart eines gesetzlich geregelten Messgeräts, einer Komponente und/oder eines Softwaremoduls abhängig ist.

Anmerkung: Bauartspezifische Parameter sind Teil der rechtlich relevanten Software.

Universalgerät *(universal device)*: Ein Gerät, das nicht für einen bestimmten Zweck konstruiert ist, sondern durch Software für eine rechtlich relevante Aufgabe angepasst werden kann.

Nutzerschnittstelle *(user interface)*: Eine Schnittstelle, die es ermöglicht, Informationen zwischen einem Menschen und dem Messgerät oder seinen (Hardware-) Komponenten oder Softwaremodulen auszutauschen.

Anmerkung: Typische Beispiele für Nutzerschnittstellen sind Schalter, Tastatur, Maus, Display, Monitor, Drucker, Touch-Screen, ein Softwarefenster auf einem Bildschirm einschließlich der Software, die dieses erzeugt.

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

Verifikation *(verification)*: Die Bereitstellung eines objektiven Nachweises dafür, dass ein gegebener Gegenstand spezifische Anforderungen erfüllt.

Verifizierung eines Messgeräts *(verification of a measuring instrument)*: Das Konformitätsbewertungsverfahren (außer der Baumusterprüfung), das zur Anbringung eines Prüfzeichens und/oder zur Ausstellung eines Prüfzertifikats führt.

2 Verwendung des Leitfadens

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

2.1 Gesamtstruktur des Leitfadens

Der Leitfaden besteht aus einem strukturierten Satz von Anforderungsblöcken. Die Gesamtstruktur des Leitfadens berücksichtigt die Einteilung von Messgeräten in Basiskonfigurationen sowie die Einteilung in sogenannte IT-Konfigurationen. Die Anforderungsblöcke werden durch instrumentenspezifische Anforderungen ergänzt.

Demnach gibt es drei Arten von Anforderungssätzen:

1. Anforderungen für zwei Basiskonfigurationen von Messgeräten (als Typ P und U bezeichnet) sowie Anforderungen für Betriebssysteme (als Anhang O bezeichnet),
2. Anforderungen für IT-Konfigurationen (als Anhänge L, T, S und D bezeichnet) und
3. Instrumentenspezifische Anforderungen (als Anhänge I1, I2, … bezeichnet).

Die erste Anforderungsart ist auf alle Geräte anwendbar. Bezüglich des Betriebssystems und der Anwendbarkeit des betreffenden Anhangs O, siehe Unterkapitel 2.2. Die zweite Anforderungsart betrifft die folgenden IT-Konfigurationen: Speicherung von Messdaten (L), Messdatenübertragung (T), Software-Download (D) sowie Softwaretrennung (S). Jeder Satz dieser Anforderungen ist nur dann anwendbar, wenn die dazugehörige Funktion vorhanden ist.
Die letzte Anforderungsart bietet eine Sammlung weiterer, instrumentenspezifischer Anforderungen. Die Nummerierung ist an die Nummerierung der instrumentenspezifischen Anhänge der MID angelehnt. Der Satz von Anforderungsblöcken, der für ein bestimmtes Messgerät verwendet werden kann, ist schematisch in **Abbildung 2-1** dargestellt.

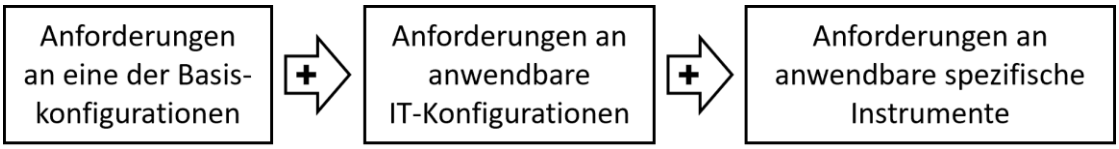
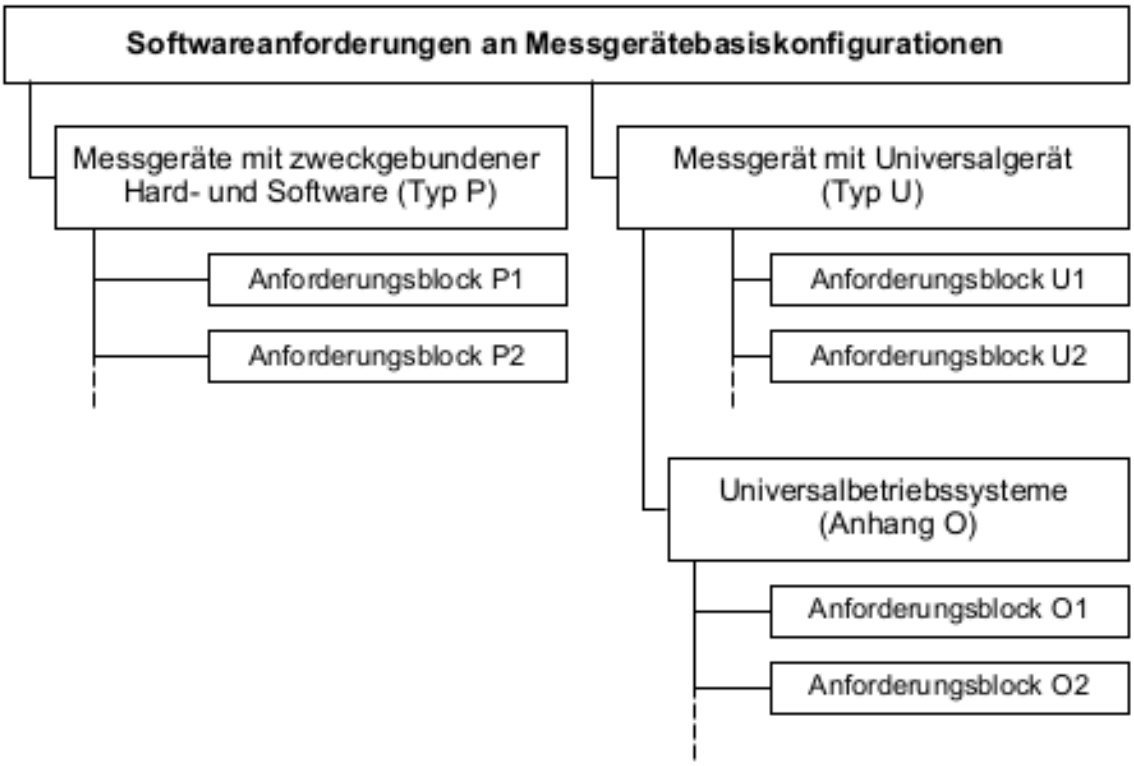
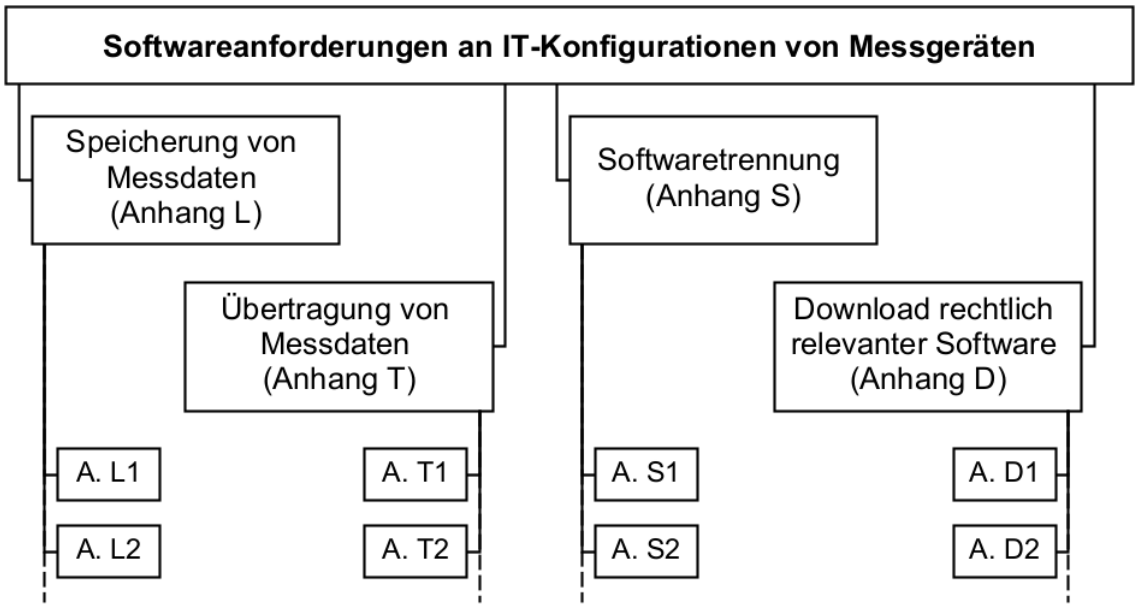


Abbildung 2-1: Arten von Anforderungssätzen, die auf ein Gerät angewandt werden sollten


Softwareanforderungen an Messgerätebasiskonfigurationen
Messgeräte mit zweckgebundener Hard- und Software (Typ P)
Messgerät mit Universalgerät (Typ U)
Anforderungsblock P1
Anforderungsblock P2
Anforderungsblock U1
Anforderungsblock U2
Universalbetriebssysteme (Anhang O)
Anforderungsblock O1
Anforderungsblock O2


Softwareanforderungen an IT-Konfigurationen von Messgeräten
Speicherung von Messdaten (Anhang L)
Übertragung von Messdaten (Anhang T)
Softwaretrennung (Anhang S)
Download rechtlich relevanter Software (Anhang D)
A. L1
A. L2
A. T1
A. T2
A. S1
A. S2
A. D1
A. D2

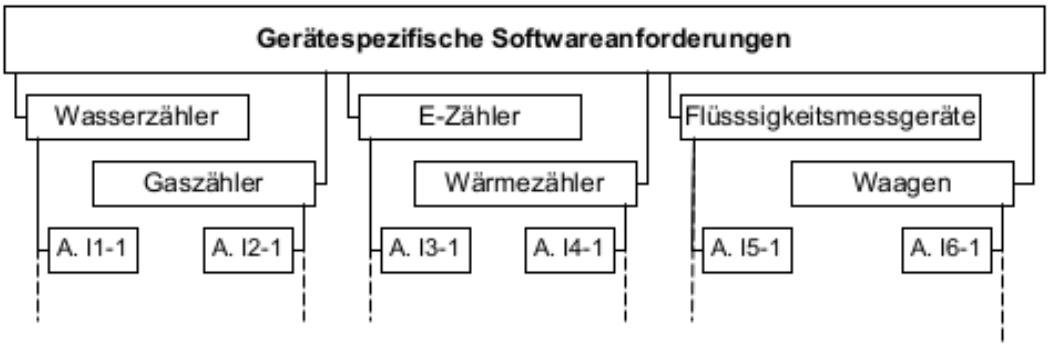


Abbildung 2-2: Übersicht über die Anforderungssätze

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

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

2.2 Auswahl der geeigneten Teile des Leitfadens

Der vorliegende umfassende Softwareleitfaden ist auf eine Vielzahl von Geräten anwendbar. Der Leitfaden ist modular aufgebaut. Die entsprechenden Anforderungssätze lassen sich durch Beachtung folgenden Verfahrens leicht auswählen.
Siehe **Abbildung 2-2** für einen Überblick über die unterschiedlichen Anforderungssätze.

Schritt 1: *Auswahl der Basiskonfiguration (P oder U)*

Es muss nur einer der beiden Anforderungssätze für Basiskonfigurationen angewendet werden. Dabei ist zu entscheiden, mit welcher Basiskonfiguration das Gerät übereinstimmt: als Messgerät mit zweckgebundener Hard- und Software (Typ P, siehe Kapitel 4) oder als Messgerät mit Universalgerät (Typ U, siehe Kapitel 5). Falls Typ U ausgewählt wird und das Messgerät mit einem rechtlich relevanten Betriebssystem ausgestattet ist, d. h., das Betriebssystem wird benutzt, um die wesentlichen Anforderungen der MID zu erfüllen, oder kann genutzt werden, um die Erfüllung der Anforderungen zu beeinflussen, dann muss der Anhang für Betriebssysteme (Anhang O) gleichzeitig angewandt werden. Falls Anhang O nicht anwendbar ist, da die im Anhang genannten Voraussetzungen nicht erfüllt sind, muss die gesamte Software des Geräts als Typ P behandelt werden. Falls nur ein Teilgerät oder eine Komponente des Geräts untersucht wird, entscheide man sich entsprechend für das jeweilige Teilgerät. Anzuwenden ist immer der vollständige Anforderungssatz, der zur jeweiligen Basiskonfiguration und entsprechend Anhang O gehört.

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

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

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

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

Schritt 4: *Auswahl der geeigneten Risikoklasse (Anhang I)*

Die Risikoklasse ist entsprechend der Definition im jeweiligen instrumentenspezifischen Anhang I, Kapitel 11 auszuwählen. Dort ist die Risikoklasse einheitlich für eine Messgeräteart definiert oder weiter in Kategorien, Anwendungsfelder usw. unterteilt. Sobald die entsprechende Risikoklasse identifiziert wurde, müssen nur noch die jeweiligen Anforderungen und die Validierungsanleitung berücksichtigt werden.

2.3 Arbeit mit einem Anforderungsblock

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

<table>
<tr><td colspan="3">Titel der Anforderung</td></tr>
<tr><td colspan="3">Hauptaussage der Anforderung</td></tr>
<tr><td colspan="3">Detaillierende Anmerkungen (Anwendungsbereich, zusätzliche Erklärungen, Ausnahmen usw.)</td></tr>
<tr><td colspan="3">Erforderliche Dokumentation (eventuell nach Risikoklassen unterteilt)</td></tr>
<tr><td>Validierungsanleitung für eine Risikoklasse</td><td>Validierungsanleitung für eine andere Risikoklasse</td><td>...</td></tr>
<tr><td>Beispiel einer akzeptablen Lösung für eine Risikoklasse</td><td>Beispiel einer akzeptablen Lösung für eine andere Risikoklasse</td><td>...</td></tr>
</table>

Abbildung 3-3: Aufbau eines Anforderungsblocks

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

Hinweise für den Hersteller:

- Erfüllen der Hauptaussage sowie der zusätzlichen detaillierenden Anmerkungen.
- Bereitstellen der Dokumentation wie gefordert.

- Akzeptable Lösungen sind Beispiele, die die Anforderung erfüllen. Es besteht keine Verpflichtung, sie zu befolgen.
- Die Validierungsanleitung hat informativen Charakter.

Hinweise für Benannte Stellen:

- Die Hauptaussage sowie die zusätzlichen detaillierenden Anmerkungen sind zu beachten.
- Die Validierungsanleitung ist zu befolgen.
- Die Vollständigkeit der bereitgestellten Dokumentation ist zu bestätigen.

2.4 Arbeiten mit Checklisten

Checklisten sind ein Mittel, um sicherzustellen, dass alle Anforderungen innerhalb eines Kapitels durch den Hersteller oder Prüfer abgedeckt wurden. Sie sind Teil des Prüfberichts. 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 Anforderungsblöcken zu entnehmen.

Durchführung:

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

3 Definition von Risikoklassen

3.1 Allgemeiner Grundsatz

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

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

3.2 Beschreibung der Stufen von Gegenmaßnahmen für die Risikofaktoren

Für die jeweiligen Stufen werden die folgenden Festlegungen benutzt:

Stufen für den Softwareschutz

Niedrig: Es sind keine besonderen Schutzmaßnahmen gegen absichtliche Änderungen erforderlich.

Mittel: Die Software ist gegen absichtliche Änderungen geschützt, die mit Hilfe von leicht verfügbaren und einfachen, gängigen Softwarewerkzeugen (z. B. Texteditoren) vorgenommen werden können.

Hoch: Die Software ist gegen absichtliche Änderungen geschützt, die mit Hilfe von anspruchsvollen Softwarewerkzeugen (z. B. Debuggern oder Festplatteneditoren, Softwareentwicklungswerkzeugen usw.) vorgenommen werden können.

Stufen für die Softwareprüfung

Niedrig: Mit dem Gerät wird eine Standard-Baumusterfunktionsprüfung durchgeführt. Eine zusätzliche Softwareprüfung ist nicht erforderlich.

Mittel: Zusätzlich zur Prüfung der Stufe "Niedrig" wird die Software auf Basis ihrer Dokumentation geprüft. Die Dokumentation beinhaltet die Beschreibung der Softwarefunktionen, die Parameterbeschreibung usw. Praktische Tests der softwaregestützten Funktionen (Stichproben) können ausgeführt werden, um die Plausibilität der Dokumentation und die Wirksamkeit der Schutzmaßnahmen zu überprüfen.

Hoch: Zusätzlich zu den Prüfungen der Stufe "Mittel" wird ein Tiefentest der Software ausgeführt, normalerweise auf Basis des Quellcodes.

Software-Konformitätsebene

Niedrig: Die rechtlich relevante Software einzelner Geräte gilt als konform mit der rechtlich relevanten Software des in der Prüfung befindlichen Gerätetyps, wenn die Funktionalität der Software der technischen Dokumentation des Gerätetyps entspricht. Der Binärcode der Software selbst muss nicht unbedingt identisch mit der Software des Gerätetyps sein.

Mittel: Zusätzlich zur Konformitätsebene "niedrig" ist der Binärcode der rechtlich relevanten Software einzelner Geräte identisch mit der Software des in der Prüfung (oder Revision) befindlichen Gerätetyps. Softwaretrennung ist erlaubt, wenn die Einschränkungen in Teil S des vorliegenden Leitfadens (Kapitel 9) erfüllt sind.

Hoch: Der Binärcode der vollständigen Software, die in den einzelnen Geräten implementiert ist, ist identisch mit der Software des in der Prüfung befindlichen Gerätetyps. Eine Softwaretrennung ist nicht mehr relevant.

3.3 Ableitung von Risikoklassen

Von den 27 theoretisch möglichen Stufenkombinationen sind nur 3 oder höchstens 6 von praktischem Interesse (Risikoklassen B, C, D, zukünftig A, E und F). Sie decken alle Messgeräteklassen ab, die unter die Bestimmungen der MID fallen. Darüber hinaus bieten sie genügend Spielraum für den Fall geänderter Risikobewertungen. Die Klassen werden in Tabelle 3-1 definiert. Die Tabelle ist so zu interpretieren, dass eine bestimmte Risikoklasse mit Hilfe der entsprechenden Stufenkombination der notwendigen Gegenmaßnahmen definiert wird.

Risikoklasse	Softwareschutz	Softwareprüfung	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 3-1: *Definition der Risikoklassen*

3.4 Interpretation der Risikoklassen

Risikoklasse A: Dies ist die niedrigste Risikoklasse überhaupt. Es sind keine besonderen Maßnahmen gegen absichtliche 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 offengehalten.

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

Die Softwareprüfung wird auf Basis der Dokumentation ausgeführt. Folglich ermöglicht die Baumusterprüfbescheinigung verschiedene Umsetzungen der gleichen Dokumentation, wenn die Messgeräte auf den Markt gebracht werden[1].

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

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

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

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

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

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

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

4.1 Technische Beschreibung

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

Das eingebettete IT-System wird insbesondere wie folgt charakterisiert:

- Die Software ist ausschließlich für den Messzweck konstruiert. Zusätzliche Funktionen für die Sicherung von Software und Daten, für die Übertragung von Daten und den Download von Software gelten als für den Messzweck konstruiert.
- Die Nutzerschnittstelle ist für den Messzweck ausgelegt, d. h., sie wird normalerweise in einem Betriebsmodus verwendet, der der gesetzlichen Kontrolle unterliegt. Das Umschalten in einen Betriebsmodus, der nicht der gesetzlichen Kontrolle unterliegt, ist möglich.
- Ein Betriebssystem oder Subsysteme davon können vorhanden sein, wenn
  - die gesamte Kommunikation von der rechtlich relevanten Software gesteuert wird,
  - sie das Laden oder Ändern von Modulen, Parametern oder Daten oder das Ausführen von Programmen nicht erlauben,
  - sie die Änderung der Umgebung der rechtlich relevanten Anwendung usw. nicht erlauben.
    Dies beinhaltet, dass der Zugangsschutz voreingestellt sein muss und nicht Ergebnis einer entsprechenden nachfolgenden Konfiguration dieser Komponenten ist.
- Die Softwareumgebung ist unveränderlich; es gibt keine internen oder externen Mittel für die Programmierung oder Änderung der Software in ihrem eingebetteten Status. Software-Download ist erlaubt, wenn die spezifischen Anforderungen von Anhang D (Kapitel 10) beachtet werden.

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 Nutzerschnittstelle, der Menüs und der Dialoge.* *c. Den Software-Identifikator bzw. die Software-Identifikatoren der rechtlich relevanten Software.* *d. Einen Überblick über die Systemhardware, z. B. Block-Schaltbild, Computerart(en), Netzwerktyp usw.* *e. Das Betriebshandbuch.*

Risikoklasse B	Risikoklasse C	Risikoklasse D
P2: Software-Identifikation *Die rechtlich relevante Software muss eindeutig gekennzeichnet sein. Der Identifikator bzw. die Identifikatoren müssen dauerhaft durch das Gerät oder auf Befehl oder während des Betriebs angezeigt werden.*		
Detaillierende Anmerkungen: 1. Rechtlich relevante Software-Identifikatoren können unabhängig oder Teil gut strukturierter Identifikatoren sein. Im zweiten Fall müssen die rechtlich relevanten Software-Identifikatoren klar erkennbar sein. 2. Wenn verschiedene Softwareversionen gültige Umsetzungen desselben Baumusters sind (z. B. für Geräte in Risikoklasse B), dann müssen die rechtlich relevanten Software-Identifikatoren die gleichen für diese Versionen sein. 3. Die rechtlich relevanten Software-Identifikatoren werden als bauartspezifische Parameter betrachtet. 4. Die rechtlich relevanten Software-Identifikatoren müssen ohne ein zusätzliches Werkzeug problemlos darstellbar sein. 5. Der bzw. die Identifikatoren werden dauerhaft auf einem geschützten Schild, auf Befehl oder beim Startvorgang dargestellt.		
Erforderliche Dokumentation: 1. Die Dokumentation muss die Software-Identifikatoren auflisten und beschreiben, wie diese erzeugt werden, wie sie geschützt werden, wie sie dargestellt werden und wie sie strukturiert sind, um sowohl zwischen rechtlich relevanten Software-Identifikatoren und anderen unterscheiden als auch ihre Eindeutigkeit bewerten zu können. 2. Die Dokumentation muss aufführen, welches rechtlich relevante Modul von welchem rechtlich relevanten Software-Identifikator abgedeckt ist.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob in der Dokumentation alle rechtlich relevanten Software-Identifikatoren angegeben sind. • ob alle rechtlich relevanten Module klar beschrieben sind, so dass nachvollziehbar ist, welches Modul von welchem Software-Identifikator abgedeckt wird. • die Beschreibung der Erzeugung und Visualisierung aller rechtlich relevanten Software-Identifikatoren. • ob alle rechtlich relevanten Software-Identifikatoren eindeutig sind (besonders bei Revisionen). *Funktionsprüfungen:* • Es ist zu prüfen, ob die rechtlich relevanten Software-Identifikatoren wie in der Dokumentation beschrieben visualisiert werden können. • Es ist nachzuprüfen, ob die dargestellten rechtlich relevanten Software-Identifikatoren mit den in der Dokumentation angegebenen Identifikatoren identisch sind. • Die rechtlich relevanten Software-Identifikatoren sind von anderen Identifikatoren unterscheidbar.		
Beispiel einer akzeptablen Lösung: a) eine Prüfsumme über den ausführbaren Code. b) jede beliebige Zeichenreihe, die evtl. von einer Versionsnummer ergänzt wird, c) jede beliebige Zahlen-, Buchstaben- oder andere Zeichenreihe, Bitte beachten: Wählt der Hersteller einen gemischten Identifikator für die rechtlich relevante und die nicht rechtlich relevante Software, ist eine einfache Lösung zur Unterscheidung der Identifikatoren die Verwendung von Platzhaltern in der Baumusterprüfbescheinigung, z. B. "abc1.xx", wobei "abc1" für die rechtlich relevante Software und "xx" als Platzhalter für nicht rechtlich relevante Software steht.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation Identisch mit den Risikoklassen B bis D
Validierungsanleitung Identisch mit den Risikoklassen B bis D

Risikoklasse B	Risikoklasse C	Risikoklasse D

P3: Einflussnahme über die Nutzerschnittstellen

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

Detaillierende Anmerkungen:

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

Erforderliche Dokumentation:

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

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

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

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

Funktionsprüfungen:

- Durchführung praktischer Tests (Stichproben) mit dokumentierten Befehlen.
- Test einiger Tastenkombinationen dahingehend, ob diese keinen Einfluss auf die rechtliche relevante Software, die gerätespezifischen Parameter und die Messdaten haben. Im Falle eines Opensource-Betriebssystems mit geschlossener Konsole sind einige nicht dokumentierte Standardbefehle einzugeben, um darauf zu prüfen, dass sie nicht akzeptiert werden.

Beispiel einer akzeptablen Lösung:

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

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

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

Auf Basis des Quellcodes ist zu prüfen:

- ob die Software so aufgebaut ist, dass der Datenfluss bezüglich der Befehle eindeutig definiert ist und nur in der rechtlich relevanten Software realisiert wird.
- ob unzulässiger Datenfluss von der Nutzerschnittstelle zu den rechtlich relevanten Datendomänen erfolgt.
- ob die Befehle richtig entschlüsselt werden. Das Überprüfen kann mit Werkzeugen oder manuell erfolgen.
- ob im Quellcode nicht dokumentierte Befehle vorhanden sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D

P4: Einflussnahme über die Kommunikationsschnittstellen

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

Detaillierende Anmerkungen:

1. Jeder Befehl muss eindeutig einer eingeleiteten Funktion oder Datenänderung zugeordnet werden können.
2. Befehle, die nicht dokumentiert sind, dürfen keine Wirkung auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten haben.
3. Die Module, die die Befehle interpretieren, müssen als rechtlich relevante Software betrachtet werden.
4. Schnittstellen, die Befehle mit unzulässigen Auswirkungen auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten zulassen, müssen versiegelt oder auf sonstige angemessene Weise geschützt werden. Dies gilt auch für Schnittstellen, die nicht vollständig bewertet werden können.
5. Diese besondere Anforderung gilt nicht, wenn ein Software-Download entsprechend Anhang D durchgeführt wird.

Erforderliche Dokumentation:

Verfügt das Gerät über eine Schnittstelle, muss die Dokumentation umfassen:

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

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

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

Funktionsprüfungen:

- Ausführen praktischer Tests (Stichproben) mit Peripherieausstattung.

Beispiel einer akzeptablen Lösung:

Ein rechtlich relevantes Modul empfängt und interpretiert die Daten von der Schnittstelle. Es leitet nur erlaubte Befehle zu den anderen rechtlich relevanten Modulen weiter. Alle unbekannten oder nicht erlaubten Signal- oder Codefolgen werden zurückgewiesen und haben keine Auswirkung auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten.

Zusätze für Risikoklasse E

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

Quellcode der rechtlich relevanten Software.

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

Auf Basis des Quellcodes ist zu prüfen:

- ob die Software so aufgebaut ist, dass der Datenfluss bezüglich der Befehle eindeutig in der rechtlich relevanten Software definiert ist und nachvollzogen werden kann.
- ob unzulässiger Datenfluss von der Nutzerschnittstelle zu den rechtlich relevanten Datendomänen erfolgt.
- ob die Befehle richtig entschlüsselt werden. Das Überprüfen kann mit Werkzeugen oder manuell erfolgen.
- ob im Quellcode nicht dokumentierte Befehle vorhanden sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D

P5: Sicherung und Schutz der rechtlich relevanten Software und der gerätespezifischen Parameter

Rechtlich relevante Software und gerätespezifische Parameter müssen gegen unbeabsichtigte Änderungen gesichert und vor zufälligen Änderungen geschützt werden.

Detaillierende Anmerkungen:

1. Die Software muss in der Lage sein, mögliche Änderungen infolge physikalischer Effekte (elektromagnetische Störung, Temperatur, Vibration usw.) zu erkennen.
2. Es sind Maßnahmen zu implementieren, um die Nutzerschnittstellen gegen unbeabsichtigte Fehlbedienung zu sichern.

Erforderliche Dokumentation:

Die Dokumentation sollte die Maßnahmen aufzeigen, die zur Erkennung und zur Sicherung der rechtlich relevanten Software und der gerätespezifischen Parameter gegen unbeabsichtigte Änderungen genutzt wurden, und beschreiben, wie die rechtlich relevante Software und die gerätespezifischen Parameter vor zufälligen Änderungen geschützt sind.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob Maßnahmen gegen zufällige oder unbeabsichtigte Änderungen beschrieben und angemessen sind.

Funktionsprüfungen:

- Durch geeignete Stichproben ist zu überprüfen, ob Software und gerätespezifische Parameter entweder nicht geändert werden können oder nur nach erfolgreicher Prüfung eines Sicherungsmechanismus, wie z. B. der Eingabe eines Passworts, geändert werden können.

Beispiel einer akzeptablen Lösung:

- Die zufällige Veränderung von rechtlich relevanter Software und gerätespezifischen Parametern wird überprüft, indem periodisch die Prüfsumme(n) berechnet und automatisch mit den hinterlegten Sollwerten verglichen werden. Stimmt der Vergleich nicht überein, sind zum Gerät passende Reaktionen erforderlich (z. B. Anhalten der Messung, entsprechende Anzeige der Messdaten, siehe Anhang I für Empfehlungen).
- Alternativmethoden sind möglich, wenn sich der Änderungsstatus der Software mit ihrer Hilfe identifizieren lässt.
- Zum Thema Fehlererkennung siehe Anhang I.

Zusätze für Risikoklasse E

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

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

Auf Basis des Quellcodes ist zu prüfen:

- ob die Maßnahmen zum Erkennen von Änderungen angemessen sind.
- ob alle rechtlich relevanten Module und alle gerätespezifischen Parameter von der Prüfsumme abgedeckt sind.

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">P6: Schutz von Software und Messdaten
Rechtlich relevante Software und Messdaten müssen vor absichtlichen Änderungen geschützt werden.</td></tr>
<tr><td colspan="3">Detaillierende Anmerkungen:
1. Zum Thema Schutz gegen Manipulation durch die Nutzerschnittstelle, siehe P3.
2. Zum Thema Schutz gegen Manipulation durch die Kommunikationsschnittstelle, siehe P4.
3. Messdaten gelten als ausreichend geschützt, wenn gewährleistet ist, dass sie nur von rechtlich relevanter Software verarbeitet werden können. Falls keine nicht rechtlich relevante Software vorhanden ist, ist dies durch den Schnittstellenschutz (P3, P4) adressiert. Im Falle nicht rechtlich relevanter Software wird zusätzlicher interner Schutz gegen Einflüsse nicht rechtlich relevanter Software durch Anhang S gewährleistet.
4. Speichergeräte, die Software oder Messdaten enthalten, müssen gegen Austausch geschützt werden.</td></tr>
<tr><td></td><td colspan="2">5. Eine Prüfsumme oder eine Alternativmethode mit dem gleichen Schutzniveau ist zur Verfügung zu stellen, um das Erkennen von Softwaremodifikationen zu unterstützen.
6. Die berechnete Prüfsumme oder eine Alternativanzeige der Softwaremodifikation ist auf Befehl für Kontrollzwecke sichtbar zu machen.
7. Die Prüfsumme oder Alternativanzeige wird über die rechtlich relevante Software berechnet. Das Modul, das die Prüfsummen oder Alternativanzeigen erzeugt, ist rechtlich relevant.
8. Wird eine Prüfsumme verwendet, muss der Algorithmus eine Schlüssellänge von mindestens 4 Byte besitzen (siehe auch Anhänge L und T).
9. Bezüglich des Umgangs mit Schlüsseln, siehe auch L5 und T5.</td></tr>
<tr><td colspan="3">Erforderliche Dokumentation:
In der Dokumentation müssen die Schutzmethoden beschrieben sein.</td></tr>
<tr><td colspan="3">• Beschreibung von Maßnahmen, die ergriffen wurden, um die Software zu schützen, insbesondere die Beschreibung der Berechnungsmethode für Prüfsummen sowie die Sollprüfsummen oder Alternativmethoden mit der entsprechenden Sollanzeige.
• Beschreibung der Methoden, die einen Austausch des Speichers verhindern, der die rechtlich relevante Software enthält.
• Beschreibung des Programmiermodus und dessen Abschaltung, falls zutreffend.</td></tr>
<tr><td colspan="3">Validierungsanleitung:
Auf Basis der Dokumentation ist zu prüfen:
• ob die dokumentierten Schutzmaßnahmen gegen Austausch des Speichergerätes, das die rechtlich relevante Software und die Messdaten enthält, ausreichend sind.
• ob die Prüfsumme(n) oder Alternativanzeige(n) die rechtlich relevante Software abdecken.

Funktionsprüfungen:
• Praktisches Testen des Programmiermodus und Prüfung, ob das Abschalten funktioniert.
• Vergleich berechneter Prüfsummen oder Alternativanzeigen mit den Sollwerten.</td></tr>
</table>

Beispiel einer akzeptablen Lösung: a) Um zu verhindern, dass der physische Speicher entfernt und ausgetauscht wird, ist entweder das Gerätegehäuse oder der physische Speicher selbst geschützt. b) Das Gerät ist versiegelt und die Schnittstellen genügen den Anforderungen P3 und P4.	**Beispiel einer akzeptablen Lösung:** (zusätzlich zu a) und b)) c) Der ausführbare Code wird mittels Prüfsummen geschützt. Das Programm berechnet seine eigene Prüfsumme und vergleicht sie mit einem Sollwert, der im ausführbaren Code selbst verborgen ist. Wenn der Selbsttest fehlschlägt, wird das Modul gesperrt. Eine CRC-32 Prüfsumme mit einem geheimen Startwert (im ausführbaren Code versteckt) wird genutzt.

Zusätze für Risikoklasse E

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

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

Auf Basis des Quellcodes ist zu prüfen:

- ob die Maßnahmen zur Erfassung von absichtlichen Änderungen angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D

P7: Parameterschutz

Gerätespezifische Parameter müssen gegen absichtliche Modifizierungen geschützt werden.

Detaillierende Anmerkungen:

1. Bestimmte gerätespezifische Parameter können vom Verwender geändert werden, vorausgesetzt, dass sie durch eine Prüfeinrichtung geschützt sind, die jegliche Änderung der rechtlich relevanten Parameter automatisch und unauslöschlich aufzeichnet, z. B. in einem Audit Trail.
2. Falls für den Zweck der Verifikation eines Messgerätes notwendig, muss es möglich sein, die aktuellen relevanten Parametereinstellungen anzuzeigen oder auszudrucken.
3. Die Aufzeichnungen, die den Nachweis eines Eingriffs ermöglichen, müssen auf Befehl über eine Anzeige oder einen Ausdruck verfügbar gemacht werden.

Erforderliche Dokumentation:

1. Die Dokumentation muss beschreiben, wie die gerätespezifischen Parameter geschützt sind, ob sie eingestellt werden dürfen und wie sie eingestellt werden.
2. Die Dokumentation muss beschreiben, wie die gerätespezifischen Parameter zum Zweck der Verifikation eines Messgeräts angezeigt oder ausgedruckt werden können.
3. Die Dokumentation muss beschreiben, wie die Aufzeichnungen, die den Nachweis eines Eingriffs ermöglichen, angezeigt oder ausgedruckt werden können.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob Änderung oder Justierung gerätespezifischer Parameter ohne Nachweis eines Eingriffs unmöglich ist.
- ob alle relevanten gerätespezifischen Parameter (falls vorhanden, in Anhang I angegeben) geschützt sind.
- ob alle Aufzeichnungen, die den Nachweis eines Eingriffs ermöglichen, angezeigt oder ausgedruckt werden.

Funktionsprüfungen:

- Überprüfen, ob alle gerätespezifischen Parameter angemessen geschützt sind.
- Überprüfen, ob alle gerätespezifischen Parameter angezeigt oder ausgedruckt werden können.
- Überprüfen, ob alle Aufzeichnungen, die den Nachweis eines Eingriffs ermöglichen, angezeigt oder ausgedruckt werden können.

Beispiel einer akzeptablen Lösung:

a) Gerätespezifische Parameter, die nicht vom Nutzer eingestellt werden dürfen, sind durch Versiegelung des Geräts oder des Speichergehäuses geschützt und der Schaltkreiseingang, der Schreiben aktiviert/sperrt, wurde durch einen dazugehörigen versiegelten Jumper oder Schalter deaktiviert.

• Änderungen der gerätespezifischen Parameter werden in einem Audit Trail registriert, d. h., es erfolgt eine Informationsaufzeichnung in einem nicht löschbaren Speicher. Jeder Eintrag wird automatisch von der rechtlich relevanten Software erzeugt und enthält:
  • den Identifikator des Parameters (z. B. den Namen),
  • den Parameterwert (den aktuellen oder den vorherigen Wert),
  • den Zeitstempel der Änderung
Der Audit Trail kann nicht ohne Zerstörung eines Siegels gelöscht oder geändert werden. Der Inhalt des Audit Trails ist dann auf der Anzeige sichtbar oder wird auf Befehl gedruckt.	

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Maßnahmen zum Schutz der gerätespezifischen Parameter angemessen sind.

Risikoklasse C	**Risikoklasse D**
P8: Dargestellte Messdaten *Die Authentizität der dargestellten Messdaten muss garantiert sein und die Darstellung muss klar und von allen Informationen begleitet sein, die notwendig sind, um den Nutzer über die Bedeutung des Ergebnisses zu informieren.*	

Detaillierende Anmerkungen:

1. Es darf nicht möglich sein, rechtlich relevante Software zur Darstellung von Messdaten betrügerisch nachzuahmen (vorzutäuschen).
2. Die Bedeutung aller dargestellten rechtlich relevanten Daten muss klar sein. Alle dargestellten rechtlich relevanten Daten müssen voneinander unterscheidbar sein.
3. Dargestellte rechtlich relevante Messdaten müssen klar unterscheidbar von nicht rechtlich relevanten Daten sein.
4. Die dargestellten Messdaten müssen von allen Informationen begleitet werden, die notwendig sind, um sie zu interpretieren (z. B. Quantität, Einheit, Sensornummer, Skalierungsfaktor). Bezüglich notwendiger Informationen, die die Daten begleiten müssen, siehe L1, T1. Die Sensornummer (falls benötigt, um das Ergebnis korrekt zu interpretieren) ist ein rechtlich relevanter Parameter, der geschützt und gesichert werden muss, siehe P5/U5 und P7/U7.

Erforderliche Dokumentation:

- Benennung aller Module, die die Darstellung der rechtlich relevanten Messdaten realisieren.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen,

- ob die Darstellung der Messdaten nur durch rechtlich relevante Software ausgeführt werden kann.

Funktionsprüfungen:

- Überprüfen, ob die Bedeutung aller dargestellten rechtlich relevanten Messdaten klar ist und ob sie voneinander unterschieden werden können.
- Überprüfen durch Sichtkontrolle, ob die Darstellung der Messdaten leicht unterscheidbar von anderen möglicherweise ebenfalls dargestellten Informationen ist.
- Überprüfen durch Sichtkontrolle, ob die dargestellten Messdaten von allen notwendigen Informationen begleitet werden.
- Falls für die korrekte Interpretation des Ergebnisses notwendig, ist zu prüfen, ob die Datenquelle identifiziert ist und von der rechtlich relevanten Software dargestellt wird.

Beispiel einer akzeptablen Lösung:

1. Die Darstellung enthält nicht rechtlich relevante Daten, die klar von rechtlich relevanten Messdaten unterschieden werden können.
2. Die Sensoreinheit verschlüsselt die Messwerte mit einem Schlüssel (z. B. einer geheimen Zufallszahl), der nur der rechtlich relevanten Software auf dem Messgerät mit zweckgebundener Hard- und Software bekannt ist. Nur die rechtlich relevante Software kann die Messwerte entschlüsseln und benutzen, nicht rechtlich relevante Module oder Komponenten können dies nicht, da sie den Schlüssel nicht kennen. Zur Schlüsselhandhabung siehe Anhang T.
3. Vor dem Senden von Messwerten stößt der Sensor eine Handshake-Sequenz mit der rechtlich relevanten Software auf dem Messgerät mit zweckgebundener Hard- und Software an, die auf geheimen Schlüsseln basiert. Nur wenn das Programm auf dem Messgerät mit zweckgebundener Hard- und Software korrekt kommuniziert, sendet die Sensoreinheit ihre Messwerte. Zur Schlüsselhandhabung siehe Anhang T.

4. Die in 1. / 2. verwendete geheime Zufallszahl wird gewählt sowie der Sensoreinheit und der Software auf dem Messgerät mit zweckgebundener Hard- und Software ohne Zerstörung eines Siegels übergeben.	4. Die in 1. / 2. verwendete geheime Zufallszahl wird gewählt sowie der Sensoreinheit und der Software auf dem Messgerät mit zweckgebundener Hard- und Software nur nach Zerstörung eines Siegels übergeben.

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

Zusätze für Risikoklasse E

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

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

Auf Basis des Quellcodes ist zu prüfen:

- ob die rechtlich relevante Software die dargestellten Messergebnisse erzeugt.
- ob alle genutzten Maßnahmen korrekt sind, um die Darstellung der Messdaten durch rechtlich relevante Software zu gewährleisten.

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

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

5.1 Technische Beschreibung

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

Hardwarekonfiguration

a) Ein modulares, auf ein Universalgerät gestütztes System. Das Computersystem kann ein Stand-Alone-System, Teil eines geschlossenen Netzes (z. B. Ethernet, Token-Ring-LAN) oder Teil eines offenen Netzes (z. B. Internet) sein.

b) Da das System für universelle Zwecke ausgelegt ist, befindet sich der Messsensor normalerweise außerhalb des Computersystems und ist über eine Kommunikationsverbindung angekoppelt.

b) Die Nutzerschnittstelle bietet neben dem Betriebsmodus für die Messaufgabe weitere Funktionen, die nicht unter rechtlicher Kontrolle stehen.

c) Speichermedien können fest installiert (z. B. Festplatte), entfernbar (z. B. USB) oder entfernt vorhanden (remote) sein.

Softwarekonfiguration

d) Üblicherweise wird ein Betriebssystem verwendet.

e) Neben der Anwendung des Messgeräts können sich gleichzeitig auch andere Softwareanwendungen auf dem System befinden.

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

Folgen für die Risikoklassifikation

Die Software von Geräten vom Typ U ist sehr viel leichter zugänglich als die Software von Geräten vom Typ P. Der Schutz der Softwareintegrität muss im Vergleich zu Geräten vom Typ P erhöht werden. Insbesondere wird eine Prüfsumme oder ein gleichwertiges Mittel erwartet, um die Integritätsprüfungen des Softwarecodes zu unterstützen. Die Folge ist, dass die Software-Konformitätsebene „niedrig“ (nur funktionelle Übereinstimmung der Software mit der technischen Dokumentation des in der Prüfung befindlichen Gerätetyps) kein adäquates Mittel ist, um die Softwareintegrität zu sichern. Dies bedeutet, dass die Risikoklasse C die niedrigste Risikoklasse ist, in die Geräte vom Typ U eingestuft werden können.

5.2 Spezifische Softwareanforderungen an Typ U

Risikoklassen C bis E
U1: Dokumentation *Zusätzlich zur spezifischen Dokumentation, die in jeder der folgenden Anforderungen erforderlich ist, muss die Dokumentation grundsätzlich Folgendes umfassen:* *a. Eine Beschreibung der rechtlich relevanten Softwarefunktionen, der Bedeutung der Daten usw.* *b. Eine Beschreibung der Nutzerschnittstelle, der Menüs und der Dialoge.* *c. Den Software-Identifikator bzw. die Software-Identifikatoren der rechtlich relevanten Software.* *d. Einen Überblick über die Systemhardware, z. B. Block-Schaltbild, Computerart(en), Netzwerktypen usw.* *e. Zur Dokumentation bzgl. Des Betriebssystems, siehe Anhang O.* *f. Das Betriebshandbuch.*

Risikoklasse C und D
U2: Software-Identifikation *Die rechtlich relevante Software muss eindeutig gekennzeichnet sein. Der Identifikator bzw. die Identifikatoren müssen dauerhaft durch das Gerät oder auf Befehl oder während des Betriebs angezeigt werden.*
Detaillierende Anmerkungen: 1. Rechtlich relevante Software-Identifikatoren können unabhängig oder Teil gut strukturierter Identifikatoren sein. 2. Für den Fall, dass ein rechtlich relevanter Software-Identifikator in einen Gesamtidentifikator eingebettet ist, muss er deutlich unterscheidbar sein. 3. Die rechtlich relevanten Identifikatoren müssen für jedes rechtlich relevante Modul, mit dem das Gerät ausgestattet ist, eindeutig sein. 4. Die rechtlich relevanten Identifikatoren müssen ohne zusätzliches Werkzeug problemlos darstellbar sein. 5. Bezüglich der Identifikation von Betriebssystemteilen siehe O6. Die detaillierenden Anmerkungen hier gelten in Verbindung mit O6 für die Identifikation des Betriebssystems. 6. Die rechtlich relevanten Software-Identifikatoren sind bauartspezifische Parameter und müssen als solche geschützt werden (siehe U5 und U6). Wenn die Identifikatoren nicht untrennbar mit der Software selbst verbunden sind, sind andere Schutzmaßnahmen erforderlich. 7. Der bzw. die Identifikatoren werden dauerhaft, auf Befehl oder beim Startvorgang dargestellt.
Erforderliche Dokumentation: Die Dokumentation muss die Software-Identifikatoren auflisten und beschreiben, wie diese erzeugt werden, wie sie geschützt werden, wie sie dargestellt werden und, gegebenenfalls, wie sie strukturiert sind, um zwischen rechtlich relevanten Identifikatoren und anderen unterscheiden zu können.
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob in der Dokumentation alle rechtlich relevanten Software-Identifikatoren angegeben sind. • ob alle rechtlich relevanten Module klar beschrieben sind, so dass nachvollziehbar ist, welches Modul von welchem Software-Identifikator abgedeckt wird. • die Beschreibung der Erzeugung und Visualisierung aller rechtlich relevanten Software-Identifikatoren. • ob alle rechtlich relevanten Software-Identifikatoren eindeutig sind (besonders bei Revisionen). *Funktionsprüfungen:* • Die Software-Identifikatoren können so dargestellt werden, wie in der Dokumentation beschrieben. • Die dargestellten Identifikatoren stimmen mit den in der Dokumentation angegebenen Identifikatoren überein. • Die rechtlich relevanten Software-Identifikatoren sind von anderen Identifikatoren unterscheidbar.

Beispiel einer akzeptablen Lösung:

a) eine Prüfsumme über den ausführbaren Code.
b) eine Zeichenreihe, die von einer Versionsnummer ergänzt wird.
c) jede beliebige Zahlen-, Buchstaben- oder andere Zeichenreihe.

- Wählt der Hersteller einen gemischten Identifikator für die rechtlich relevante und die nicht rechtlich relevante Software, ist eine einfache Lösung zur Unterscheidung der Identifikatoren die Verwendung von Platzhaltern in der Baumusterprüfbescheinigung, z. B. „abc1.xx“, wobei „abc1“ für die rechtlich relevante Software und „xx“ als Platzhalter für nicht rechtlich relevante Software steht.

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

Risikoklasse C	**Risikoklasse D**
U3: Einflussnahme über die Nutzerschnittstellen *Die über die Nutzerschnittstellen eingegebenen Befehle dürfen die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten nicht unzulässig beeinflussen.*	
Detaillierende Anmerkungen: 1. Jeder Befehl muss eindeutig einer eingeleiteten Funktion oder Datenänderung zugeordnet werden können. 2. Befehle, die nicht dokumentiert sind, dürfen keine Wirkung auf die rechtlich relevante Software, gerätespezifische Parameter und Messdaten haben. 3. Die Module, die die Befehle interpretieren, müssen als rechtlich relevant betrachtet werden.	
Erforderliche Dokumentation: Wenn das Gerät die Fähigkeit zum Befehlsempfang hat, muss die Dokumentation Folgendes enthalten: • Beschreibung von Befehlen und ihrer Wirkung auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten. • Eine Beschreibung, wie die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten vor dem Einfluss anderer Eingaben geschützt werden.	
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob alle dokumentierten Befehle zulässig sind, d. h., ob sie eine erlaubte Auswirkung auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten haben. • Prüfen der Schutzmaßnahmen gegen Einflüsse von anderen Eingaben. *Funktionsprüfungen:* • Durchführung praktischer Tests (Stichproben) mit dokumentierten Befehlen. • Test einiger Tastenkombinationen dahingehend, ob diese keinen Einfluss auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten haben. • Im Falle eines Opensource-Betriebssystems mit geschlossener Konsole sind einige nicht dokumentierte Standardbefehle zu testen, um darauf zu prüfen, dass sie nicht akzeptiert werden.	

Beispiel einer akzeptablen Lösung:	**Beispiel einer akzeptablen Lösung:**
• Ein rechtlich relevantes Modul filtert unzulässige Befehle heraus. Nur dieses Modul empfängt die Befehle und es kann nicht umgangen werden. Jede falsche Eingabe ist gesperrt.	• Für den Einsatz des Messsystems ist ein Konto mit nur eingeschränkten Berechtigungen eingerichtet. Der Zugriff auf das Administratorkonto ist entsprechend U6 gesperrt. • Die Befehlszeile ist geschlossen, d. h., der Nutzer kann keine Programme laden, Programme schreiben oder Befehle für das Betriebssystem ausführen.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklasse D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklasse D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Software so aufgebaut ist, dass der Datenfluss bezüglich der Befehle in der rechtlich relevanten Software eindeutig definiert ist und nachvollzogen werden kann. • ob unzulässiger Datenfluss von der Nutzerschnittstelle zu den rechtlich relevanten Bereichen erfolgt. • ob die Befehle richtig entschlüsselt werden. Das Überprüfen kann mit Werkzeugen oder manuell erfolgen. • ob im Quellcode nicht dokumentierte Befehle vorhanden sind.

Risikoklasse C	Risikoklasse D

U4: Einflussnahme über die Kommunikationsschnittstellen

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

Detaillierende Anmerkungen:

1. Jeder Befehl muss eindeutig einer eingeleiteten Funktion oder Datenänderung zugeordnet werden können.
2. Befehle, die nicht dokumentiert sind, dürfen keine Wirkung auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten haben.
3. Die Module, die die Befehle interpretieren, müssen als rechtlich relevant betrachtet werden.
4. Schnittstellen, die Befehle mit unzulässigen Auswirkungen auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten zulassen, müssen versiegelt oder auf sonstige angemessene Weise geschützt werden. Dies gilt auch für Schnittstellen, die nicht vollständig bewertet werden können.
5. Diese besondere Anforderung gilt nicht, wenn ein Software-Download entsprechend Anhang D durchgeführt wird.

Hinweis: Wenn das Betriebssystem Fernsteuerung oder –zugriff gestattet, bezieht sich die Anforderung U3 auf die Kommunikationsschnittstelle bzw. die angeschlossenen Fernzugriffsterminals.

Erforderliche Dokumentation:

Verfügt das Gerät über eine Schnittstelle, muss die Dokumentation umfassen:

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

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob alle dokumentierten Befehle zulässig sind, d. h., ob sie eine erlaubte Auswirkung auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten haben.
- Die Schutzmaßnahmen gegen Einflüsse von anderen Befehlen.

Funktionsprüfungen:

- Ausführen praktischer Tests (Stichproben) mit Peripherieausstattung.

Beispiele akzeptabler Lösungen:

- Ein rechtlich relevantes Modul empfängt und interpretiert Befehle von der Schnittstelle. Es leitet nur erlaubte Befehle zu den anderen rechtlich relevanten Modulen weiter. Alle unbekannten oder nicht erlaubten Befehle werden zurückgewiesen und haben keine Auswirkung auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten.
- Die Betriebssystemregel für serielle Verbindungen und Firewall-Einstellungen für Netzwerkverbindungen verhindert, dass eine unzulässige Befehlsausführung die rechtlich relevante Anwendung beeinflusst.

Zusätze für Risikoklasse E

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

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

Auf Basis des Quellcodes ist zu prüfen:

- ob die Software so aufgebaut ist, dass der Datenfluss bezüglich der Befehle eindeutig in der rechtlich relevanten Software definiert ist und nachvollzogen werden kann.
- ob kein unzulässiger Datenfluss von der Nutzerschnittstelle zu den zu schützenden Bereichen erfolgt.
- ob die Befehle richtig entschlüsselt werden. Das Überprüfen kann mit Werkzeugen oder manuell erfolgen.
- ob der Quellcode nicht dokumentierte Befehle enthält.

Risikoklasse C	Risikoklasse D

U5: Sicherung und Schutz der rechtlich relevanten Software und der gerätespezifischen Parameter

Rechtlich relevante Software und gerätespezifische Parameter müssen gegen unbeabsichtigte Änderungen gesichert und vor zufälligen Änderungen geschützt werden.

Detaillierende Anmerkungen:

1. Die Software muss in der Lage sein, mögliche Änderungen infolge physikalischer Effekte (elektromagnetische Störung, Temperatur, Vibration usw.) zu erkennen.
2. Es sind Maßnahmen zu implementieren, um die Nutzerschnittstellen gegen unbeabsichtigte Fehlbedienung zu sichern.
3. Die zufällige Modifikation der rechtlich relevanten Software und der gerätespezifischen Parameter muss mittels periodischer Berechnung der Prüfsumme(n) und automatischen Vergleichs mit hinterlegten Sollwerten geprüft werden. Stimmt der Vergleich nicht überein, sind Reaktionen erforderlich, die für das Gerät angemessen sind (z. B. Anhalten der Messung, Anzeige der Messdaten, siehe Kapitel 10 für Empfehlungen). Alternativmethoden sind möglich, wenn sich der Änderungsstatus der Software mit ihrer Hilfe identifizieren lässt.
4. Bezüglich zusätzlicher Schutzmaßnahmen, die im Betriebssystem zu implementieren sind, siehe O4.

Erforderliche Dokumentation:

- Beschreibung der Maßnahmen, die genutzt wurden, um die rechtlich relevante Software und die gerätespezifischen Parameter gegen unbeabsichtigte Änderungen zu sichern, und wie die rechtlich relevante Software und die gerätespezifischen Parameter gegen zufällige Änderungen geschützt sind.
- Beschreibung der Prüfsummenmethode und der Reaktionen im Falle der Nichtübereinstimmung.
- Beschreibung, wie und wo die Sollprüfsumme(n) oder die Alternativanzeigen des Änderungsstatus abgelegt werden.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob Maßnahmen gegen zufällige und unbeabsichtigte Änderungen beschrieben und angemessen sind.
- ob Prüfsummen die rechtlich relevante Software abdecken.
- ob die Methoden zur Prüfsummenberechnung, zum Vergleich und zu Reaktionen im Falle der Nichtübereinstimmung korrekt sind.

Beispiel einer akzeptablen Lösung:

- Um Missbrauch des Betriebssystems, Überschreiben oder Löschen rechtlich relevanter Software und aller gerätespezifischen Parameter zu verhindern, werden die Schutz- und Geheimhaltungsrechte, die durch das Betriebssystem oder die Programmiersprache zur Verfügung stehen, in vollem Umfang genutzt.
- Alle Nutzerrechte für das Löschen, Verschieben oder Verändern rechtlich relevanter Software werden entfernt und der Zugriff wird über Dienstprogramme kontrolliert.
- Auf zufällige Modifikation von rechtlich relevanter Software und aller gerätespezifischer Parameter wird geprüft, indem eine Prüfsumme über den entsprechenden ausführbaren Code berechnet und mit dem Sollwert verglichen wird, wonach entsprechende angemessene Reaktionen eingeleitet werden, wenn der ausführbare Code und/oder die gerätespezifischen Parameter verändert worden sind. Siehe Anhang I für Empfehlungen bezüglich angemessener Reaktionen.

Zusätze für Risikoklasse E

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

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

Auf Basis des Quellcodes ist zu prüfen:

- ob die Maßnahmen zum Erkennen von Änderungen angemessen sind.
- ob alle rechtlich relevanten Module und alle gerätespezifischen Parameter von der Prüfsumme abgedeckt sind.

<table>
<tr><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="2">U6: Schutz von Software und Messdaten
Rechtlich relevante Software und Messdaten müssen vor absichtlichen Änderungen geschützt werden.</td></tr>
<tr><td colspan="2">Detaillierende Anmerkungen:
1. Messdaten gelten als ausreichend geschützt, wenn gewährleistet ist, dass sie nur von rechtlich relevanter Software verarbeitet werden können. Darauf wird im Punkt Schnittstellenschutz in den U-Anforderungen U3 und U4 eingegangen. Im Falle nicht rechtlich relevanter Software wird zusätzlicher interner Schutz gegen Einflüsse nicht rechtlich relevanter Software durch Anhang S gewährleistet.
2. Speichergeräte, in denen die Software und die Messdaten aufbewahrt werden, müssen vor Austausch geschützt sein.
3. Eine Prüfsumme oder eine Alternativmethode mit dem gleichen Schutzniveau ist zur Verfügung zu stellen, um das Erkennen von Softwaremodifikationen zu unterstützen. Die berechnete Prüfsumme oder eine Alternativanzeige der Softwaremodifikation ist auf Befehl für Kontrollzwecke sichtbar zu machen.
4. Die Prüfsumme oder Alternativanzeige wird über die rechtlich relevante Software berechnet. Das Modul, das die Prüfsummen oder Alternativanzeigen erzeugt, ist rechtlich relevant.
5. Bezüglich zusätzlicher Schutzmaßnahmen, die im Betriebssystem zu implementieren sind, siehe O4 und O7.
6. Wird eine Prüfsumme verwendet, muss der Algorithmus eine Schlüssellänge von mindestens 4 Byte haben.</td></tr>
<tr><td></td><td>7. Generell ist ein Universalgerät nur dann geeignet, wenn zusätzliche Hardware zur Unterstützung des Schutzes verwendet werden kann.
8. Was Algorithmen und Mindestschlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden.</td></tr>
<tr><td colspan="2">Erforderliche Dokumentation:
• Beschreibung von Maßnahmen, die genutzt wurden, um die Software zu schützen, insbesondere die Beschreibung der Berechnungsmethode für Prüfsummen sowie die Sollprüfsummen oder Alternativmethoden mit der entsprechenden Sollanzeige.
• Beschreibung der Methoden zum Schutz der Massenspeicher vor Austausch, falls zutreffend.
• Beschreibung, wie die Prüfsumme oder eine Alternativanzeige dargestellt wird.</td></tr>
<tr><td colspan="2">Validierungsanleitung:
Auf Basis der Dokumentation ist zu prüfen:
• ob die dokumentierten Schutzmaßnahmen gegen Austausch des Speichergerätes, das die rechtlich relevante Software und die Messdaten enthält, ausreichend sind.
• ob die Prüfsumme(n) oder Alternativanzeigen die rechtlich relevante Software umfassen.
• ob die Maßnahmen, mit denen verhindert werden soll, dass rechtlich relevante Software mit Hilfe des Betriebssystems geändert oder ausgetauscht wird, angemessen sind.

Funktionsprüfungen:
• Vergleich berechneter Prüfsummen oder Alternativanzeigen mit den Sollwerten.</td></tr>
<tr><td></td><td>Auf Basis der Dokumentation ist zu prüfen:
• ob die genutzten Maßnahmen dem geforderten hohen Schutzniveau gemäß dem Stand der Technik entsprechen.</td></tr>
</table>

Beispiel einer akzeptablen Lösung: 1. Der ausführbare Code wird mittels Prüfsummen geschützt. Das Modul berechnet seine eigene Prüfsumme und vergleicht sie mit einem Sollwert, der im ausführbaren Code selbst verborgen ist. Wenn der Selbsttest fehlschlägt, wird das Programm gesperrt. Eine CRC-32 Prüfsumme mit einem geheimen Startwert (im ausführbaren Code versteckt) wird verwendet. Der Zugang zum Administratorkonto wird mittels eines automatisch generierten Passworts gesperrt, das niemandem bekannt ist. Ein Umgehen der Schutzmaßnahmen des Betriebssystems durch direktes Schreiben auf den Massenspeicher oder dessen Austausch wird durch Versiegelung verhindert. 2. Die unerlaubte Änderung der rechtlich relevanten Software wird über die Zugriffskontrolle oder die Datenschutzattribute des Betriebssystems verhindert. Die Administrationsebene dieser Systeme ist durch Versiegelung oder ein gleichwertiges Mittel gesichert.	**Beispiel einer akzeptablen Lösung:** • Der ausführbare Code wird durch die Speicherung der rechtlich relevanten Software in einer geeigneten Einsteckeinheit gesichert, die versiegelt ist. Die Einsteckeinheit enthält einen Read-Only-Speicher und einen Mikrocontroller.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen C und D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklasse D): *Auf Basis des Quellcodes ist zu prüfen:* • die Kommunikation mit der zusätzlichen Sicherungshardware, • ob Änderungen der rechtlich relevanten Software erkannt werden.

Risikoklasse C	**Risikoklasse D**
U7: Parameterschutz *Gerätespezifische Parameter müssen gegen absichtliche Modifizierungen geschützt werden.*	
Detaillierende Anmerkungen: 1. Bestimmte gerätespezifische Parameter können vom Verwender geändert werden, vorausgesetzt, dass sie durch eine Prüfeinrichtung geschützt sind, die jegliche Änderung der rechtlich relevanten Parameter automatisch und unauslöschlich aufzeichnet, z. B. in einem Audit Trail. 2. Falls für den Zweck der Verifikation eines Messgeräts notwendig, muss es möglich sein, die aktuellen relevanten Parametereinstellungen anzuzeigen oder auszudrucken. 3. Die Aufzeichnungen, die den Nachweis eines Eingriffs ermöglichen, müssen auf Befehl über eine Anzeige oder einen Ausdruck verfügbar gemacht werden.	
Erforderliche Dokumentation: 1. Die Dokumentation muss beschreiben, wie die gerätespezifischen Parameter geschützt sind, ob sie eingestellt werden dürfen und wie sie eingestellt werden. 2. Die Dokumentation muss beschreiben, wie die gerätespezifischen Parameter zum Zweck der Verifikation angezeigt oder ausgedruckt werden können. 3. Die Dokumentation muss beschreiben, wie die Aufzeichnungen, die den Nachweis eines Eingriffs ermöglichen, angezeigt oder ausgedruckt werden können.	

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob Änderung oder Justierung gerätespezifischer Parameter ohne Nachweis eines Eingriffs unmöglich ist.
- ob alle relevanten gerätespezifischen Parameter (falls vorhanden, in Anhang I angegebenen) geschützt sind.
- ob alle Aufzeichnungen, die den Nachweis eines Eingriffs ermöglichen, angezeigt oder ausgedruckt werden.

Funktionsprüfungen:

- Überprüfen, ob alle gerätespezifischen Parameter angemessen geschützt sind.
- Überprüfen, ob alle gerätespezifischen Parameter angezeigt oder ausgedruckt werden können.
- Überprüfen, ob alle Aufzeichnungen, die den Nachweis eines Eingriffs ermöglichen, angezeigt oder ausgedruckt werden können.

Beispiel einer akzeptablen Lösung:

- Gerätespezifische Parameter, die nicht vom Nutzer eingestellt werden dürfen, sind durch Versiegelung des Geräts oder des Speichergehäuses geschützt und der Schaltkreiseingang, der Schreiben aktiviert/sperrt, wurde durch einen dazugehörigen versiegelten Jumper oder Schalter deaktiviert.
- Gerätespezifische Parameter werden durch einen Audit Trail geschützt. Änderungen der gerätespezifischen Parameter werden in einem Audit Trail registriert, d. h., es erfolgt eine Informationsaufzeichnung in einem nicht löschbaren Speicher. Jeder Eintrag wird automatisch von der rechtlich relevanten Software erzeugt und enthält:
  - den Identifikator des Parameters (z. B. den Namen),
  - den Parameterwert (den aktuellen oder den vorherigen Wert),
  - den Zeitstempel der Änderung.

  Der Audit Trail kann nicht ohne Zerstörung eines Siegels gelöscht oder geändert werden. Der Inhalt des Audit Trails ist dann auf der Anzeige sichtbar oder wird auf Befehl gedruckt.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen C und D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen C und D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Maßnahmen zum Schutz der gerätespezifischen Parameter angemessen sind.

Risikoklasse C	**Risikoklasse D**
U8: Dargestellte Messdaten *Die Authentizität der dargestellten Messdaten muss garantiert sein und die Darstellung muss klar und von allen Informationen begleitet sein, die notwendig sind, um den Nutzer über die Bedeutung des Ergebnisses zu informieren.*	

Detaillierende Anmerkungen:

1. Es darf nicht möglich sein, rechtlich relevante Software zur Darstellung von Messdaten betrügerisch nachzuahmen (vorzutäuschen).
2. Die Bedeutung aller dargestellten rechtlich relevanten Daten muss klar sein. Alle dargestellten rechtlich relevanten Daten müssen voneinander unterscheidbar sein.
3. Dargestellte rechtlich relevante Messdaten müssen klar unterscheidbar von nicht rechtlich relevanten Daten sein.
4. Die dargestellten Messdaten müssen von allen Informationen begleitet werden, die notwendig sind, um sie zu interpretieren (z. B. Quantität, Einheit, Sensornummer, Skalierungsfaktor). Bezüglich notwendiger Informationen, die die Daten begleiten müssen, siehe L1, T1. Die Sensornummer ist ein rechtlich relevanter Parameter, der geschützt und gesichert werden muss, siehe P5/U5 und P7/U7.

Erforderliche Dokumentation:

- Benennung aller Module, die die Darstellung der rechtlich relevanten Messdaten realisieren.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob die Darstellung der Messdaten nur durch rechtlich relevante Software ausgeführt werden kann.

Funktionsprüfungen:

- Überprüfen, ob die Bedeutung aller dargestellten rechtlich relevanten Messdaten klar ist und ob sie voneinander unterschieden werden können.
- Überprüfen durch Sichtkontrolle, ob die Darstellung der Messdaten leicht unterscheidbar von anderen möglicherweise ebenfalls dargestellten Informationen ist.
- Überprüfen durch Sichtkontrolle, ob die dargestellten Messdaten von allen notwendigen Informationen begleitet werden.
- Falls für die korrekte Interpretation des Ergebnisses notwendig, ist zu prüfen, ob die Datenquelle identifiziert ist und von der rechtlich relevanten Software dargestellt wird.

Beispiel einer akzeptablen Lösung:

1. Die Sensoreinheit verschlüsselt die Messwerte mit einem Schlüssel, der auf dem Universalgerät nur der rechtlich relevanten Software bekannt ist (z. B. eine geheime Zufallszahl). Nur das rechtlich relevante Modul kann die Messwerte entschlüsseln und benutzen, nicht rechtlich relevante Module auf dem Universalgerät können dies nicht, da sie den Schlüssel nicht kennen. Zur Schlüsselhandhabung siehe Anhang T.
2. Vor dem Senden von Messwerten stößt der Sensor eine Handshake-Sequenz mit der rechtlich relevanten Software auf dem Universalgerät an, die auf geheimen Schlüsseln basiert. Nur wenn das Programm auf dem Universalgerät korrekt kommuniziert, sendet die Sensoreinheit ihre Messwerte. Zur Schlüsselhandhabung siehe Anhang T.

3. Die in 1. / 2. verwendete geheime Zufallszahl wird gewählt sowie der Sensoreinheit und der Software auf dem Universalgerät ohne Zerstörung eines Siegels übergeben.	3. Die in 1. / 2. verwendete geheime Zufallszahl wird gewählt sowie der Sensoreinheit und der Software auf dem Universalgerät nur nach Zerstörung eines Siegels übergeben.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen C und D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen C und D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die rechtlich relevante Software die dargestellten Messergebnisse erzeugt. • ob alle genutzten Maßnahmen korrekt sind, um die Darstellung der Messdaten durch rechtlich relevante Software zu gewährleisten.

6 Anhang O: Universalbetriebssysteme

Die spezifischen Anforderungen in diesem Kapitel treffen nur zu, wenn das Betriebssystem einer Komponente des Messgerätes rechtlich relevant ist, beispielsweise, wenn das Betriebssystem genutzt wird, um die wesentlichen Anforderungen der MID zu erfüllen, oder wenn es Auswirkungen auf die Einhaltung der Anforderungen haben kann. Sie sind eine Ergänzung zu den spezifischen Anforderungen an Software für Messgeräte mit Universalgerät (Typ-U-Anforderungen). Diese Anforderungen müssen nicht bei Messgeräten von Typ P angewendet werden.

6.1 Technische Beschreibung

Software wird als *Universalbetriebssystem* bezeichnet, wenn Systemressourcen eines Messgeräts (CPU, Speicher, Schnittstelle) von dieser Software verwaltet und der

rechtlich relevanten Anwendung zur Verfügung gestellt werden. Zusätzlich muss das Betriebssystem eine Mehrnutzerfähigkeit und einen Administrationsmodus haben.

Jedes Universalbetriebssystem, das nach diesem Anhang evaluiert wird, muss die folgenden Grundvoraussetzungen erfüllen:

- es muss betriebsbewährt sein,
- es muss für den Universalzweck geeignet sein,
- es muss dem Stand der Technik entsprechen[2] und
- es darf nicht vom Hersteller des Messgeräts oder des Teilgeräts selbst entwickelt worden sein. Jedoch kann ein Hersteller oder Produzent zu dem Betriebssystem beitragen, wenn es um Treiber oder Module geht, die speziell für die rechtlich relevante Aufgabe programmiert wurden, solange die Voraussetzungen von O6 und O7 erfüllt werden. Das heißt, Treiber oder Module, die speziell für eine rechtlich relevante Aufgabe programmiert wurden, müssen eine eigene Identifikation und einen eigenen Schutz haben.

In diesem Fall kann die Untersuchung des Universalbetriebssystems auf die rechtlich relevante Konfiguration basierend auf den Anforderungen in Anhang O beschränkt werden.

Jede implementierte Schutzmaßnahme kann mit Maßnahmen im Bereich der Hardware oder der rechtlich relevanten Anwendung kombiniert werden.

6.2 Anwendbarkeit der Anforderungen für Komponenten

In Bezug auf Standard-Betriebssysteme unterscheidet diese Erweiterung zwischen zwei Kategorien von Messgerätekomponenten. Für Definitionen von Komponenten der Kategorien 1 und 2 siehe Kapitel 1.
Dieses Kapitel ist nur auf Messgerätekomponenten anzuwenden, die separat gemäß den Bedingungen des WELMEC-Leitfadens 8.8 evaluiert werden können. Im Falle eines kompletten Geräts sind die Anforderungen einer Komponente der Kategorie 1 anzuwenden.

---

[2] d. h., Patches für alle bekannten Bugs und Schwachstellen wurden installiert

Für Komponenten der Kategorie 2:

- ist O2 nicht anwendbar.
- gelten O3, O4 und O5 vollständig.
- gelten O1, O6 und O7 für die Konfiguration/Einstellungen des Betriebssystems.

Ist dies der Fall, sind regelmäßige Updates des Betriebssystems möglich, solange sie die Konfiguration nicht beeinflussen. Technische Arbeitsgruppen können entscheiden, welche Komponenten der Kategorie 2 (wenn überhaupt) unter diese Ausnahme fallen. Für einige Betriebssystemtypen kann ein Update grundlegende Änderungen mit sich bringen, die auch die Konfiguration beeinflussen (bspw. ein großes Versionsupdate für Windows oder eine debianbasierte Linuxdistribution). In diesem Fall würde die obengenannte Ausnahme nicht gelten.

6.3 Spezifische Anforderungen an die Konfiguration von Universalbetriebssystemen

<table>
<tr><th>Risikoklasse C</th><th>Risikoklasse D</th><th>Risikoklasse E</th></tr>
<tr><td colspan="3">O1: Hardwareschutz
Der Teil der Hardware, auf dem das rechtlich relevante Betriebssystem läuft, muss gegen absichtliche Änderungen geschützt sein.</td></tr>
<tr><td colspan="3">Detaillierende Anmerkungen:
1. Bei Komponenten der Kategorie 1 und kompletten Geräten der Kategorie 1 muss das rechtlich relevante Betriebssystem gegen Entfernung oder Austausch geschützt sein.
2. Hardware-Schnittstellen, die das Betriebssystem beeinflussen können, sind entweder von der Stromzufuhr zu trennen, vom Betriebssystem aus zu deaktivieren, durch eine Hardware-Siegelung zu schützen oder an eine rückwirkungsfreie Schnittstelle zu koppeln (siehe O5).
3. Schnittstellen mit direktem Speicherzugriff müssen durch eine Hardware-Siegelung geschützt sein.
4. Der Speicherschutz des Betriebssystems muss aktiviert sein, um das Auslesen sensiblen kryptografischen Materials zu verhindern.</td></tr>
<tr><td>Erforderliche Dokumentation:
• Eine Liste aller Komponenten mit einem Betriebssystem.
• Beschreibung der Schutzmaßnahmen für Massenspeicher.
• Beschreibung der Schutzmaßnahmen für Hardware-Schnittstellen.</td><td colspan="2">Erforderliche Dokumentation (zusätzlich zur Dokumentation für Risikoklasse C):
• Falls kryptografisches Material genutzt wird: Beschreibung der Schutzmaßnahmen für flüchtige Speicher und Speichergeräte.</td></tr>
<tr><td colspan="3">Validierungsanleitung:
Auf Basis der Dokumentation ist zu prüfen:
• ob sämtliche Komponenten mit einem rechtlich relevanten Betriebssystem dokumentiert sind.
• ob alle Hardware-Schnittstellen geschützt bzw. für den rechtlich relevanten Datenaustausch notwendig sind. Ist dies der Fall, sind sie mit einer rückwirkungsfreien Schnittstelle auszustatten, siehe U4.
• ob sämtliche Maßnahmen zum Schutz von Speicher, Massenspeicher und Hardware-Schnittstellen effektiv und angemessen sind.</td></tr>
<tr><td></td><td colspan="2">Auf Basis der Konfigurationsdateien ist zu prüfen:
• ob die Konfiguration des Betriebssystems zum Speicherschutz mit den dokumentierten Maßnahmen übereinstimmt.
Funktionsprüfungen:
• ob die zusätzlichen Schutzmaßnahmen für das rechtlich relevante Betriebssystem und kryptografisches Material wirksam sind.</td></tr>
</table>

Beispiel einer akzeptablen Lösung:

- Das Gehäuse des Messgeräts ist physisch durch Siegel geschützt, um den Austausch von Massenspeichern zu verhindern, oder Massenspeicher werden während der Verwendung mit gesiegelten Verbindungen versehen.
- Eine Hardware-Siegelung wird genutzt, um sicherzustellen, dass das Massenspeichergerät, auf dem sich das rechtlich relevante Betriebssystem befindet, weder ausgetauscht noch entfernt werden kann.

	• Kryptografisches Material (z. B. Passwörter) wird in einer separaten Hardwarekomponente gespeichert, die durch das Betriebssystem gegen Zugriff geschützt ist.

Risikoklasse C	Risikoklasse D	Risikoklasse E

O2: Bootvorgang

Für Komponenten der Kategorie 1 *und komplette Geräte muss die Konfiguration des Bootvorgangs die gleiche konfigurierte Ausführungsumgebung für die rechtlich relevanter Software gewährleisten.*

Detaillierende Anmerkungen:

1. Der Bootprozess des Betriebssystems muss eindeutig und reproduzierbar sein.
2. Die rechtlich relevante Softwareanwendung muss in den Bootvorgang des Universalgeräts eingebunden sein.
3. Die Bootkonfiguration muss gegen Modifizierungen geschützt sein.
4. Am Ende des Bootvorgangs muss eine Vertrauenskette über die einzelnen Komponenten des Bootvorgangs hergestellt sein.
5. Die Verarbeitung der Vertrauenskette kann unterbrochen werden, wenn die Integrität der Vertrauenskette bewahrt bleibt.
6. Das Booten über offene Schnittstellen muss unterbunden sein.

	7. Der Bootprozess muss durch angemessene Maßnahmen abhängig vom Schutzniveau abgesichert sein.

Erforderliche Dokumentation:

- Informationen bezüglich der Bootkonfiguration des Betriebssystems (bspw. Massenspeicher, Partitionen, Kernelparameter).
- Beschreibung der Schutzmaßnahmen für den Bootprozess.
- Beschreibung der Struktur der Vertrauenskette.
- Beschreibung der Umgebung des gebooteten Betriebssystems für die rechtlich relevante Software.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob die Konfiguration des Bootprozesses gegen unzulässige Modifizierungen geschützt ist.
- ob das Betriebssystem bei jedem Start in dieselbe abgesicherte Umgebung für die rechtlich relevante Software gebootet wird.
- dass es keine nicht dokumentierten Unterbrechungen des Bootvorgangs gibt.
- ob das Booten über offene Schnittstellen unterbunden wird.

	Auf Basis der Dokumentation ist zu prüfen: • ob die genutzten kryptografischen Maßnahmen wirksam sind und den Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen für Datensicherheit entsprechen. *Auf Basis der Konfigurationsdateien ist zu prüfen:* • ob die Konfiguration des Bootloaders eindeutig ist. • ob es möglich ist, das Betriebssystem über offene Schnittstellen zu booten.

Beispiel einer akzeptablen Lösung:

- Die Startkonfiguration (BIOS) ist durch ein starkes Passwort geschützt worden.
  Die Integrität des Bootloaders und der rechtlich relevanten Teile des Betriebssystems wird mit Hilfe einer Prüfsumme überprüft.
- Ein TPM (trusted platform module) verifiziert die elektronische Signatur des Bootloaders, der Bootloader verifiziert dann das Betriebssystem, welches dann wiederum die rechtlich relevante Anwendung verifiziert und startet.

	• Abgesichertes Booten: Nur ein signierter Kernel kann vom Bootloader geladen werden. Vor dem Booten des Betriebssystems wird die elektronische Signatur des Kernels verifiziert.

Risikoklasse C	Risikoklasse D	Risikoklasse E

O3: Systemressourcen

Durch die Konfiguration des Betriebssystems muss sichergestellt werden, dass genug Ressourcen für die Ausführung der rechtlich relevanten Anwendung vorhanden sind.

Detaillierende Anmerkungen:

1. Das Betriebssystem muss so einschränkend wie möglich konfiguriert sein.
2. Die Ressourcen der rechtlich relevanten Software-Anwendung werden durch andere Software (rechtlich relevante und nicht rechtlich relevante) nicht unter das notwendige Minimum reduziert.

Erforderliche Dokumentation:

- Informationen bezüglich der Konfiguration der Teile des installierten Betriebssystems.

	• Informationen bezüglich der laufenden Prozesse während der Verwendung des Messgeräts.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob die installierten Teile des Betriebssystems angemessen und ausreichend konfiguriert sind, um den Betrieb des Messgeräts zu gewährleisten.

Funktionsprüfungen:

- ob der Export laufender Prozesse mit der Dokumentation übereinstimmt.
- Der Hersteller überprüft mithilfe der Systemauslastungsanzeige, ob genug Systemressourcen für die rechtlich relevante Anwendung während der Verwendung vorhanden sind.

Beispiel einer akzeptablen Lösung:

- Mithilfe der Paketverwaltung des Betriebssystems entfernt der Hersteller alle unnötigen Programme.
- Der Hersteller beschränkt die Laufzeit nicht rechtlich relevanter Anwendungen.
- Die Interrupt-Hierarchie ist so gestaltet, dass nachteilige Einflüsse vermieden werden.

<table>
<tr><th>Risikoklasse C</th><th>Risikoklasse D</th><th>Risikoklasse E</th></tr>
<tr><td colspan="3">O4: Schutz in Verwendung
Das Betriebssystem muss so konfiguriert sein, dass die rechtlich relevante Software nicht unzulässigerweise von Funktionen des Betriebssystems oder anderer Software beeinflusst werden kann.
Detaillierende Anmerkungen:
1. Die Administration der rechtlich relevanten Software (Anwendung und Betriebssystem) muss gesichert sein.
2. Die Zugriffskontrolle muss so konfiguriert sein, dass die beabsichtigte Nutzung nicht unzulässig beeinflusst werden kann.
3. Die Zugriffsberechtigungen müssen regelmäßig vom rechtlich relevanten Betriebssystem überprüft werden.
4. Das Betriebssystem muss so konfiguriert sein, dass das Entfernen rechtlich relevanter Software verhindert wird.
5. Der Anschluss von Zusatzeinrichtungen darf keinen unzulässigen Einfluss auf das Betriebssystem oder die Konfigurationseinstellungen haben.</td></tr>
<tr><td colspan="3">Erforderliche Dokumentation:
• Eine Liste gemounteter oder zu mountender Speichermedien mit ihren Attributen und Richtlinien zur Einschränkung ihrer Nutzung.
• Beschreibung der Verwaltung der Benutzerzugriffskontrolle und des Schutzes des Administratorkontos.
• Beschreibung des Operationsmodus der GUI.
• Beschreibung des Anschlusses von Zusatzeinrichtungen.</td></tr>
<tr><td colspan="3">Validierungsanleitung:
Auf Basis der Dokumentation ist zu prüfen:
• ob die Nutzung der rechtlich relevanten Anwendung von der Verwaltung des Systems separiert wurde, d. h., die rechtlich relevante Anwendung kann keine rechtlich relevante Administration/Konfiguration des Betriebssystems ändern.
• ob die Sicherungsmaßnahmen des Administratorkontos ausreichend sind und dass es kein zweites Konto mit unzulässigen Administratorrechten gibt.
• dass keine unzulässige Software von gemounteten Speichermedien ausgeführt werden kann.
• dass keine unzulässigen Funktionen des Betriebssystems durch Eingabegeräte (z. B. Tastaturkürzel) oder die Benutzeroberfläche aufgerufen werden können.
• dass die Anwendungssteuerung nur die Ausführung der rechtlich relevanten Software erlaubt, es sei denn, Softwaretrennung wurde implementiert.
• dass der Anschluss von Zusatzeinrichtungen das rechtlich relevante Betriebssystem oder die Konfigurationseinstellungen nicht unzulässig beeinflusst.
• ob rechtlich relevante Einstellungen des Betriebssystems weder zurückgesetzt noch modifiziert werden können.
Funktionsprüfungen:
• ob das Administratorkonto während der Nutzung gesperrt ist.
• ob sämtliche unzulässigen Tastaturkürzel deaktiviert wurden.
• ob das Verlassen oder Ändern des Operationsmodus der GUI unmöglich ist.
• ob die Anwendungssteuerung und die Richtlinien für Speichermedien sowie Zusatzeinrichtungen wirksam sind.
• ob die rechtlich relevanten Einstellungen nach einem Neustart beibehalten werden.</td></tr>
<tr><td colspan="2"></td><td>Auf Basis der Konfigurationsdateien ist darauf zu prüfen, dass:
• Nutzer- und Gruppenrechte, das Administratorkonto,
• die Konfiguration der Anwendungssteuerung,
• gemountete Speichermedien sowie Partitionen oder Medien mit Zugriffsattributen,
• Richtlinien für Speichermedien und Zusatzeinrichtungen
den Informationen in der Dokumentation entsprechen und korrekt konfiguriert sind.</td></tr>
</table>

Beispiel einer akzeptablen Lösung: • Alle rechtlich relevanten Anwendungen sind in einer dynamisch linkbaren Bibliothek (DLL) auf einem PC gebündelt. • Kryptografische Mittel stellen sicher, dass nur die rechtlich relevante dynamisch linkbare Bibliothek (DLL) mit dem Sensor, der an den PC angeschlossen ist, kommunizieren kann. • Das Fenster, das die rechtlich relevanten Daten anzeigt, wird durch Prozeduren in der rechtlich relevanten dynamisch linkbaren Bibliothek (DLL) generiert und kontrolliert. • Während der Messung überprüfen diese Prozeduren zyklisch, ob das relevante Fenster noch immer über allen anderen offenen Fenstern liegt. Wenn nicht, setzen die Prozeduren das Fenster nach oben, während die Prozesspriorisierung sicherstellt, dass andere I/O Geräte die CPU nicht dauerhaft blockieren.	**Beispiel einer akzeptablen Lösung:** • Das Betriebssystem verfügt über ein gesichertes Administratorkonto für die Administration sowie über ein Nutzerkonto mit eingeschränkten Rechten für die Nutzung während des Messbetriebs. • Das Betriebssystem startet bei jedem Start in einen Kioskmodus, in dem nur die rechtlich relevante Anwendung zugänglich ist. Tastaturkürzel wurden auf die rechtlich relevante Nutzung begrenzt. • Zugriff auf austauschbare Medien und Zusatzeinrichtungen wurde mithilfe von Gruppenrichtlinien eingeschränkt. • Es gibt keine Verzeichnisse mit Schreib- und Ausführungsrechten für Dateien auf dem System. • Das Administratorkonto wurde dauerhaft deaktiviert.

Risikoklasse C	Risikoklasse D	Risikoklasse E

O5: Rückwirkungsfreie Schnittstellen

Funktionen des Betriebssystems, die über offene Schnittstellen zugänglich sind, dürfen weder die rechtlich relevante Software noch rechtlich relevante Parameter oder Messdaten unzulässig beeinflussen.

Detaillierende Anmerkungen:

1. Die Kommunikation mit dem rechtlich relevanten Betriebssystem muss über rückwirkungsfreie Schnittstellen stattfinden.
2. Bei Softwaretrennung auf einem Betriebssystem gelten die Anhänge S und T für offene Netze für die Übertragung von rechtlich relevanten Messdaten über rückwirkungsfreie Schnittstellen des Betriebssystems.
3. Wenn die Konfiguration des Betriebssystems sicherstellt, dass es sich bei dem an einer offenen Schnittstelle angeschlossenen Kommunikationspartner nur um eine zertifizierte Komponente handeln kann und die Verbindung geschützt ist, ist keine weitere Prüfung der Schnittstelle erforderlich.

Erforderliche Dokumentation:

- Beschreibung der Konfiguration des Betriebssystems für offene Hardware- und Softwareschnittstellen und wie diese geschützt sind.
- Eine Liste von offenen Hardware- und Softwareschnittstellen, die nicht vom Betriebssystem konfiguriert sind.
- Eine Liste aller akzeptierten Befehle für und ihres Einflusses auf alle offenen Schnittstellen, die vom Betriebssystem verwaltet werden.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- dass offene Schnittstellen keinen unzulässigen Einfluss auf das rechtlich relevante Betriebssystem, seine Konfiguration, die rechtlich relevante Software-Anwendung, rechtlich relevante Parameter oder Messdaten haben.

	Auf Basis der Konfigurationsdateien ist darauf zu prüfen: dass unzulässiger Einfluss für die folgenden offenen Schnittstellen verhindert wird: • Netzwerkschnittstellen (offene und geschlossene Ports, verwendete Protokolle und Befehle, Richtlinien) • serielle Schnittstellen (Befehlsinterpreter der Anwendung, Richtlinien für die Benutzerkontensteuerung) • Softwareschnittstellen des Betriebssystems (Zugriffskontrolle, verwendete Befehle) Zusätzlich ist zu prüfen: • ob die genutzten kryptografischen Mittel wirksam sind und den Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen für Datensicherheit entsprechen. *Funktionsprüfungen:* • Kontrolle der Wirksamkeit der Konfiguration von offenen seriellen Schnittstellen. • Kontrolle der Wirksamkeit der Konfiguration von offenen Netzwerkschnittstellen.
Beispiel einer akzeptablen Lösung: • Alle Hardware-Schnittstellen mit Messdatenaustausch sind über das Betriebssystem (Netzwerk-Firewall, USB-Richtlinien) konfiguriert.	
	• Nutzung von IT-Sicherheitsprotokollen (VPN, IPSEC) für offene Netze.

Risikoklasse C	Risikoklasse D	Risikoklasse E

O6: Identifikation des Betriebssystems und seiner Konfiguration

Das Betriebssystem und die Konfiguration des Betriebssystems müssen identifizierbar sein. Die Identifikation des Betriebssystems und die Identifikation der Konfiguration des Betriebssystems müssen auf Befehl oder während des Betriebs angezeigt werden.

Detaillierende Anmerkungen:

1. Falls die rechtlich relevante Software und das Konto der Messanwendung durch eine spezifische Konfiguration des Betriebssystems geschützt sind, müssen die relevanten Dateien einen eigenen Identifikator haben.
2. Die Identifikation muss Module (Kernelmodule, Treiber, Bibliotheken) des Betriebssystems einschließen, die modifiziert wurden oder speziell für eine rechtlich relevante Aufgabe programmiert wurden.

Erforderliche Dokumentation:

- Allgemeine Informationen zum Betriebssystem (Hersteller, Distribution, Produktname, Kernelversion).
- Informationen zur Identifikation der Module des Betriebssystems, die für die rechtlich relevante Aufgabe konfiguriert wurden.
- Informationen zur Identifikation modifizierter oder selbstentwickelter Module des Betriebssystems für die rechtlich relevante Aufgabe.
- Eine Liste aller genutzten Identifikatoren sowie eine Beschreibung, wie sie erzeugt werden, ihrer Bedeutung und wie sie von nicht rechtlich relevanten Identifikatoren unterschieden werden können.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob alle Identifikatoren der Konfiguration des rechtlich relevanten Betriebssystems dokumentiert wurden.
- ob alle Identifikatoren von modifizierten oder hinzugefügten Modulen dokumentiert wurden.
- ob alle Identifikatoren des Betriebssystems eindeutig sind und dass die rechtlich relevanten Module des Betriebssystems vollständig und verständlich erfasst sind.
- ob Erzeugung, Darstellung und Schutz der Identifikatoren sowie ihre Unterscheidbarkeit zu anderen nicht rechtlich relevanten Identifikatoren vollständig dokumentiert und frei von Widersprüchen ist.

Funktionsprüfungen:

- Die Angaben der Identifikatoren des Betriebssystems sind mit der Dokumentation zu vergleichen.

Beispiel einer akzeptablen Lösung:

- Der Identifikator besteht aus dem Namen des Betriebssystemherstellers, dem Produktnamen und der Version des Betriebssystems. Alternativ werden Name und Version der Distribution sowie die Kernelversion genutzt.
- Darüber hinaus werden die für die rechtlich relevante Aufgabe konfigurierten Module des Betriebssystems mittels einer Prüfsumme identifiziert.

Risikoklasse C	Risikoklasse D	Risikoklasse E

O7: Schutz des Betriebssystems

Das Betriebssystem muss gegen absichtliche Modifizierungen geschützt werden.

Detaillierende Anmerkungen:

1. Module des Betriebssystems (Kernelmodule, Treiber, Bibliotheken), die speziell für eine rechtlich relevante Aufgabe programmiert sind, müssen ihren eigenen Schutz haben.
2. Die Schutzmaßnahmen für das Betriebssystem müssen alle rechtlich relevanten Module einschließen. Es kann eine Ausnahme gemacht werden, um die Bootloader-Konfiguration anstelle des Bootloaders selbst in die Schutzmaßnahme einzubeziehen, wenn dieser nicht Teil des Dateisystems des Betriebssystems ist.
3. Wenn eine Prüfsumme oder eine gleichwertige Schutzmaßnahme verwendet wird, muss sie mit Hilfe des Betriebssystems berechnet werden. Die berechnete Prüfsumme oder eine gleichwertige Schutzmaßnahme muss vom Betriebssystem oder einer rechtlich relevanten Anwendung angezeigt werden.
4. Die Integrität des rechtlich relevanten Betriebssystems muss periodisch überprüft werden. Wenn die Integritätsprüfung fehlschlägt, sind geräteadäquate Reaktionen erforderlich.
5. Aktualisierungen der rechtlich relevanten Module des Betriebssystems werden von dieser Anforderung nicht erfasst. Solche Aktualisierungen würden unter Anhang D fallen.

	6. Die Prüfsumme muss mit kryptografisch starken Methoden ermittelt werden.

Erforderliche Dokumentation:

- Dokumentation der Schutzmaßnahmen des Betriebssystems
- Beschreibung der Methoden zur Erzeugung und Anzeige der Schutzmaßnahmen
- Ausführliche Liste der rechtlich relevanten Module des Betriebssystems

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob alle rechtlich relevanten Module des Betriebssystems ausreichend von den Schutzmaßnahmen abgedeckt sind.
- ob Erzeugung und Darstellung der Schutzmaßnahmen vollständig und widerspruchsfrei dokumentiert sind.

Funktionsprüfungen:

- Wenn eine Prüfsumme verwendet worden ist: Die Angabe der Prüfsumme für die rechtlich relevanten Module des Betriebssystems ist zu prüfen (siehe Definition für Kategorien 1 und 2) und mit den Sollwerten zu vergleichen, die in der Dokumentation angegeben sind.
- Wenn alternative Maßnahmen verwendet wurden: Der Prototyp ist zu prüfen und mit der Dokumentation zu vergleichen.

	• Es ist zu überprüfen, ob die genutzten kryptografischen Maßnahmen wirksam sind und den Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen für Datensicherheit entsprechen.
Beispiel einer akzeptablen Lösung: • Linux: Prüfsumme über Bootloader, Kernel und das Verzeichnis /etc. • Windows: Prüfsumme über Teile des Systemverzeichnisses, Teile der exportierten Registry und Teile der Richtlinieneinstellungen für Benutzerrechte, Firewall, USB usw.	
• Die Prüfsumme ist ein CRC32.	• Die Prüfsumme ist ein SHA-Wert (secure hashing algorithm) mit einer von der ENISA empfohlenen Länge.

7 Anhang L: Speicherung von Messdaten

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

Die Speicherung beginnt zu dem Zeitpunkt, an dem eine Messung physisch abgeschlossen ist, und endet an dem Zeitpunkt, an dem alle durch die rechtlich relevante Software zu erledigenden Prozesse beendet sind. Die Anforderungen können ebenso auf die anschließende Langzeitspeicherung des Messergebnisses zum Zweck der Bereitstellung für rechtlich relevante Zwecke nach Abschluss der Messung angewendet werden.

7.1 Technische Beschreibung

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

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

Tabelle 7-1: Technische Beschreibung der Langzeitspeicherung

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

7.2 Spezifische Softwareanforderungen an die Speicherung

Risikoklasse B	Risikoklasse C	Risikoklasse D

L1: Vollständigkeit der gespeicherten Messdaten

Die gespeicherten Messdaten müssen von sämtlichen relevanten Informationen begleitet werden, die für rechtlich relevante Zwecke nötig sind.

Detaillierende Anmerkungen:

1. Die gespeicherten Messdaten müssen auf die Messung rückführbar sein, die die Daten erzeugt hat.
2. Die gespeicherten Messdaten müssen für die Kontrolle von Rechnungen ausreichend sein.
3. Die Art der notwendigen Informationen kann von der Geräteart abhängen.
4. Eine Voraussetzung, um diese besondere Anforderung zu erfüllen, ist die Identifizierung jedes gespeicherten Datensatzes.

Erforderliche Dokumentation:

Beschreibung aller Felder des Messdatensatzes.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob alle für die rechtlich relevanten Zwecke notwendigen Informationen im Messdatensatz enthalten sind.

Beispiel einer akzeptablen Lösung:

- Ein rechtlich und messtechnisch vollständiger Messdatensatz besteht aus den folgenden Feldern:
  - gemessener Mengenwert/gemessene Mengenwerte mit der richtigen Auflösung
  - Maßeinheit
  - Preis je Einheit oder zu zahlender Preis (falls zutreffend)
  - Datum und Uhrzeit der Messung (falls zutreffend)
  - Identifikator des Geräts
  - Ort der Messung (falls zutreffend)
- Die Messdaten werden mit der gleichen Auflösung, den gleichen Werten, Einheiten usw. gespeichert, wie auf dem Lieferschein angegeben oder ausgedruckt.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Datensätze korrekt aufgebaut werden.

Risikoklasse B	Risikoklasse C	Risikoklasse D

L2: Sicherung und Schutz gespeicherter Messdaten

Die gespeicherten Messdaten müssen gegen unbeabsichtigte Änderung gesichert und vor zufälliger Änderung geschützt sein.

Detaillierende Anmerkungen:

1. Gespeicherte Messdaten müssen von zusätzlichen redundanten Informationen begleitet sein, damit die Software, die diese Daten abruft, auswertet, anzeigt oder anderweitig verarbeitet, verifizieren kann, dass die Messdaten nicht infolge physikalischer Effekte (elektromagnetische Störung, Temperatur, Vibration usw.) verändert worden sind.
2. Es müssen Maßnahmen zur Sicherung von Messdaten implementiert werden, sodass sie nicht geändert werden und nur unter folgenden Bedingungen gelöscht werden können:
   a. Messdaten, die aus einem gemessenen Mengenwert bestehen, der ein Zwischenergebnis darstellt (siehe Kapitel 14), können nicht vom Nutzer gelöscht werden. Sie können aber automatisch gelöscht werden, wenn das nächste Modul oder die nächste Komponente eine ordnungsgemäße Ausführung der erwarteten Maßnahmen bestätigt.
   b. Bei anderen Messgeräten als Verbrauchsmessgeräten kann das Messergebnis nach Ablauf der Frist, in der ein dauerhafter Nachweis angefordert werden kann, gelöscht werden. Die Regelungen zur Mindestdauer der Speicherung von Messergebnissen bleiben den nationalen Vorschriften vorbehalten und gehen daher über den Rahmen dieses Leitfadens hinaus.
   c. Für Verbrauchsmessgeräte darf die gemessene Gesamtmenge nie gelöscht werden, d. h., diese Register müssen durch eine Hardware-Siegelung gegen Zurücksetzen gesichert werden. Bezüglich weiterer Informationen siehe WELMEC-Leitfäden 11.1, 11.3 und 13.1.

Erforderliche Dokumentation:

Die Methode, wie die Sicherung gegen unzulässige Änderungen realisiert ist, und wie die auslesende Software die Integrität der Messdaten überprüfen kann.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob eine Methode zur Erkennung zufälliger Datenänderungen implementiert ist.
- ob die Methode alle Daten erfasst.
- dass die Daten nicht gelöscht werden können, solange nicht alle Bedingungen erfüllt sind. Im Falle manueller Löschungen ist zu prüfen, ob diese erst nach erfolgreicher Überprüfung einer Sicherungsmaßnahme möglich sind, z. B., wenn ein Passwort eingegeben wird.

Funktionsprüfungen:

- Überprüfen durch praktische Stichproben, ob Messergebnisse nur gelöscht werden können, wenn die Bedingungen erfüllt sind. Im Falle manueller Löschungen ist zu prüfen, ob diese erst nach erfolgreicher Überprüfung einer Sicherungsmaßnahme möglich sind, z. B., wenn ein Passwort eingegeben wird.

Beispiel einer akzeptablen Lösung:

- Zur Erkennung 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, und im Gegensatz zu Anforderung L3 ist weder der Startwert des CRC-Registers noch das Generatorpolynom, d. h. der Divisor im Algorithmus, geheim. Startwert und Generatorpolynom sind gleichermaßen beiden Modulen bekannt, welche die Prüfsummen erzeugen und überprüfen.
- Messergebnis bzw. Rechnungsdateien werden durch das Anbringen eines automatischen Zeitstempels bei der Erzeugung und eines Kennzeichens, ob die Rechnung bezahlt oder unbezahlt ist, geschützt. Ein Dienstprogramm löscht oder verschiebt Dateien nur, wenn die Rechnungen bezahlt sind oder die Aufbewahrungsfrist abgelaufen ist.
- Das Messergebnis wird nicht ohne vorherige Genehmigung gelöscht, z. B. mittels Dialogs oder Fensters, die eine Löschbestätigung und ein Passwort abfragen.
- Das Messergebnis darf automatisch überschrieben werden, wenn ein angemessener Schutz der aufzubewahrenden Datensätze vorhanden ist. Ein Parameter, der die Mindestaufbewahrungszeit festlegt, kann bei Inbetriebnahme entsprechend den Bedürfnissen des Nutzers und der Datenspeichergröße eingestellt und gesichert werden. Das Gerät muss anhalten, wenn der Speicher voll und kein Datensatz alt genug zum Überschreiben ist. In diesem Fall kann manuelles Löschen (mit vorheriger Genehmigung und Eingabe eines Passworts) durchgeführt werden.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Maßnahmen zum Schutz der gespeicherten Daten angemessen und korrekt implementiert sind.

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">L3: Schutz gespeicherter Messdaten
Die gespeicherten Messdaten müssen vor absichtlichen Änderungen geschützt sein.</td></tr>
<tr><td colspan="3">Detaillierende Anmerkungen:
1. Die Sicherung muss gegen absichtliche Änderungen wirksam sein, die von leicht verfügbaren und handhabbaren Softwarewerkzeugen vorgenommen werden.
2. Gespeicherte Messdaten müssen von zusätzlichen redundanten Informationen begleitet sein, damit die Software, die diese Daten abruft, auswertet, anzeigt oder anderweitig verarbeitet, die Integrität der Messdaten verifizieren kann.</td></tr>
<tr><td colspan="2"></td><td>3. Der Schutz muss auch gegen absichtliche Änderungen wirksam sein, die durch spezielle, anspruchsvolle Softwarewerkzeuge ausgeführt werden.
4. Was Algorithmen und Mindestschlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden.
5. Auch wenn Algorithmus und Schlüssel das hohe Niveau erfüllen, setzt eine technische Lösung mit einem Standard-PC dieses Schutzniveau nicht um, sofern es nicht geeignete Schutzmaßnahmen für die Module gibt, die den Datensatz signieren oder überprüfen (siehe Basisleitfaden U für Messgeräte mit Universalgerät, detaillierende Anmerkungen U6-Risikoklasse D).</td></tr>
<tr><td colspan="3">Erforderliche Dokumentation:
Die Methode zur Umsetzung der Schutzmaßnahmen gegen unzulässige absichtliche Änderungen und wie die lesende Software die Integrität der Messdaten prüfen kann.</td></tr>
<tr><td colspan="2">Validierungsanleitung:
Auf Basis der Dokumentation ist zu prüfen:
• wenn eine Prüfsumme oder elektronische Signatur verwendet wird:
  • ob die Prüfsumme oder elektronische Signatur über den gesamten Datensatz erzeugt wird und
  • ob die rechtlich relevante Software, welche die Daten liest und eine Prüfsumme berechnet oder eine elektronische Signatur entschlüsselt, die berechneten Werte mit den Sollwerten vergleicht.
• ob geheime Daten (z. B. Schlüsselinitialwert, falls verwendet) gegen das Ausspähen mit einfachen Werkzeugen geheim gehalten werden.</td><td>Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C):
Auf Basis der Dokumentation ist zu prüfen:
• ob die genutzten Maßnahmen dem geforderten hohen Schutzniveau gemäß dem Stand der Technik entsprechen.</td></tr>
</table>

Beispiel einer akzeptablen Lösung: Das Modul des Speichergeräts berechnet eine CRC-32 des Datensatzes und hängt sie an den Datensatz an. Für diese Berechnung wird ein geheimer Startwert verwendet. Dieser Startwert wird als Schlüssel verwendet und als Konstante im ausführbaren Code gespeichert. Das lesende Modul hat diesen Startwert ebenfalls in seinem ausführbaren Code gespeichert. Vor der Verwendung des Datensatzes berechnet das lesende Modul die Prüfsumme und vergleicht diese mit der im Datensatz gespeicherten. Stimmen beide Werte überein, liegt keine Verfälschung des Datensatzes vor. Andernfalls geht das Modul von einer Verfälschung aus, verwirft den Datensatz und zeigt an, dass die Messdaten beschädigt sind.	**Beispiel einer akzeptablen Lösung:** Das rechtlich relevante Speichermodul generiert eine elektronische Signatur für den gespeicherten Datensatz. Diese wird an den gespeicherten Datensatz angehängt. Die zum Signieren verwendeten privaten und öffentlichen Schlüssel werden in einem Hardware-Sicherheitsmodul generiert, das den privaten Schlüssel vor Manipulation oder Auslesen schützt und den öffentlichen Schlüssel exportiert. Das lesende Modul verifiziert die elektronische Signatur mittels des öffentlichen Schlüssels, um die Authentizität und Integrität des Datensatzes zu überprüfen. Um die Herkunft des Datensatzes nachzuweisen, muss das Lesemodul wissen, ob der öffentliche Schlüssel wirklich zum Speichermodul gehört. Daher wird der öffentliche Schlüssel auf dem Display des Messgeräts angezeigt und kann einmalig registriert werden, z. B. zusammen mit der Seriennummer des Messgeräts, wenn es im Feld verifiziert wird. Im Falle einer Unregelmäßigkeit geht das Modul von einer Verfälschung aus, verwirft den Datensatz und zeigt an, dass die Messdaten fehlerhaft sind.
Zusätze für Risikoklasse E	
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.	
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklasse D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Maßnahmen zur Integritätssicherung angemessen und korrekt implementiert sind.	

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

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

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklasse D):

Auf Basis des Quellcodes ist zu prüfen:

- ob die Datensätze korrekt aufgebaut sind und zuverlässig auf Messgerät und Messung zurückgeführt werden.

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">L5: Schutz vertraulicher Informationen
Vertrauliche Informationen müssen geheim gehalten und gegen Änderungen sowie Kompromittierung geschützt werden.</td></tr>
<tr><td colspan="3">Detaillierende Anmerkungen:
1. Nur die rechtlich relevante Software darf Lesezugriff auf vertrauliche Informationen haben.
2. Die Sicherungsmaßnahmen müssen gewährleisten, dass keine Änderungen mittels leicht verfügbarer und handhabbarer Softwarewerkzeuge vorgenommen werden können.
3. Je nach Schutzmaßnahme können die vertraulichen Informationen aus Schlüsseln, Generatorpolynomen, Startwerten, Seeds etc. bestehen.</td></tr>
<tr><td colspan="2"></td><td>4. Die Schutzmaßnahmen müssen gewährleisten, dass keine Änderungen mit speziellen, anspruchsvollen Softwarewerkzeugen ausgeführt werden können.
5. 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 Messgeräte mit Universalgerät U6).</td></tr>
<tr><td colspan="3">Erforderliche Dokumentation:
Beschreibung der Verwaltung von geheimen Informationen und der Mittel zur Geheimhaltung von Schlüsseln und anderen Informationen.</td></tr>
<tr><td colspan="2">Validierungsanleitung:
Auf Basis der Dokumentation ist zu prüfen:
• ob die geheimen Informationen kompromittiert werden können.</td><td>Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C):
Auf Basis der Dokumentation ist zu prüfen:
• ob die genutzten Maßnahmen dem geforderten hohen Schutzniveau gemäß dem Stand der Technik entsprechen.</td></tr>
<tr><td colspan="2">Beispiel einer akzeptablen Lösung:
Der geheime Schlüssel und zugehörige Informationen sind in Binärformat und verschlüsselt im ausführbaren Code der rechtlich relevanten Software gespeichert. Die Software bietet keine Funktionen zur Anzeige und zum Bearbeiten dieser Daten und der flüchtige Speicher wird durch die Betriebssystemkonfiguration geschützt, um das Auslesen sensiblen kryptografischen Materials zu verhindern, siehe O1.</td><td>Beispiel einer akzeptablen Lösung:
Der geheime Schlüssel befindet sich in einem Hardwareteil, der physisch versiegelt werden kann. Die Software bietet keine Funktionen zur Anzeige oder zum Bearbeiten dieser Daten.</td></tr>
</table>

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklasse D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Maßnahmen für den Umgang mit geheimen Informationen angemessen sind.

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">L6: Abruf, Verifizierung und Anzeige gespeicherter Messdaten
Falls Messdaten für rechtlich relevante Zwecke verwendet werden, muss es eine rechtlich relevante Komponente oder ein Modul für das Lesen, die Verifizierung, die Behandlung und die Anzeige gespeicherter Messdaten geben.</td></tr>
<tr><td colspan="3">Detaillierende Anmerkungen:
1. Die rechtlich relevante Software muss in der Lage sein, die gespeicherten Messdaten zu lesen, zu verifizieren, zu behandeln und anzuzeigen. Bezüglich der Anforderungen an die Darstellung von Messdaten, siehe P8/U8.
2. Die abgerufenen Messdaten müssen verifiziert sein.
3. Im Falle einer Unregelmäßigkeit dürfen die Messdaten nicht für weitere rechtlich relevante Zwecke genutzt werden. Die Daten müssen als ungültig registriert werden. Diese Registrierung ist zu messergebnisrelevanten Daten zu zählen.
4. Die angezeigten oder gedruckten Messdaten müssen auf jegliche Unregelmäßigkeit der Messdaten hinweisen.</td></tr>
<tr><td colspan="3">Erforderliche Dokumentation:
• Beschreibung der Funktionen der Abrufsoftware.
• Beschreibung, wie die Messdaten verifiziert werden.
• Beschreibung, wie beschädigte Daten behandelt und angezeigt werden.</td></tr>
<tr><td colspan="3">Validierungsanleitung:
Auf Basis der Dokumentation ist zu prüfen:
• ob die Abrufsoftware die erforderlichen Fähigkeiten hat.
Funktionsprüfungen:
• Durchführung von Stichprobenüberprüfungen darauf, ob der Abruf alle erforderlichen Informationen liefert.</td></tr>
<tr><td colspan="2">Beispiel einer akzeptablen Lösung:
• Das rechtlich relevante Modul des Speichergeräts berechnet eine CRC-32 des Datensatzes und hängt sie an den Datensatz an, siehe L3. Für diese Berechnung wird ein geheimer Startwert verwendet. Dieser Startwert wird als Schlüssel verwendet und als Konstante im ausführbaren Code gespeichert. Das lesende Modul hat diesen Startwert ebenfalls in seinem ausführbaren Code gespeichert. Vor der Verwendung des Datensatzes berechnet das lesende Modul die Prüfsumme und vergleicht diese mit der im Datensatz gespeicherten. Stimmen beide Werte überein, liegt keine Verfälschung des Datensatzes vor. Andernfalls geht das Modul von einer Verfälschung aus, verwirft den Datensatz und zeigt an, dass die Messdaten beschädigt sind.</td><td>Beispiel einer akzeptablen Lösung:
• Das rechtlich relevante Speichermodul generiert eine elektronische Signatur für den gespeicherten Datensatz. Diese wird an den gespeicherten Datensatz angehängt. Die zum Signieren verwendeten privaten und öffentlichen Schlüssel werden in einem Hardware-Sicherheitsmodul generiert, das den privaten Schlüssel vor Manipulation oder Auslesen schützt und den öffentlichen Schlüssel exportiert. Das lesende Modul verifiziert die elektronische Signatur mittels des öffentlichen Schlüssels, um die Authentizität und Integrität des Datensatzes zu überprüfen. Um die Herkunft des Datensatzes nachzuweisen, muss das Lesemodul wissen, ob der öffentliche Schlüssel wirklich zum Speichermodul gehört. Daher wird der öffentliche Schlüssel auf dem Display des Messgeräts angezeigt und kann einmalig registriert werden, z. B. zusammen mit der Seriennummer des Messgeräts, wenn es im Feld verifiziert wird.
• Im Falle einer Unregelmäßigkeit geht das Modul von einer Verfälschung aus, verwirft den Datensatz und zeigt an, dass die Messdaten fehlerhaft sind.</td></tr>
<tr><th colspan="3">Zusätze für Risikoklasse E</th></tr>
</table>

Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Maßnahmen zum Lesen, Überprüfen elektronischer Signaturen usw. angemessen und korrekt implementiert sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D

L7: Automatisches Speichern

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

Detaillierende Anmerkungen:

1. Die Speicherfunktion darf nicht von der Entscheidung des Bedieners abhängen.
2. In Fällen, in denen der Bediener die Entscheidung treffen muss, ob er ein Messergebnis akzeptiert oder nicht, müssen die Messdaten automatisch gespeichert werden, nachdem die Entscheidung getroffen wurde.

Erforderliche Dokumentation:

- Beschreibung der automatischen Speicherung.
- Beschreibung der grafischen Benutzeroberfläche im Falle von bedienerabhängigen Speicherentscheidungen.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob der Speicherprozess automatisch abläuft.

Funktionsprüfungen:

- Stichprobenkontrollen, ob die Messdaten nach der Messung oder nach Annahme des Messergebnisses automatisch gespeichert werden. Es ist zu darauf zu prüfen, dass es keine Schaltflächen oder Menüpunkte zum Unterbrechen oder Deaktivieren der automatischen Speicherung gibt.

Beispiel einer akzeptablen Lösung:

In der grafischen Benutzeroberfläche (GUI) gibt es weder Menüpunkte noch Schaltflächen, die ein manuelles Anstoßen des Speicherns von Messergebnissen unterstützen. Die Messwerte werden zusammen mit messergebnisrelevanten Daten wie Zeitstempel und Signatur in einen Datensatz gepackt und sofort nach der Messung bzw. nach Annahme des Messergebnisses gespeichert.

Zusätze für Risikoklasse E

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

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

Auf Basis des Quellcodes ist zu prüfen:

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

Risikoklasse B	Risikoklasse C	Risikoklasse D

L8: Speicherkapazität und -dauer

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

Detaillierende Anmerkungen:

1. Wenn ein Speicher voll ist oder entfernt oder vom Gerät getrennt wird, muss eine Warnung an den Bediener gegeben werden.
2. Es muss sichergestellt sein, dass nur abgelaufene Messdaten überschrieben werden können.
3. Die Regelungen hinsichtlich des Mindestzeitraums für die Speicherung von Messdaten und der geforderten Kennzeichnungen sind nationalen Regelungen überlassen und liegen daher außerhalb des Anwendungsbereiches dieses Leitfadens.
4. Die Informationen über die Speicherkapazität müssen verfügbar sein.

Erforderliche Dokumentation:

- Speicherkapazität, Beschreibung der Verwaltung der Messdatenspeicherung.
- Beschreibung des Verhaltens des Geräts, wenn der Speicher voll ist oder entfernt wurde.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

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

Funktionsprüfungen:

- Überprüfen, ob eine Warnung erfolgt, wenn der Speicher voll ist oder, falls zutreffend, wenn er entfernt wurde.

Beispiel einer akzeptablen Lösung:

- Für unterbrechbare Messungen, wenn der Speicher nicht mehr verfügbar ist, bevor die Messung abgeschlossen ist: Das Messgerät hat einen Puffer, der groß genug für die Speicherung der aktuellen Messdaten ist. Es wird kein neuer Messvorgang begonnen und die gepufferten Werte werden zur späteren Übertragung in einen neuen Speicher aufbewahrt.
- Nicht unterbrechbare Messungen: Das kumulative Register wird zu einem späteren Zeitpunkt, wenn der Speicher wieder verfügbar ist, ausgelesen und übertragen.
- Messdaten werden automatisch von einem Werkzeug überschrieben, das prüft, ob die Messdaten veraltet sind (den jeweiligen Zeitraum regeln nationale Bestimmungen). Das Dienstprogramm fordert die Löscherlaubnis vom Benutzer und die Daten werden in der Reihenfolge „älteste zuerst“ gelöscht.

Zusätze für Risikoklasse E

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

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

Auf Basis des Quellcodes ist zu prüfen:

- ob die Maßnahmen für die Speicherung angemessen und korrekt implementiert sind.

8 Anhang T: Messdatenübertragung über Kommunikationsnetze

Die spezifischen Anforderungen dieses Kapitels gelten nur, wenn Messdaten für rechtlich relevanten Zwecke über Kommunikationsnetze übertragen werden. Wenn dies der Fall ist, müssen die Messdaten von einer rechtlich relevanten Komponente bzw. einem Modul übertragen und empfangen werden.

Sie bilden einen Anhang zu den spezifischen Anforderungen sowohl an die Software eines Messgerätes mit zweckgebundener Hard- und Software (Typ-P-Anforderungen) als auch an die Software von Messgeräten mit Universalgerät (Typ-U-Anforderungen).

Wenn Software auf ein Gerät heruntergeladen wird, das der gesetzlichen Kontrolle unterliegt, gelten die Anforderungen des Anhangs D.

8.1 Technische Beschreibung

In der folgenden Tabelle sind zwei Netzwerkkonfigurationen aufgezeigt.

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

Tabelle 8-1: Technische Beschreibung der Kommunikationsnetze.

8.2 Spezifische Softwareanforderungen an die Messdatenübertragung

Risikoklasse B	Risikoklasse C	Risikoklasse D
T1: Vollständigkeit der übertragenen Messdaten *Die übertragenen Messdaten müssen alle relevanten Informationen enthalten, die zur Darstellung oder Weiterverarbeitung der Messdaten in der Empfangseinheit nötig sind.*		
Detaillierende Anmerkungen: Die Vollständigkeit hängt individuell vom Typ der Messung ab.		
Erforderliche Dokumentation: Beschreibung aller Felder des Messdatensatzes.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob alle Informationen für die weitere Messdatenverarbeitung in der Empfangseinheit im Datensatz enthalten sind.		
Beispiel einer akzeptablen Lösung: Der Messdatensatz umfasst die folgenden Felder: • gemessener Mengenwert/gemessene Mengenwerte mit der richtigen Auflösung • Maßeinheit • Preis je Einheit oder zu zahlender Preis (falls zutreffend) • Datum und Uhrzeit der Messung (falls zutreffend) • Identifikator des Geräts, falls zutreffend (Datenübertragung) • Ort der Messung (falls zutreffend)		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Datensätze korrekt aufgebaut sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D

T2: Sicherung und Schutz übertragener Messdaten

Die übertragenen Messdaten müssen gegen unbeabsichtigte Änderung gesichert und vor zufälliger Änderung geschützt sein.

Detaillierende Anmerkungen:

1. Es müssen Maßnahmen zur Sicherung gegen unbeabsichtigte Änderungen und zur Erkennung von Änderungen oder zum Verlust übertragener Messdaten implementiert werden.

Erforderliche Dokumentation:

Beschreibung der verwendeten Methoden zur Sicherung der übertragenen Messdaten und zur Erkennung von Übertragungsfehlern oder Verlust von übertragenen Messdaten.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob eine Methode zur Sicherung übertragener Messdaten und zum Erkennen von Übertragungsfehlern oder Verlust von Messdaten umgesetzt ist.

Beispiel einer akzeptablen Lösung:

- Die übertragenen Messdaten werden von zusätzlichen redundanten Informationen begleitet, die es der Software des Empfängers ermöglichen, zufällige Datenübertragungsfehler zu erkennen.
- Zum Erkennen von Messdatenänderungen wird mit dem CRC-16-Algorithmus eine Prüfsumme über sämtliche Byte des gesamten Datensatzes berechnet und in den zu übertragenden Datensatz eingefügt.
- Im Fall von Übertragungsfehlern verwirft das empfangende Modul den Datensatz und fordert die erneute Übertragung der Daten.

  Hinweis: Der Algorithmus ist nicht geheim und, im Gegensatz zu Anforderung T3, sind es auch weder der Startwert des CRC-Registers noch das Generatorpolynom, d. h. der Divisor im Algorithmus. Startwert und Generatorpolynom sind gleichermaßen beiden Modulen bekannt, welche die Prüfsummen erzeugen und verifizieren.
- Nutzung von Mitteln, die von Übertragungsprotokollen, z. B. TCP/IP, IFSF, bereitgestellt werden.

Zusätze für Risikoklasse E

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

Quellcode der rechtlich relevanten Software.

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

Auf Basis des Quellcodes ist zu prüfen:

- ob die Maßnahmen zum Schutz der übertragenen Daten angemessen und korrekt implementiert sind.

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">T3: Schutz übertragener Messdaten
Die gespeicherten Messdaten müssen vor absichtlichen Änderungen geschützt sein.</td></tr>
<tr><td colspan="3">Detaillierende Anmerkungen:
1. Diese Anforderung bezieht sich nur auf offene Netze, nicht auf geschlossene Netze.
2. Die Sicherung muss gegen absichtliche Änderungen wirksam sein, die von leicht verfügbaren und handhabbaren Softwarewerkzeugen vorgenommen werden.</td></tr>
<tr><td colspan="2"></td><td>3. Der Schutz muss auch gegen absichtliche Änderungen wirksam sein, die durch spezielle, anspruchsvolle Softwarewerkzeuge ausgeführt werden.
4. Was Algorithmen und Mindestschlüssellängen betrifft, müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden.
5. Um die hohe Schutzstufe zu erfüllen, sind geeignete Schutzmittel für das Softwaremodul (z. B. Hardwareunterstützung), das einen Datensatz signiert oder verifiziert, notwendig (siehe auch Kapitel 5 für Software auf Messgeräten mit Universalgeräten, spezifische Anforderung U6, detaillierende Anmerkung 7 für Risikoklasse D).</td></tr>
<tr><td colspan="3">Erforderliche Dokumentation:
Beschreibung der Schutzmethode.</td></tr>
<tr><td colspan="3">Validierungsanleitung:
Auf Basis der Dokumentation ist zu prüfen:
• ob eine angemessene Methode ausgewählt wurde.</td></tr>
</table>

Beispiel einer akzeptablen Lösung: • Das sendende Modul berechnet eine CRC-32 des Datensatzes und hängt sie an den Datensatz an. Für diese Berechnung wird ein geheimer Startwert verwendet. Dieser Startwert wird als Schlüssel verwendet und als Konstante im ausführbaren Code gespeichert. Das empfangende Modul hat diesen Startwert ebenfalls in seinem ausführbaren Code gespeichert. Vor der Verwendung des Datensatzes berechnet das empfangende Modul die Prüfsumme und vergleicht diese mit der im Datensatz gespeicherten. Stimmen beide Werte überein, liegt keine Verfälschung des Datensatzes vor. Andernfalls geht das Modul von einer Verfälschung aus, verwirft den Datensatz und fordert die erneute Übertragung der Daten an.	**Beispiel einer akzeptablen Lösung:** Das rechtlich relevante Sendemodul generiert eine elektronische Signatur für den übertragenen Datensatz. Diese wird an den übertragenen Datensatz angehängt. Die zum Signieren verwendeten privaten und öffentlichen Schlüssel werden in einem Hardware-Sicherheitsmodul generiert, das den privaten Schlüssel vor Manipulation oder Auslesen schützt und den öffentlichen Schlüssel exportiert. Das Empfangsmodul verifiziert die elektronische Signatur mittels des öffentlichen Schlüssels, um die Authentizität und Integrität des Datensatzes zu überprüfen. Um die Integrität und Authentizität des Datensatzes nachzuweisen, muss das Empfangsmodul wissen, ob der öffentliche Schlüssel wirklich zum Speichermodul gehört. Daher wird der öffentliche Schlüssel auf dem Display des Messgeräts angezeigt und kann einmalig registriert werden, z. B. zusammen mit der Seriennummer des Messgeräts, wenn es im Feld verifiziert wird. Im Falle einer Unregelmäßigkeit geht das Empfangsmodul von einer Verfälschung aus, verwirft den Datensatz und fordert die erneute Übertragung der Daten an.
Zusätze für Risikoklasse E	
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.	
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Maßnahmen zur Integritätsgarantie übertragener Messdaten angemessen sind.	

Risikoklasse B	Risikoklasse C	Risikoklasse D

T4: Rückführbarkeit der übertragenen Messdaten

Es muss möglich sein, übertragene Messdaten, die zu rechtlich relevanten Zwecken genutzt werden, auf die Messung sowie auf die rechtlich relevante Komponente/das Modul/das Messinstrument, die die Daten generiert haben, zurückzuführen.

Detaillierende Anmerkungen:

1. Diese Anforderung bezieht sich nur auf offene Netze, nicht auf geschlossene Netze.
2. Die Rückführbarkeit erfordert die korrekte Zuordnung (Verknüpfung) von Messdaten zu der Messung, bei der die Daten erzeugt wurden.
3. Rückführbarkeit erfordert die korrekte Zuordnung (Verknüpfung) von Messdaten zum Messgerät, das die Messdaten erzeugt hat.
4. Die Rückführbarkeit auf Messungen setzt eine Identifizierung der Messungen voraus.
5. Die Rückführbarkeit auf ein Messgerät setzt eine Identifizierung des Messgeräts voraus.
6. Die Sicherung muss gegen absichtliche Änderungen wirksam sein, die von leicht verfügbaren und handhabbaren Softwarewerkzeugen vorgenommen werden.

		7. Der Schutz muss auch gegen absichtliche Änderungen wirken, die durch spezielle, anspruchsvolle Softwarewerkzeuge ausgeführt werden. 8. Was Algorithmen und Mindestschlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden.

Erforderliche Dokumentation:

- Beschreibung der zur Gewährleistung der Rückführbarkeit genutzten Methode.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob die Mittel zur Gewährleistung der Rückführbarkeit angemessen sind.

Beispiel einer akzeptablen Lösung:

- Jeder Datensatz hat eine eindeutige (sequentielle) Identifikationsnummer, die den Zeitpunkt enthält, zu dem die Messung genommen wurde (Zeitstempel).
- Jeder Messdatensatz enthält Informationen über die Herkunft der Messdaten, d. h. die Seriennummer oder ein Identitätsmerkmal des Messgerätes, das die Daten erzeugt hat.
- In offenen Netzen ist die Rückführbarkeit zur Komponente oder zum Modul oder zum Messgerät gewährleistet, wenn der Messdatensatz eine eindeutige elektronische Signatur trägt. Die elektronische Signatur deckt alle diese Felder des Messdatensatzes ab.
- Der Empfänger des Messdatensatzes überprüft alle Daten auf Plausibilität.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Maßnahmen zur Gewährleistung der Rückführbarkeit der übertragenen Messdaten angemessen sind.

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">T5: Schutz vertraulicher Informationen
Vertrauliche Informationen müssen geheim gehalten und gegen Änderungen sowie Kompromittierung geschützt werden.</td></tr>
<tr><td colspan="3">Detaillierende Anmerkungen:
1. Nur die rechtlich relevante Software darf Lesezugriff auf vertrauliche Informationen haben.
2. Die Schutzmaßnahmen müssen gewährleisten, dass keine Änderungen mittels leicht verfügbarer und handhabbarer Softwarewerkzeuge vorgenommen werden können.
3. Je nach Schutzmaßnahme können die vertraulichen Informationen aus Schlüsseln, Generatorpolynomen, Startwerten, Seeds etc. bestehen.</td></tr>
<tr><td colspan="2"></td><td>4. Der Schutz muss gewährleisten, dass nur die rechtlich relevante Software Lesezugriff hat und dass keine Änderungen oder Modifizierungen mit speziellen, anspruchsvollen Softwarewerkzeugen ausgeführt werden können.
5. 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 Messgeräte mit Universalgerät U6).</td></tr>
<tr><td colspan="3">Erforderliche Dokumentation:
Beschreibung der Verwaltung von geheimen Informationen und der Mittel zur Geheimhaltung von Schlüsseln und anderen Informationen sowie die Beschreibung von Maßnahmen gegen Modifizierungen dieser.</td></tr>
<tr><td colspan="2">Validierungsanleitung:
Auf Basis der Dokumentation ist zu prüfen:
• ob die geheimen Informationen weder offengelegt noch verändert werden können.</td><td>Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B und C):
Auf Basis der Dokumentation ist zu prüfen:
• ob die genutzten Maßnahmen dem geforderten hohen Schutzniveau gemäß dem Stand der Technik entsprechen.</td></tr>
<tr><td colspan="2">Beispiel einer akzeptablen Lösung:
Der geheime Schlüssel und zugehörige Informationen sind in Binärformat und verschlüsselt im ausführbaren Code der rechtlich relevanten Software gespeichert. Die Systemsoftware bietet keine Funktionen zur Anzeige und zum Bearbeiten dieser Daten und der flüchtige Speicher wird durch die Betriebssystemkonfiguration geschützt, um das Auslesen sensiblen kryptografischen Materials zu verhindern. Siehe O1.</td><td>Beispiel einer akzeptablen Lösung:
Der geheime Schlüssel befindet sich in einem Hardwareteil, der physisch versiegelt werden kann. Die Software bietet keine Funktionen zur Anzeige und zum Bearbeiten dieser Daten.</td></tr>
</table>

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklasse D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Maßnahmen für die Handhabe vertraulicher Informationen angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
T6: Empfang, Verifizierung und Handhabung übertragener Messdaten *Falls Messdaten für rechtlich relevante Zwecke verwendet werden, muss es eine rechtlich relevante Komponente oder ein Modul für den Empfang, die Verifizierung, Handhabung und Anzeige übertragener Messdaten geben.*		
Detaillierende Anmerkungen: 1. Die rechtlich relevante Software muss in der Lage sein, die übertragenen Messdaten zu empfangen, zu verifizieren, zu behandeln und anzuzeigen. Bezüglich der Anforderungen an die Darstellung von Messdaten, siehe P8/U8. 2. Die empfangenen Messdaten müssen verifiziert sein. 3. Im Falle einer Unregelmäßigkeit dürfen die Messdaten nicht für weitere rechtlich relevante Zwecke genutzt werden. Entweder verwirft das Empfangsmodul den Datensatz und fordert eine erneute Übertragung der Daten, oder es registriert den Empfang eines beschädigten Datensatzes. Diese Registrierung ist zu messergebnisrelevanten Daten zu zählen. 4. Die angezeigten oder gedruckten Messdaten müssen auf jegliche Unregelmäßigkeit der Messdaten hinweisen.		
Erforderliche Dokumentation: • Beschreibung der Funktionen der Empfangssoftware. • Beschreibung, wie die Messdaten verifiziert werden. • Beschreibung, wie beschädigte Daten behandelt und angezeigt werden.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob beschädigte Daten nicht akzeptiert und entweder durch die korrekten Daten ersetzt oder entsprechend registriert werden. *Funktionsprüfungen:* • Überprüfen, ob korrumpierte Messdaten nicht akzeptiert werden und entweder durch die korrekten Daten ersetzt oder entsprechend registriert werden.		
Beispiel einer akzeptablen Lösung: • Das rechtlich relevante Modul des sendenden Geräts berechnet eine CRC-32 des Datensatzes und hängt sie an den Datensatz an, siehe T2 und T3. Für diese Berechnung wird ein geheimer Startwert verwendet. Dieser Startwert wird als Schlüssel verwendet und als Konstante im ausführbaren Code gespeichert. Das empfangende Modul hat diesen Startwert ebenfalls in seinem ausführbaren Code gespeichert. Vor der Verwendung des Datensatzes berechnet das empfangende Modul die Prüfsumme und vergleicht diese mit der im Datensatz gespeicherten. Stimmen beide Werte überein, liegt keine Verfälschung des Datensatzes vor. Andernfalls geht das Modul von einer Verfälschung aus, verwirft den Datensatz und fordert eine erneute Übertragung der Daten an.		**Beispiel einer akzeptablen Lösung:** • Die rechtlich relevante sendende Software generiert eine elektronische Signatur für den übertragenen Datensatz. Diese wird an den übertragenen Datensatz angehängt, siehe T2 und T3. Das Empfangsmodul verifiziert die elektronische Signatur mittels des öffentlichen Schlüssels, um die Authentizität und Integrität des Datensatzes zu überprüfen. Um die Herkunft des Datensatzes nachzuweisen, muss das Lesemodul wissen, ob der öffentliche Schlüssel wirklich zum Sendemodul gehört. Daher wird der öffentliche Schlüssel auf dem Display des Messgeräts angezeigt und kann einmalig registriert werden, z. B. zusammen mit der Seriennummer des Messgeräts, wenn es im Feld verifiziert wird. Im Falle einer Unregelmäßigkeit geht das Modul von einer Verfälschung aus, verwirft den Datensatz und fordert eine erneute Übertragung der Daten an.

Zusätze für Risikoklasse E

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

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

Auf Basis des Quellcodes ist zu prüfen:

- ob die Maßnahmen für die Handhabung beschädigter Messdaten angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D

T7: Übertragungsverzögerung

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

Detaillierende Anmerkungen:

Die Zeitintervalle der Datenübertragung müssen so gewählt werden, dass unter den ungünstigsten Bedingungen die Messung nicht unzulässig beeinflusst wird.

Erforderliche Dokumentation:

Beschreibung des Konzepts, wie die Messung gegen Übertragungsverzögerungen geschützt wird.

Validierungsanleitung:

- Überprüfen des Konzeptes, das gewährleistet, dass die Messung durch Übertragungsverzögerungen nicht beeinflusst wird.

Beispiel einer akzeptablen Lösung:

Implementierung von Übertragungsprotokollen für Feldbusse.

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Maßnahmen für die Handhabung von Übertragungsverzögerungen angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D
T8: Verfügbarkeit von Übertragungsdiensten *Wenn Netzwerkdienste nicht verfügbar sind, dürfen keine Messdaten verloren gehen.*		
Detaillierende Anmerkungen: 1. Es darf nicht möglich sein, Messdaten durch Verzögern oder Unterdrücken der Übertragung zu korrumpieren. 2. Das sendende Gerät muss in der Lage sein, mit zufällig auftretenden Übertragungsstörungen umzugehen. 3. Die Reaktion des Messgerätes auf einen Ausfall der Übertragungsdienste hängt vom Messprinzip ab (siehe Anhang I).		
Erforderliche Dokumentation: Beschreibung der Schutzmaßnahmen gegen Übertragungsunterbrechungen oder andere Fehler.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • die genutzten Maßnahmen, um die Messdaten bei Übertragungsstörungen und Unterbrechung zu schützen. *Funktionsprüfungen:* • Stichprobenüberprüfungen darauf, dass keine relevanten Daten aufgrund einer Übertragungsunterbrechung verloren gehen.		
Beispiel einer akzeptablen Lösung: 1) Unterbrechbare Messungen: die Messung wird abgeschlossen, obwohl die Übertragung unterbrochen ist. Jedoch muss das Messgerät oder das Gerät, das die rechtlich relevanten Daten überträgt, einen Puffer haben, der groß genug für die Speicherung der aktuellen Messung ist. Danach kann keine neue Messung gestartet werden und die gepufferten Werte müssen für die spätere Übertragung aufbewahrt werden. Für weitere Beispiele siehe Anhang I. 2) Nicht unterbrechbare Messungen: Das kumulative Register kann zu einem späteren Zeitpunkt ausgelesen und übertragen werden, wenn die Verbindung wieder besteht.		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Maßnahmen für die Reaktion auf unterbrochene Übertragungsdienste angemessen sind.

9 Anhang S: Softwaretrennung

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

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

9.1 Technische Beschreibung

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

9.2 Spezifische Softwareanforderungen an die Softwaretrennung

Risikoklasse B	Risikoklasse C	Risikoklasse D
S1: Umsetzung der Softwaretrennung Es muss einen Teil der Software geben, der die gesamte rechtlich relevante Software sowie sämtliche Parameter enthält und der eindeutig von anderen Teilen der Software getrennt ist.		
Detaillierende Anmerkungen: 1. Die rückwirkungsfreie Softwareschnittstelle selbst (siehe S3) ist rechtlich relevant. 2. Bezüglich der Festlegung, ob Software, Parameter oder Daten rechtlich relevant sind oder nicht, siehe Kapitel 15.		
Erforderliche Dokumentation: Benennung sämtlicher Module, die zur rechtlich relevanten Software gehören.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob die Benennung korrekt und die Liste der genannten Module vollständig ist.		
Beispiel einer akzeptablen Lösung:		

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): *Auf Basis des Quellcodes ist zu prüfen:* • ob alle Module, die an der Messwertverarbeitung beteiligt sind, als rechtlich relevante Software aufgelistet sind. (Überprüfen z. B. durch Datenflussanalyse mit Softwarewerkzeugen oder manuell.)

Risikoklasse B	Risikoklasse C	Risikoklasse D

S2: Gemischte Anzeige

Die rechtlich relevante Anzeige muss von der rechtlich relevanten Software generiert werden und muss klar von der nicht rechtlich relevanten Anzeige unterscheidbar sein.

Detaillierende Anmerkungen:

1. Die rechtlich relevante Anzeige muss gegen Einflussnahme durch die nicht rechtlich relevante Software geschützt sein, siehe S1.
2. Die rechtlich relevante Software erzeugt die rechtlich relevante Anzeige und darf der nicht rechtlich relevanten Software erst nach Anzeige des Messergebnisses Zugriff auf die Messdaten gewähren.
3. Die rechtlich relevante Anzeige muss so angezeigt werden, dass erkennbar ist, dass es sich um die rechtlich relevante Anzeige handelt.
4. Die rechtlich relevante Anzeige muss ab Beginn der Messung und bis zur Anzeige des Messergebnisses sichtbar sein. Somit kann der Benutzer prüfen, ob die Anzeige die notwendigen Messdaten, z. B. den Stückpreis, enthält. Für weitere Hinweise im Falle der Nutzung eines Betriebssystems siehe O8.

Erforderliche Dokumentation:

- Benennung der Module, die die Anzeige der rechtlich relevanten Messdaten realisieren.
- Beschreibung, wie verhindert wird, dass nicht rechtlich relevante Software Zugriff auf die Messdaten erhält, bevor das Messergebnis angezeigt wird.
- Beschreibung, wie die rechtlich relevante Anzeige von der nicht rechtlich relevanten Anzeige unterscheidbar ist.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- dass die nicht rechtlich relevante Software vor Anzeige der Messdaten keinen Zugriff auf dieselben erhält.

Funktionsprüfungen:

Durch Sichtkontrolle beurteilen, ob rechtlich relevante Anzeigen klar von der nicht rechtlich relevanten Anzeige unterscheidbar sind.

Beispiel einer akzeptablen Lösung:

- Die rechtlich relevante Anzeige wird in einem dedizierten Teil des Displays dargestellt, der von der rechtlich relevanten Software kontrolliert wird. Die für die Anwendung erforderlichen technischen Maßnahmen sind:
  a. Nicht rechtlich relevante Module erhalten keinen Zugriff auf die Messdaten, bis die Messdaten angezeigt worden sind.
  b. Die Anwendung wird periodisch aktualisiert. Das assoziierte Modul überprüft, dass die Anwendung sichtbar ist, solange die Messung nicht abgeschlossen ist. Die Verarbeitung der Messdaten wird abgebrochen, wann immer die Anwendung geschlossen wird oder nicht vollständig sichtbar ist.
- Die rechtlich relevante Anzeige wird in einem Fenster dargestellt, das von der rechtlich relevanten Software kontrolliert wird. Das Fenster befindet sich immer zuoberst. Siehe Anhang O4.

Zusätze für Risikoklasse E

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

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

Auf Basis des Quellcodes ist zu prüfen:

- ob die rechtlich relevante Software die Anzeige der Messdaten erzeugt.
- ob die durchgeführte Umsetzung der gemischten Anzeige korrekt ist.
- ob diese Anzeige von nicht rechtlich relevanten Modulen nicht geändert oder unterdrückt werden kann.

Risikoklasse B	Risikoklasse C	Risikoklasse D

S3: Rückwirkungsfreie Softwareschnittstelle

Die Interaktion und der Datenaustausch zwischen der rechtlich relevanten und der nicht rechtlich relevanten Software muss ausschließlich über eine rückwirkungsfreie Softwareschnittstelle durchgeführt werden, die sich vollständig unter der Kontrolle der rechtlich relevanten Software befindet.

Detaillierende Anmerkungen:

1. Diese Anforderung gilt für alle Arten von Interaktionen und sämtlichen Datenaustausch zwischen der rechtlich relevanten und der nicht rechtlich relevanten Software.
2. Die gesamte Kommunikation muss ausschließlich über die definierte rückwirkungsfreie Softwareschnittstelle ausgeführt werden.
3. Es sind nur Wechselwirkungen und Datenflüsse erlaubt, die den Messprozess und insbesondere die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten nicht unzulässig beeinflussen.
4. Zeitablaufsteuerung und Laufzeit des Messprozesses dürfen nicht von der nicht rechtlich relevanten Software beeinflusst werden.
5. Im Falle einer Softwaretrennung auf einem Betriebssystem, siehe auch O4.
6. Die rückwirkungsfreie Softwareschnittstelle zwischen rechtlich relevanter und nicht rechtlich relevanter Software muss so klein wie möglich sein und darf keine unnötigen Funktionalitäten umfassen. Sie muss vollständig unter der Kontrolle der rechtlich relevanten Software stehen.

Erforderliche Dokumentation: Beschreibung der rückwirkungsfreien Softwareschnittstelle

- Beschreibung der Schnittstelle einschließlich der Beschreibung der erlaubten Wechselwirkungen und Datenflüsse.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob die Funktionen der rechtlich relevanten Software und Aktionen des Messprozesses, die über die rückwirkungsfreie Softwareschnittstelle ausgelöst werden können, definiert und beschrieben sind.
- ob die Daten, die über die rückwirkungsfreie Softwareschnittstelle ausgetauscht werden können, definiert und beschrieben sind.
- Es sind Plausibilitätsprüfungen zur Vollständigkeit der Beschreibung der Wechselwirkungen und des Datenaustauschs durchzuführen.

Beispiel einer akzeptablen Lösung:

- Die nicht rechtlich relevante Software wird in einer Bibliothek zur Berechnung nicht rechtlich relevanter Daten gekapselt. Somit hat die rechtlich relevante Software die volle Kontrolle über alle Interaktionen mit der nicht rechtlich relevanten Software. Jeder Aufruf der rechtlich relevanten Software der Bibliothek inklusive der übermittelten Daten wird dokumentiert. Keine Datenübertragung hat einen unzulässigen Einfluss auf die rechtlich relevante Software.

Zusätze für Risikoklasse E

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

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

Auf Basis des Quellcodes ist zu prüfen:

- ob im Softwareentwurf der Datenfluss in der rechtlich relevanten Software eindeutig definiert ist und überprüft werden kann.
- der Datenfluss über die Softwareschnittstelle (mittels geeigneter Softwarewerkzeuge oder manuell). Es ist zu prüfen, ob der vollständige Datenfluss zwischen den Softwareteilen dokumentiert wurde. Nach unzulässigen Datenflüssen ist zu suchen.
- ob die von nicht rechtlich relevanter Software ausgelösten Wechselwirkungen dokumentiert sind. Nach unzulässigen Wechselwirkungen ist zu suchen.

10 Anhang D: Download von rechtlich relevanter Software

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

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

10.1 Technische Beschreibung

Der Rahmen von Konfigurationen, die grundsätzlich für einen Software-Download geeignet sind, ist groß. Er wird in der folgenden Tabelle beschrieben:

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

Tabelle 10-1: Technische Beschreibung der Konfigurationen für den automatischen Software-Download

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

10.2 Spezifische Softwareanforderungen

Risikoklasse B	Risikoklasse C	Risikoklasse D

D1: Download-Mechanismus

Beide Phasen des Software-Downloads, die Übertragung und die anschließende Installation der Software, müssen automatisch erfolgen und dürfen den Schutz der rechtlich relevanten Software nicht beeinflussen.

Detaillierende Anmerkungen:

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

Erforderliche Dokumentation:

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

Validierungsanleitung:

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

Funktionsprüfungen:

- Durchführen von mindestens einem Software-Download zur Überprüfung seines korrekten Ablaufs.

Beispiel einer akzeptablen Lösung:

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

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

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

Zusätze für Risikoklasse E

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

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

Auf Basis des Quellcodes ist zu prüfen:

- ob die Maßnahmen zur Ausführung des Downloadprozesses angemessen sind.

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">D2: Authentifizierung der übertragenen Software
Es müssen Mittel eingesetzt werden, die sicherstellen, dass die übertragene Software authentisch ist.
Detaillierende Anmerkungen:
1. Bevor die übertragene Software installiert wird, ist zu überprüfen, ob:
a. die Software authentisch ist, d. h., ob sie vom Hersteller des Messgeräts stammt,
b. die Software zum Messgerät gehört, auf dem es installiert werden soll.
2. Ein negatives Prüfergebnis ist als Übertragungsfehler anzusehen und gemäß D1 zu behandeln.</td></tr>
<tr><td colspan="2"></td><td>3. Was Algorithmen und Mindestschlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden.</td></tr>
<tr><td colspan="3">Erforderliche Dokumentation:
Die Dokumentation muss beschreiben, wie die in den detaillierenden Anmerkungen genannten Überprüfungen ausgeführt werden.</td></tr>
<tr><td colspan="3">Validierungsanleitung:
Auf Basis der Dokumentation ist zu prüfen:
• ob die beschriebenen Überprüfungen angemessen sind.
Funktionsprüfungen:
• Überprüfung, dass die Installation nicht authentischer oder nicht zum Gerät gehörender Software gesperrt ist.</td></tr>
<tr><td colspan="3">Beispiel einer akzeptablen Lösung:
1.a Authentizität: Aus Gründen der Integrität (siehe D3) wird eine elektronische Signatur über den Softwareteil erzeugt, der heruntergeladen werden soll. Die Authentizität ist gewährleistet, wenn ein Schlüssel, der im rechtlich relevanten Softwareteil des Geräts gespeichert ist, die Herkunft der elektronischen Signatur vom Hersteller des Geräts bestätigt. Der Abgleich der Signatur erfolgt automatisch. Der Schlüssel kann nur durch Brechen eines Siegels ausgetauscht werden.
1.b Richtige Messgerätebauart: Die Überprüfung der Gerätebauart erfordert den automatischen Abgleich der Gerätebauartidentifikation (in der rechtlich relevanten Software des Gerätes gespeichert) mit einer Kompatibilitätsliste (der Software beigefügt).</td></tr>
</table>

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): *Auf Basis des Quellcodes ist zu prüfen:* • ob Maßnahmen für die Überprüfung der in den detaillierenden Anmerkungen aufgeführten Bedingungen genutzt werden.

<table>
<tr><th>Risikoklasse B</th><th>Risikoklasse C</th><th>Risikoklasse D</th></tr>
<tr><td colspan="3">D3: Schutz der heruntergeladenen Software
Heruntergeladene Software muss gegen absichtliche Änderungen geschützt werden.</td></tr>
<tr><td colspan="3">Detaillierende Anmerkungen:
1. Bevor die übertragene Software installiert wird, ist zu prüfen, ob die Software während der Übertragung unverändert blieb.
2. Ein negatives Prüfergebnis ist als Übertragungsfehler anzusehen und gemäß D1 zu behandeln.</td></tr>
<tr><td colspan="2"></td><td>3. Was Algorithmen und Mindestschlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institutionen, die für die Datensicherheit verantwortlich sind, berücksichtigt werden.</td></tr>
<tr><td colspan="3">Erforderliche Dokumentation:
Die Dokumentation muss beschreiben, wie die Überprüfungen durchgeführt werden.</td></tr>
<tr><td colspan="3">Validierungsanleitung:
Auf Basis der Dokumentation ist zu prüfen:
• ob die beschriebene Überprüfung angemessen ist.
Funktionsprüfungen:
• Überprüfung, ob die Installation von veränderter Software verhindert wird.</td></tr>
<tr><td colspan="2">Beispiel einer akzeptablen Lösung:
• Integrität wird nachgewiesen, indem eine Prüfsumme über die rechtlich relevante Software gebildet und mit der Prüfsumme verglichen wird, die der Software beigefügt ist.
• Akzeptabler Algorithmus: CRC, geheimer Startwert, Länge 32 Bit. Der Startwert ist im rechtlich relevanten Modul gespeichert.</td><td>Beispiel einer akzeptablen Lösung:
• SHA mit RSA wird als ein Signaturalgorithmus verwendet. Der Schlüssel für die Entschlüsselung wird im rechtlich relevanten Softwareteil gespeichert und kann nicht ohne Brechen eines Siegels ausgetauscht werden.</td></tr>
</table>

Zusätze für Risikoklasse E
Erforderliche Dokumentation (zusätzlich zur für Risikoklassen B bis D geforderten Dokumentation): Quellcode der rechtlich relevanten Software.
Validierungsanleitung (zusätzlich zur Anleitung für Risikoklassen B bis D): *Auf Basis des Quellcodes ist zu prüfen:* • ob die Maßnahmen zur Integritätsüberprüfung angemessen sind.

Risikoklasse B	Risikoklasse C	Risikoklasse D

D4: Rückführbarkeit des Downloads rechtlich relevanter Software

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

Detaillierende Anmerkungen:

1. Sämtliche relevanten Daten, die einen Download oder einen Downloadversuch nachvollziehbar machen, müssen aufgezeichnet und geschützt werden. Relevante Daten umfassen Datum und Zeit des Downloads, Identifikator(en) der Software, Herkunft der Übertragung sowie eine Erfolgsnotiz.
2. Die aufgezeichneten Daten müssen für einen angemessenen Zeitraum zur Verfügung stehen (der Zeitraum hängt von Regelungen außerhalb der MID ab).
3. Die aufgezeichneten Daten müssen auf Abruf dargestellt werden.
4. Die Mittel und Aufzeichnungen zur Sicherung der Rückführbarkeit sind Teil der rechtlich relevanten Software und müssen als solche geschützt werden.

Erforderliche Dokumentation:

Die Dokumentation muss beschreiben,

- wie die Mittel zur Rückführbarkeit umgesetzt und geschützt sind,
- welche Struktur die Aufzeichnungen haben,
- wie die aufgezeichneten Daten dargestellt werden können.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob die umgesetzten Mittel zur Sicherung der Rückführbarkeit die in den detaillierenden Anmerkungen aufgeführten Bedingungen erfüllen.

Funktionsprüfungen:

- Überprüfung der Funktionalität dieser Mittel während eines Software-Downloads.

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

Auf Basis der Dokumentation ist zu prüfen:

- ob die genutzten Maßnahmen dem geforderten hohen Schutzniveau gemäß dem Stand der Technik entsprechen.

Beispiel einer akzeptablen Lösung:

- Audit Trail. Das Messgerät ist mit einem Audit Trail ausgestattet, der automatisch zumindest das Datum und den Zeitpunkt des Downloads, den Identifikator der heruntergeladenen rechtlich relevanten Software, den Identifikator der sendenden Stelle und einen Erfolgseintrag aufzeichnet. Für jeden Downloadversuch, unabhängig davon, ob dieser erfolgreich war oder nicht, wird ein Eintrag erzeugt.
- Nachdem die Kapazität des Audit Trails erreicht wurde, wird durch technische Mittel sichergestellt, dass weitere Downloads nicht möglich sind. Der Audit Trail kann nur durch Brechen eines Siegels gelöscht und nur von den Prüfstellen neu gesiegelt werden.

Zusätze für Risikoklasse E

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

Validierungsanleitung (zusätzlich zur Anleitung für Risikoklasse D):

Auf Basis des Quellcodes ist zu prüfen:

- ob die Maßnahmen für die Überwachung des Downloadprozesses angemessen sind.
- ob die Maßnahmen zum Schutz der aufgezeichneten Einträge im Audit Trail angemessen sind.

11 Anhang I: Instrumentenspezifische Softwareanforderungen

Dieser Anhang ist als Zusatz zu den allgemeinen Softwareanforderungen der vorangegangenen Kapitel gedacht und darf nicht getrennt von den Teilen P oder U und den übrigen Anhängen betrachtet werden (siehe Kapitel 2). Er spiegelt die instrumentenspezifischen Anhänge der MID (MI-x) wider und enthält spezifische 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 instrumentenspezifischen 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.

11.1 Struktur

Es gibt verschiedene instrumentenspezifische Softwareaspekte, die für einen bestimmten Messgerätetyp in Betracht gezogen werden können. Diese Aspekte sollten systematisch wie folgt behandelt werden: Jedes instrumentenspezifische Unterkapitel sollte in die folgenden Kategorien unterteilt sein.

11.1.1 Spezifische Vorschriften, Normen und andere normative Dokumente

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

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

11.1.2 Technische Beschreibung

Hier können

- Beispiele für die gebräuchlichsten spezifischen technischen Konfigurationen,
- die Anwendung der Teile P, U und der Anhänge zu diesen Beispielen sowie

- nützliche (instrumentenspezifische) Checklisten sowohl für den Hersteller als auch für den Prüfer

aufgeführt werden. In der Beschreibung sollte erwähnt werden:

- das Messprinzip (kumulierende 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, auf einen Universalrechner gestütztes 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 Netzes, z. B. Ethernet, Token-Ring-LAN, oder Teil eines offenen Netzes, 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 Nutzerschnittstelle 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. interner ROM) oder entfernbar (z. B. Floppy Disk, CD-RW, Smart-Media-Karte, Speicherstick)?
- 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?

11.1.3 Spezifische Softwareanforderungen

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

11.1.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Hier können Beispiele für

- gerätespezifische Parameter (z. B. Individualkonfiguration und Kalibrierparameter eines bestimmten Messgeräts),

- bauartspezifische Parameter (z. B. spezielle Parameter, die bei der Bauartprüfung festgelegt werden) oder
- spezifische, rechtlich relevante Funktionen

aufgeführt werden.

11.1.5 Weitere Aspekte

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

11.1.6 Einstufung in Risikoklassen

Hier sollte die angemessene Risikoklasse für Messgeräte des entsprechenden Typs festgelegt werden. Dies kann

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

11.2 Wasserzähler

11.2.1 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 III (MI-001).

11.2.2 Technische Beschreibung

11.2.2.1 Hardwarekonfiguration

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

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

11.2.2.2 Softwarekonfiguration

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

11.2.2.3 Messprinzip

Wasserzähler kumulieren kontinuierlich das verbrauchte Wasservolumen. Das kumulierte Volumen wird auf dem Messgerät angezeigt. Es werden verschiedene Prinzipien angewendet.

Die Volumenmessung kann normalerweise nicht wiederholt werden.

11.2.2.4 Fehlererkennung und -reaktion

Die Anforderung 7.1.2 des Anhangs III (MI-001) behandelt elektromagnetische Störgrößen. Es ist notwendig, diese Anforderung für softwaregesteuerte Geräte zu interpretieren, da das Entdecken einer Störgröße sowie das Beheben dieser nur durch das Zusammenwirken spezieller Hardwareteile und spezieller Software möglich ist. Aus Softwaresicht macht es keinen Unterschied, was der Grund für eine Störgröße war (elektromagnetisch, elektrisch, mechanisch usw.): die Verfahren zur Wiederaufnahme des Normalbetriebs sind immer gleich.

„Nach der Einwirkung einer elektromagnetischen Störgröße muss der Wasserzähler

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

11.2.3 Spezifische Softwareanforderungen

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

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

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-3: Zusätzliche Funktionalität[3] *Zusätzliche Funktionalität, beispielsweise die Vorauszahlung oder Intervallmessung[4], sollte die rechtlich relevanten Messfunktionen nicht beeinflussen (wie im MID-Anhang III Wasserzähler (MI-001) spezifiziert).*		
Detaillierende Anmerkungen: Zusätzliche Funktionalität ist zugelassen, vorausgesetzt, sie beeinflusst nicht die rechtlich relevanten Messfunktionen, wie im MID-Anhang III Wasserzähler (MI-001) spezifiziert.		
Erforderliche Dokumentation: Siehe S1 bis S3.		
Validierungsanleitung: Siehe S1 bis S3.		
Beispiel einer akzeptablen Lösung: Siehe S1 bis S3.		

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

[3] Der Hersteller sollte immer die nationalen Anforderungen bezüglich der zusätzlichen Funktionalität berücksichtigen.

[4] Bezüglich der Intervallmessung sind zusätzliche Anweisungen im WELMEC-Leitfaden 11.2 enthalten.

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

Risikoklasse B	Risikoklasse C	Risikoklasse D

I1-6: MID-Anhang I, 8.5 Rücksetzen kumulierter Messdaten verhindern

Im Falle von Sichtanzeigen von Messgeräten zur Messung von Versorgungsleistungen dürfen sich die Sichtanzeige der Gesamtliefermenge oder die Sichtanzeigen, aus denen die Gesamtliefermenge abgeleitet werden kann und die ganz oder teilweise als Grundlage für die Abrechnung dienen, während des Betriebs nicht zurücksetzen lassen.

Detaillierende Anmerkungen:

- Kumulative Register eines Messgeräts sind vor dem anwendbaren Konformitätsbewertungsverfahren zurückzusetzen. Während eines Konformitätsbewertungsverfahrens nach Anhang D, F oder H1 müssen die Wasserzähler mit sämtlichen Sicherungs- und Schutzvorrichtungen gemäß TEC versehen werden, wonach eine Rückstellung der kumulierten Messdaten ohne Nachweis eines Eingriffs nicht mehr möglich sein darf.
- Totalisatoren der kumulativen Register eines Messgeräts müssen zurückgesetzt werden, bevor das betreffende Konformitätsbewertungsverfahren beendet ist. Während des Konformitätsbewertungsverfahrens nach Anhang D, F oder H1 müssen die Wasserzähler mit allen Sicherheitsvorrichtungen gemäß TEC ausgestattet sein, die den Nachweis eines Eingriffs in die Zählerregister nach der Rückstellung der kumulierten Messdaten gewährleisten sollen.

Kumulative Register dürfen nicht während der Verwendung im Verteilernetz zurückgesetzt werden.

Hinweis: festgelegt in ISO 4064 unter 6.8.2. - Elektronische Sicherungseinrichtungen

Erforderliche Dokumentation:

Dokumentation der Schutzmaßnahmen gegen das Rücksetzen der Mengenregister.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob das Rücksetzen der kumulierten, rechtlich relevanten Messdaten gesichert ist und ob die vorgesehenen Schutzmaßnahmen den Nachweis eines Eingriffs ermöglichen.

Funktionsprüfungen:

- Bestätigung der korrekten Funktion der vorgesehenen Schutzmaßnahmen, siehe auch P3/U3 und P4/U4.

Beispiel einer akzeptablen Lösung:

Das Register für die gesamte gemessene Menge muss durch eine Hardware-Versiegelung geschützt sein. Andere Register, zum Bespiel Tages- oder Nachttarifregister, dürfen mit denselben Mitteln geschützt werden wie Parameter (siehe P7/U7), vorausgesetzt, dass ein Gesamtregister (insgesamt kumulativ) verfügbar ist, welches durch eine Hardware-Versiegelung geschützt ist. Weitere Einzelheiten sind in den WELMEC-Leitfäden 11.1/13 und in der ISO 4064 Abschnitt 6.8.2. – Elektronische Sicherungseinrichtungen enthalten.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I1-7: MID Anhang I, Artikel 10.5 Ablesen der Messergebnisse *Die Messergebnisse, die als Grundlage für den zu zahlenden Preis dienen, können Ergebnisse verschiedener Register sein, die durch eine Fernbedienung, Uhr oder andere Vorrichtungen aktiviert werden. Jedes Register steht für die Gesamtmenge, die mit einem Tarif im Fakturierungsprozess verbunden ist. Die Ergebnisse sollten mit Hilfe der Nutzerschnittstelle auf verschiedenen Anzeigen periodisch oder auf Anfrage angezeigt werden können.*		
Detaillierende Anmerkungen: • Kumulative Register oder totalisierte Register der Wasserzähler können vor dem anwendbaren Konformitätsbewertungsverfahren zurückgesetzt werden. Während eines Konformitätsbewertungsverfahrens nach Anhang D, F oder H1 müssen die Verbrauchszähler vom Hersteller mit sämtlichen Schutzvorrichtungen gemäß TEC versehen werden, wonach eine Rückstellung der kumulierten Messdaten ohne Nachweis eines Eingriffs nicht mehr möglich sein darf, siehe I1-6. • Wenn der größte Anzeigebereich der Volumentotalisierung erreicht ist, misst der Anzeigebereich weiter beginnend bei null Kubikmeter, siehe auch I1-9 (Anzahl der Ziffernstellen).		
Erforderliche Dokumentation: Dokumentation der Erzielung der Messergebnisse, die als Grundlage für den zu zahlenden Preis dienen.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob die Messergebnisse korrekt gehandhabt werden. *Funktionsprüfungen:* • Bestätigen des korrekten Funktionierens der Handhabung der Messergebnisse.		
Beispiel einer akzeptablen Lösung: Wenn ein Zähler für die Zählung der Mengen in verschiedenen Registern gemäß MID (MI-001) ausgelegt ist, muss der Zähler die Gesamtmengen jedes Registers auf der Anzeige mit Hilfe der Nutzerschnittstelle (siehe P3/U3, z. B.: Tasten auf Geräten) sowie das derzeit aktive Tarifregister darstellen können. Die Ergebnisse dürfen periodisch oder auf Anfrage mit Hilfe der Nutzerschnittstelle auf verschiedenen Anzeigen dargestellt werden. Bei der Anzeige verschiedener Messergebnisse muss jedoch klar sein, welche Anzeige zu welchem Register gehört; es darf diesbezüglich keine Unklarheiten geben. Falls notwendig, können zusätzliche Beschriftungen auf dem Wasserzähler angebracht werden, die die verschiedenen Register oder die Anzeige des Testmodus benennen (siehe I1-9).		

Risikoklasse B	Risikoklasse C	Risikoklasse D

I1-8: Schutz gegen absichtliche Änderungen bei Wasserzählern vom Typ P (mit mechanischem Register)

Die berechnete Prüfsumme oder eine Alternativanzeige, um das Entdecken von Softwaremodifikationen zu unterstützen, ist auf Befehl für Kontrollzwecke sichtbar zu machen, siehe P6. Für Wasserzähler des Typs P mit mechanischem Zähler wäre als Ausnahme ein Aufprägen der Prüfsumme oder einer Alternativanzeige der Softwaremodifikation auf das Typenschild eines Messgeräts eine akzeptable Lösung, wenn die folgenden Bedingungen A, B und C erfüllt sind:

A Die Nutzerschnittstelle hat keinerlei Steuerungsfähigkeiten, um das Anzeigen des Werts der Prüfsumme oder einer alternativen Anzeige der Softwaremodifikation auf dem Display zu aktivieren, oder das Display gestattet die Anzeige dieser Werte aus technischen Gründen nicht (mechanischer Zähler).

B. Das Messgerät hat keine Schnittstelle, um den Software-Identifikator zu übermitteln.

C. Nach der Fertigung eines Zählers ist eine Änderung der Software nicht mehr möglich oder nur dann möglich, wenn auch die Hardware oder eine Hardwarekomponente, die die Software enthält, geändert wird.

Detaillierende Anmerkungen:

- Der Hersteller der Hardware bzw. der entsprechenden Hardwarekomponente ist dafür verantwortlich, dass die Prüfsumme oder eine alternative Anzeige der Softwaremodifikation ordnungsgemäß auf der betroffenen Hardware angegeben ist.
- Es gelten alle anderen detaillierenden Anmerkungen von P6.

Erforderliche Dokumentation:

Gemäß P6.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- Gemäß P6.

Funktionsprüfungen:

- Gemäß P6.

Beispiel einer akzeptablen Lösung:

Aufprägen der Prüfsumme oder einer alternativen Anzeige der Softwaremodifikation auf das Typenschild des Messgeräts.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I1-9: Anzahl der Ziffernstellen

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

Dauerdurchfluss Q3 [m^3/h]	*Mindestanzeigebereich [m^3]*
Q3 ≤ 6,3	*9 999*
6,3 < Q3 ≤ 63	*99 999*
63 < Q3 ≤ 630	*999 999*
630 < Q3 ≤ 6300	*9 999 999*

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

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

Eignung gemäß Absatz 7.6 und 10.5 von Anhang I der Richtlinie 2014/32/EU (MID):
Ein Messgerät ist so auszulegen, dass die Messvorgänge kontrolliert werden können, nachdem das Messgerät in Verkehr gebracht und in Betrieb genommen wurde. Erforderlichenfalls muss das Messgerät eine spezielle Ausrüstung oder Software für diese Kontrolle besitzen.
Darüber hinaus muss ein Messgerät, das fernabgelesen werden kann, auf jeden Fall mit einer der messtechnischen Kontrolle unterliegenden Sichtanzeige ausgestattet werden, die für den Verbraucher ohne Hilfsmittel zugänglich ist.
Wenn der maximale Anzeigebereich der Mengentotalisierung erreicht ist, misst der Anzeigebereich weiter beginnend bei null Kubikmeter.

Detaillierende Anmerkungen:

Gemäß ISO 4064 Teil 1:

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

Erforderliche Dokumentation:

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

Validierungsanleitung:

Funktionsprüfungen:

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

Beispiel einer akzeptablen Lösung:

Auf der Anzeige des Wasserzählers gibt es genügend Ziffernstellen, die sowohl die Anforderungen an die Gesamtmenge als auch die erforderliche Auflösung erfüllen.

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

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

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

Anmerkung: Es steht nicht im Einklang mit den wesentlichen Anforderungen der Richtlinie 2014/32/EU

(MID) gemäß Artikel 7.6, Anhang I, dass eine Eichbehörde, Prüfbehörde oder Benannte Stelle beim Hersteller nach speziellen Prüfeinrichtungen oder Software nachfragen muss.

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

11.2.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Der Zugang zu Mitteln für die Modifizierung der Software, der Einstellungen und/oder der Parameter, die die Bestimmung der Messergebnisse beeinflussen, muss gesichert werden[5].

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

11.2.5 Einstufung in Risikoklassen

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

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

[5] Bezüglich der Sicherung eines Wasserzählers werden im WELMEC-Leitfaden 13.3 zusätzliche Anleitungen gegeben.

11.3 Gaszähler und Mengenumwerter

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

Die spezifischen Anforderungen des vorliegenden Kapitels beruhen auf der MID, Anhang IV Gaszähler und Mengenumwerter (MI-002).
Eine Anleitung zur Sicherung von Gaszählern und Mengenumwertern ist auch im WELMEC-Leitfaden 11.3 enthalten.
Eine spezielle Anleitung bezüglich der Gaschromatographen, die als Live-Sensor an ein EVCD angeschlossen sind, sind in WELMEC-Leitfaden 11.1 enthalten.
Eine zusätzliche Anleitung oder Aktualisierungen von Anleitungen für Gaszähler und Mengenumwerter sind der WELMEC-Webseite zu entnehmen.
Die nationale Gesetzgebung bezüglich zusätzlicher Funktionalität, OIML-Empfehlungen, harmonisierte (EN) Normen und (IEC) Normen wurden nicht berücksichtigt.

11.3.2 Technische Beschreibung

11.3.2.1 Hardwarekonfiguration

Gaszähler und Mengenumwerter sind normalerweise getrennte Hardwarekomponenten.
Anzeigen oder Recheneinheiten von Gaszählern und Mengenumwertern können eine oder mehrere Schnittstellen haben, um externe Sensoreinheiten zu verbinden.
Falls ein Gaschromatograph als Live-Sensor mit einem EVCD verbunden ist, beeinflusst der Gaschromatograph das Messergebnis (Basisvolumen) des EVCD und sollte daher Teil des Konformitätsbewertungsverfahrens sein.

11.3.2.2 Softwarekonfiguration

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

11.3.2.3 Messprinzip

Gaszähler kumulieren kontinuierlich die Werte der verbrauchten Menge oder der Masse, die durch den Zähler fließt. Ein Mengenumwerter kann verwendet werden, um die Menge im Grundzustand zu berechnen.
Die Mengenmessung ist nicht wiederholbar.

11.3.2.4 Fehlererkennung und -reaktion

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

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

Siehe 3.1.2 der MID, Anhang IV Gaszähler und Mengenumwerter (MI-002).

- Ein elektronischer Mengenumwerter muss feststellen können, wenn er außerhalb des bzw. der Betriebsbereiche arbeitet, deren Parameter vom Hersteller als für die Messgenauigkeit maßgeblich angegeben wurden. In diesem Fall muss der Mengenumwerter das Integrieren der umgerechneten Menge unterbrechen, und die umgerechnete Menge kann für die Zeit des Betriebs außerhalb des bzw. der Betriebsbereiche gesondert summiert werden.
  Siehe 9.1 der MID, Anhang IV Gaszähler und Mengenumwerter (MI-002).

11.3.3 Spezifische Softwareanforderungen

11.3.3.1 Gaszähler und Mengenumwerter

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

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-2: Nicht rechtlich relevante Software und dynamisches Verhalten *Die nicht rechtlich relevante Software darf das dynamische Verhalten eines Messprozesses nicht unzulässig beeinflussen.*		
Detaillierende Anmerkungen: Diese Anforderung stellt sicher, dass das dynamische Verhalten der rechtlich relevanten Software bei Echtzeitanwendungen von Zählern nicht in unzulässiger Weise durch nicht rechtlich relevante Software beeinflusst wird, d. h., dass die Ressourcen der rechtlich relevanten Software nicht in unzulässiger Weise vom nicht rechtlich relevanten Teil gemindert werden.		
Erforderliche Dokumentation: • Beschreibung der Interrupt-Hierarchie. • Zeitdiagramm der Softwareaufgaben. Grenzen der anteiligen Laufzeit der nicht rechtlich relevanten Aufgaben.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob die Dokumentation der Grenzen der anteiligen Laufzeit der nicht rechtlich relevanten Aufgaben dem Programmierer des nicht rechtlich relevanten Softwareteils zur Verfügung steht. *Funktionsprüfungen:* • Bestätigen der korrekten Funktion bei Vorhandensein definierter Einflussgrößen und provozierter Fehler.		
Beispiel einer akzeptablen Lösung: Die Interrupt-Hierarchie ist so entworfen, dass nachteilige Einflüsse vermieden werden.		

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

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-4: Zusätzliche Funktionalität[6] *Zusätzliche Funktionalität, beispielsweise die Vorauszahlung oder Intervallmessung[7], sollte die rechtlich relevanten Messfunktionen nicht beeinflussen (wie in MID Anhang IV Gaszähler und Mengenumwerter (MI-002) spezifiziert).*		
Detaillierende Anmerkungen: • Zusätzliche Funktionalität ist zugelassen, vorausgesetzt, sie beeinflusst nicht die rechtlich relevanten Messfunktionen, wie in der MID, Anhang IV Gaszähler und Mengenumwerter (MI-002) angegeben.		
Erforderliche Dokumentation: Siehe S1 bis S3.		
Validierungsanleitung: Siehe S1 bis S3.		
Beispiel einer akzeptablen Lösung: Siehe S1 bis S3.		

[6] Der Hersteller sollte immer die nationalen Anforderungen bezüglich der zusätzlichen Funktionalität berücksichtigen.

[7] Bezüglich der Intervallmessung sind zusätzliche Anweisungen im WELMEC-Leitfaden 11.2 enthalten.

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

Risikoklasse B	Risikoklasse C	Risikoklasse D

I2-6: MID-Anhang I, 8.5 (Rücksetzen kumulierter Messdaten 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 eine Grundlage für die Bezahlung ist, nicht möglich sein.

Detaillierende Anmerkungen:

Während eines Konformitätsbewertungsverfahrens nach Anhang D, F oder H1 müssen die Verbrauchszähler vom Hersteller mit sämtlichen Sicherungs- und Schutzvorrichtungen gemäß TEC versehen werden, wonach eine Rückstellung der kumulierten Messdaten ohne Nachweis eines Eingriffs nicht mehr möglich sein darf.

Bei Gaszählern muss das Register für die gesamte gemessene Menge durch eine metrologische Hardware-Versiegelung geschützt sein.

Bei Mengenumwertern muss die Menge im Normzustand durch eine metrologische Hardware-Versiegelung geschützt sein.

Erforderliche Dokumentation:
Dokumentation der Schutzmaßnahmen gegen das Rücksetzen der Mengenregister.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob das Rücksetzen der kumulierten, rechtlich relevanten Messwerte gesichert ist und ob die vorgesehenen Schutzmaßnahmen den Nachweis eines Eingriffs ermöglichen.

Funktionsprüfungen:

- Bestätigung der korrekten Funktion der vorgesehenen Schutzmaßnahmen.

Beispiel einer akzeptablen Lösung:
Bei Gaszählern muss das Register für die gemessene Gesamtmenge durch metrologische Hardware-Versiegelungen geschützt sein. Andere Register, zum Bespiel Tages- oder Nachttarifregister, dürfen mit denselben Mitteln geschützt werden wie Parameter (siehe P7/U7), vorausgesetzt, dass ein Gesamtregister (insgesamt kumulativ) verfügbar ist, welches durch eine Hardware-Versiegelung geschützt ist. Zusätzliche Anweisungen sind in den WELMEC-Leitfäden 11.1 und 11.3 enthalten.
Bei Mengenumwertern muss die Menge im Normzustand durch metrologische Hardware-Versiegelungen geschützt sein. Die Register, die die Menge bei Messbedingungen zeigen, können auch mit denselben Mitteln wie Parameter geschützt werden (siehe P7/U7).
Hinweis: Die Menge bei Messbedingungen kann mit der Anzeige des angeschlossenen Gaszählers synchronisiert werden. Je nach nationaler Gesetzgebung müssen zusätzliche Maßnahmen ergriffen werden, z. B. Nacheichungen.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I2-7: MID Anhang I, 10.5 Ablesen der Messergebnisse

A. Die Messergebnisse, die als Grundlage für den zu zahlenden Preis dienen, können Ergebnisse verschiedener Register sein, die durch eine Fernbedienung, Uhr oder andere Vorrichtungen aktiviert werden. Jedes Register steht für die Gesamtmenge, die mit einem Tarif im Abrechnungsprozess verbunden ist. Der Zähler sollte die Ergebnisse jedes Registers mit Hilfe der Nutzerschnittstelle periodisch oder auf Anfrage darstellen.

Detaillierende Anmerkungen:

Kumulative Register eines Messgeräts können vor dem anwendbaren Konformitätsbewertungsverfahren zurückgesetzt werden. Während eines Konformitätsbewertungsverfahrens nach Anhang D, F oder H1 müssen die Verbrauchszähler vom Hersteller mit sämtlichen Schutzvorrichtungen gemäß TEC versehen werden, wonach eine Rückstellung der kumulierten Messdaten ohne Nachweis eines Eingriffs nicht mehr möglich sein darf.

Erforderliche Dokumentation:

Dokumentation der Erzielung der Messergebnisse, die als Grundlage für den zu zahlenden Preis dienen.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob die Messergebnisse korrekt gehandhabt werden.

Funktionsprüfungen:

- Bestätigen des korrekten Funktionierens der Handhabung der Messergebnisse.

Beispiel einer akzeptablen Lösung:

Wenn ein Zähler für die Zählung der Mengen gemäß MID, Anhang IV Gaszähler und Mengenumwerter (MI-002) in verschiedenen Registern ausgelegt ist, muss der Zähler die Gesamtmengen jedes Registers auf der Anzeige mit Hilfe der Nutzerschnittstelle (siehe dieser Leitfaden, z. B.: Tasten auf dem Gerät) sowie das derzeit aktive Tarifregister darstellen können. Eine akzeptable Lösung ist ebenfalls, die Ergebnisse mit Hilfe der Nutzerschnittstelle periodisch oder auf Anfrage auf verschiedenen Anzeigen darzustellen. Bei der Anzeige verschiedener Messergebnisse muss jedoch klar sein, welche Anzeige zu welchem Register gehört; es darf diesbezüglich keine Unklarheiten geben.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I2-8: Schutz gegen absichtliche Änderungen bei Gaszählern vom Typ P mit einem mechanischen Register

Die berechnete Prüfsumme oder eine Alternativanzeige, um das Entdecken von Softwaremodifikationen zu unterstützen, ist auf Befehl für Kontrollzwecke sichtbar zu machen, siehe P6, Risikoklasse C.

Für Gaszähler und Mengenumwerter vom Typ P mit einem mechanischen Zähler wäre als Ausnahme ein Aufprägen der Prüfsumme oder einer Alternativanzeige der Softwaremodifikation auf das Typenschild eines Messgeräts eine akzeptable Lösung, wenn die folgenden Bedingungen A, B und C erfüllt sind:

A Die Nutzerschnittstelle hat keinerlei Steuerungsfähigkeiten, um das Anzeigen des Werts der Prüfsumme oder einer alternativen Anzeige der Softwaremodifikation auf dem Display zu aktivieren, oder das Display gestattet die Anzeige Software-Identifikators aus technischen Gründen nicht (mechanischer Zähler).

B. *Das Messgerät hat keine Schnittstelle, um den Software-Identifikator zu übermitteln.*

C. Nach der Fertigung eines Zählers ist eine Änderung der Software nicht mehr möglich oder nur dann möglich, wenn auch die Hardware oder eine Hardwarekomponente, die die Software enthält, geändert wird.

Detaillierende Anmerkungen:

- Der Hersteller ist dafür verantwortlich, dass die Prüfsumme oder eine Alternativanzeige der Softwaremodifikation ordnungsgemäß auf der betroffenen Hardware angegeben ist.
- Es gelten alle anderen detaillierenden Anmerkungen von P6.

Erforderliche Dokumentation:

Gemäß P6.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- Gemäß P6.

Funktionsprüfungen:

- Gemäß P6.

Beispiel einer akzeptablen Lösung:

Aufprägen der Prüfsumme oder einer alternativen Anzeige der Softwaremodifikation auf das Typenschild des Messgeräts.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-9: MID, Anhang IV Gaszähler und Mengenumwerter (MI-002), 5.3 Anzahl der Ziffernstellen (Gaszähler und elektronische Mengenumwerter) *Die Anzeige der gesamten Menge muss über eine ausreichende Zahl von Ziffernstellen verfügen, um sicherzustellen, dass sie bei 8000 Stunden Zählerbetrieb bei Q_{max} nicht auf ihren Ursprungswert zurückkehrt.*		
Detaillierende Anmerkungen:		
Erforderliche Dokumentation: Dokumentation der internen Darstellung des Registers.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob es eine ausreichende Anzahl von Ziffern gibt, damit der Index nicht auf seinen anfänglichen Wert übergeht, wenn das Volumen, das bei Q_{max} innerhalb von 8000h fließt, durchgeflossen ist.		
Beispiel einer akzeptablen Lösung: Typische Werte für Hausgaszähler sind: Q_{max} = 6 m³/h. Der erforderliche Bereich beträgt 48.000 m³ und benötigt 5 Ziffernstellen, um dargestellt zu werden (derzeit zeigen mechanische und elektronische Gaszähler bis zu 99.999 m³ an, was für diese Gerätegröße mehr als ausreichend ist).		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-10: MID, Anhang IV Gaszähler und Mengenumwerter (MI-002), 5.2 Lebensdauer der Energiequelle *Eine gerätespezifische Stromquelle muss eine Lebensdauer von mindestens fünf Jahren aufweisen. Nach Ablauf von 90 % dieser Lebensdauer muss ein entsprechender Warnhinweis erscheinen.*		
Detaillierende Anmerkungen: Lebensdauer wird hier im Sinne von verfügbarer Energiekapazität verwendet. Wenn die Energiequelle vor Ort ausgetauscht werden kann, dürfen die Parameter und Messdaten während des Wechsels nicht beschädigt werden. Zusätzliche Warnungen sind erlaubt, bevor die Schwelle von 90 % erreicht ist, vorausgesetzt, diese Warnungen sind nicht verwirrend.		
Erforderliche Dokumentation: Dokumentation der Kapazität der Energiequelle, der Höchstlebensdauer (unabhängig vom Energieverbrauch), der Maßnahmen zur Bestimmung der verbrauchten oder verfügbaren Energie, Beschreibung der Mittel zur Warnung bei wenig verfügbarer Energie und beim Austauschvorgang der Batterie.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob die Maßnahmen zur Überwachung der verfügbaren Energie angemessen sind.		
Beispiel einer akzeptablen Lösung: Die Betriebsstunden oder die Wake-Up-Signale des Geräts werden gezählt, in einem nichtflüchtigen Speicher gespeichert und mit dem Nennwert der Batterielebensdauer verglichen. Sind 90 % der Lebensdauer aufgebraucht, wird eine geeignete Warnung angezeigt. Die Software erkennt den Austausch der Energiequelle und setzt den Zähler zurück. Eine weitere Lösung wäre die ständige Überwachung des Zustands der Energieversorgung. Eine sichtbare Warnung wird als angemessen angesehen, z. B. eine Botschaft auf der Anzeige oder eine Warnanzeige. Zusätzlich kann eine elektronische Schnittstelle dem Netz-/Gerätebetreiber die Warnung zur Verfügung stellen. Eine versteckte "stille" Warnung (über die elektronische Schnittstelle) allein an den Netz-/Gerätebetreiber ist keine ausreichende Lösung.		

11.3.3.2 Gaszähler

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-11: MID, Anhang IV Gaszähler und Mengenumwerter (MI-002), 5.5 Prüfelement des Gaszählers *Der Gaszähler muss mit einer Prüfvorrichtung ausgestattet sein, die eine Durchführung von Prüfungen in einem angemessenen Zeitrahmen ermöglicht.*		
Detaillierende Anmerkungen: Das Prüfelement zur Beschleunigung zeitaufwendiger Prüfverfahren wird normalerweise für die Prüfung vor Installation und Normalbetrieb verwendet. Während des Testbetriebs müssen dieselben Register und Softwareteile verwendet werden wie während des Standardbetriebsmodus.		
Erforderliche Dokumentation: Dokumentation des Prüfelements und der Anweisungen für die Aktivierung des Prüfmodus.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob alle zeitaufwendigen Prüfverfahren des Gaszählers mit Hilfe des Prüfelements ausgeführt werden können.		
Beispiel einer akzeptablen Lösung: Für Testzwecke muss die Erhöhung des Testelements oder des Impulses mindestens alle 60 Sekunden bei Q_{min}, siehe WELMEC-Leitfaden 11.1, Paragraf 2.4.4 erfolgen. Die Zeitbasis der internen Uhr kann beschleunigt werden. Prozesse, die z. B. eine Woche, einen Monat oder sogar ein Jahr dauern, und Registerüberlauf können im Prüfmodus innerhalb einer Zeitspanne von Minuten oder Stunden geprüft werden.		

11.3.3.3 Elektronischer Mengenumwerter

Risikoklasse B	Risikoklasse C	Risikoklasse D
I2-12: MID, Anhang IV Gaszähler und Mengenumwerter (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 spezifischen Messfeldes arbeitet. In diesem Fall muss der Mengenumwerter das Integrieren der umgerechneten Menge unterbrechen und die umgerechnete Menge kann für die Zeit des Betriebs außerhalb des bzw. der Betriebsbereiche gesondert aufsummiert werden.*		
Detaillierende Anmerkungen: Der Fehlerzustand muss angezeigt werden.		
Erforderliche Dokumentation: Dokumentation der verschiedenen Register für umgewandelte Menge und Ausfallmenge.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen,* • ob die Maßnahmen für den Umgang mit ungewöhnlichen Betriebszuständen angemessen 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 Zeitraums außerhalb des zulässigen Bereichs in einem Audit Trail zu speichern (siehe P7). Beide Größen können angezeigt werden. Der Nutzer kann mittels einer Zustandsanzeige eindeutig zwischen der regulären und der Ausfallanzeige unterscheiden.		

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

11.3.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Der Zugang zu Mitteln für die Modifizierung der rechtlich relevanten Software, der Einstellungen und/oder Parameter, die die Bestimmung der Ergebnisse für die Messungen beeinflussen, muss gesichert werden[8].
Zum Beispiel aber nicht ausschließlich bei Gaszählern:

Parameter	***Geschützt***	***Einstellbar***	***Anmerkung***
Kalibrierfaktor	***X***		
Linearisierungsfaktor	***X***		
Rechtlich relevante Konfiguration der Register	***X***		
Einstellungen von zum Beispiel: • ***Korrekturgeräten*** • ***Kurvenanpassung*** • ***Pulszahl*** • ***Mindestdurchfluss abgeschaltet*** • ***Ultraschall-Sensor*** • ***Geometrie der Umformer in Ultraschall-Gaszählern***	***X***		
Sonstige relevante Parameter, die das Messergebnis beeinflussen könnten	***X***		
Software-Download des rechtlich relevanten Softwareteils	***X***		

Zum Beispiel aber nicht ausschließlich bei Mengenumwertern:

Parameter	***Geschützt***	***Einstellbar***	***Anmerkung***
Kalibrierfaktor	***X***		
Linearisierungsfaktor	***X***		
Rechtlich relevante Konfiguration der Register	***X***		
Einstellungen von zum Beispiel: • ***Rechtlich relevanten Parametern einer Korrektureinrichtung, wie Parameter, die auf der Fehlerkurve eines Gaszählers beruhen*** • ***Pulswert eines Gaszählers*** • ***Gaszusammensetzung und Parameter für die Kompressibilitätsberechnung***	***X***		

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

Sonstige relevante Parameter, die das Messergebnis beeinflussen könnten	***x***		
Software-Download der rechtlich relevanten Software	***x***		

11.3.5 Einstufung in Risikoklassen

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

– **Risikoklasse C für Messgeräte vom Typ P und U.**

11.4 Elektrizitätszähler für Wirkverbrauch

11.4.1 Spezifische Vorschriften, Normen und andere normative Dokumente

Die spezifischen Anforderungen des vorliegenden Kapitels beruhen auf der MID, Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003).
Eine Anleitung zur Sicherung von Elektrizitätszählern für Wirkverbrauch ist auch im WELMEC-Leitfaden 11.3 enthalten.
Eine zusätzliche Anleitung oder Updates für Elektrizitätszähler für Wirkverbrauch sind der WELMEC-Webseite zu entnehmen.
Die nationale Gesetzgebung bezüglich zusätzlicher Funktionalität, OIML-Empfehlungen, harmonisierte (EN) Normen und (IEC) Normen wurden nicht berücksichtigt.

11.4.2 Technische Beschreibung

11.4.2.1 Hardwarekonfiguration

Elektrizitätszähler für Wirkverbrauch nehmen Spannungs- und Strommessungen als Eingänge, leiten daraus die elektrische Wirkleistung ab und integrieren diese über die Zeit, um die verbrauchte Energie zu ermitteln.

Elektrizitätszähler für Wirkverbrauch können zusammen mit externen Messwandlern betrieben werden.

11.4.2.2 Softwarekonfiguration

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

11.4.2.3 Messprinzip

Elektrizitätszähler für Wirkverbrauch kumulieren kontinuierlich die Mengenwerte der in einem Stromkreis verbrauchten Energie. Der kumulierte konsumierte Energiewert wird vom Gerät angezeigt.
Die Messung ist nicht wiederholbar.

11.4.2.4 Fehlererkennung und -reaktion

Die Anforderung in der MID, Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003), Artikel 4.3.1, beschäftigen sich mit der zulässigen Auswirkung von Störgrößen. Aus Softwaresicht macht es keinen Unterschied, was der Grund für eine Störgröße war (elektromagnetisch, elektrisch, mechanisch usw.): die Verfahren zur Wiederaufnahme des Normalbetriebs sind immer gleich.

- Nach der Einwirkung einer Störgröße:
  - muss der Betrieb des Elektrizitätszählers innerhalb der Fehlergrenzen wiederhergestellt werden,
  - muss die Durchführbarkeit sämtlicher Messfunktionen gewährleistet sein,
  - muss eine Wiederherstellung aller vor dem Einwirken der Störgröße vorhandenen Messdaten möglich sein,
  - darf die Änderung der gemessenen Energie den Grenzwert nicht überschreiten.

11.4.3 Spezifische Softwareanforderungen

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

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-2: Nicht rechtlich relevante Software und dynamisches Verhalten *Die nicht rechtlich relevante Software darf das dynamische Verhalten eines Messprozesses nicht unzulässig beeinflussen.*		
Detaillierende Anmerkungen: Diese Anforderung stellt sicher, dass das dynamische Verhalten der rechtlich relevanten Software bei Echtzeitanwendungen von Zählern nicht in unzulässiger Weise durch nicht rechtlich relevante Software beeinflusst wird, d. h., dass die Ressourcen der rechtlich relevanten Software nicht in unzulässiger Weise vom nicht rechtlich relevanten Teil gemindert werden.		
Erforderliche Dokumentation: • Beschreibung der Interrupt-Hierarchie. • Zeitdiagramm der Softwareaufgaben. Grenzen der anteiligen Laufzeit der nicht rechtlich relevanten Aufgaben.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob die Dokumentation der Grenzen der anteiligen Laufzeit der nicht rechtlich relevanten Aufgaben dem Programmierer des nicht rechtlich relevanten Softwareteils zur Verfügung steht. *Funktionsprüfungen:* • Bestätigen der korrekten Funktion bei Vorhandensein definierter Einflussgrößen und provozierter Fehler.		
Beispiel einer akzeptablen Lösung: Die Interrupt-Hierarchie ist so entworfen, dass nachteilige Einflüsse vermieden werden.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-3: Zusätzliche Funktionalität[9] *Die zusätzliche Funktionalität, beispielsweise die Vorauszahlung oder Intervallmessung[10], sollte die rechtlich relevanten Messfunktionen nicht beeinflussen (wie im MID Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003) spezifiziert).*		
Detaillierende Anmerkungen: • Zusätzliche Funktionalität ist zugelassen, solange sie nicht die in der MID, Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003) angegebenen rechtlich relevanten Messfunktionen beeinflusst.		
Erforderliche Dokumentation: Siehe S1 bis S3.		
Validierungsanleitung: Siehe S1 bis S3.		
Beispiel einer akzeptablen Lösung: Siehe S1 bis S3.		

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

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

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

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

Risikoklasse B	Risikoklasse C	Risikoklasse D

I3-7: MID-Annex I, 10.5 Ablesen der Messergebnisse

Die Messergebnisse, die als Grundlage für den zu zahlenden Preis dienen, können Ergebnisse verschiedener Register sein, die durch eine Fernbedienung, Uhr oder andere Vorrichtungen aktiviert werden. Jedes Register steht für die Gesamtmenge, die mit einem Tarif im Fakturierungsprozess verbunden ist. Die Ergebnisse müssen auf verschiedenen Anzeigen periodisch oder auf Anfrage mit Hilfe der Nutzerschnittstelle dargestellt werden können.

Detaillierende Anmerkungen:

Kumulative Register eines Messgeräts können vor dem anwendbaren Konformitätsbewertungsverfahren zurückgesetzt werden. Während eines Konformitätsbewertungsverfahrens nach Anhang D, F oder H1 müssen die Verbrauchszähler vom Hersteller mit sämtlichen Sicherungs- und Schutzmaßnahmen gemäß TEC versehen werden, wonach eine Rückstellung der kumulierten Messdaten ohne Nachweis eines Eingriffs nicht mehr möglich sein darf.

Erforderliche Dokumentation:

Dokumentation der Erzielung der Messergebnisse, die als Grundlage für den zu zahlenden Preis dienen.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob die Messergebnisse korrekt gehandhabt werden.

Funktionsprüfungen:

- Bestätigen des korrekten Funktionierens der Handhabung der Messergebnisse.

Beispiel einer akzeptablen Lösung:

Wenn ein Zähler für die Zählung der Mengen, die in MID, Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003) definiert sind, in verschiedenen Registern ausgelegt ist, muss (a) der Zähler die Gesamtmengen jedes Registers auf der Anzeige mit Hilfe der Nutzerschnittstelle (siehe dieser Leitfaden, z. B.: Tasten auf dem Gerät) sowie die derzeit aktiven Tarifregister darstellen können. Die Ergebnisse dürfen mit Hilfe der Nutzerschnittstelle periodisch oder auf Anfrage auf verschiedenen Anzeigen dargestellt werden. Bei der Anzeige verschiedener Messergebnisse muss jedoch klar sein, welche Anzeige zu welchem Register gehört; es darf diesbezüglich keine Unklarheiten geben.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I3-8: Schutz gegen absichtliche Änderungen bei Elektrizitätszählern für Wirkverbrauch vom Typ P mit einem mechanischen Register

Die berechnete Prüfsumme oder eine Alternativanzeige, um den Nachweis der Softwaremodifikation zu unterstützen, ist auf Befehl für Kontrollzwecke sichtbar zu machen, siehe P6. Für Elektrizitätszähler für Wirkverbrauch vom Typ P mit einem mechanischen Zähler wäre als Ausnahme ein Aufprägen der Prüfsumme oder eine Alternativanzeige der Softwaremodifikation auf das Typenschild eines Messgeräts eine akzeptable Lösung, wenn die folgenden Bedingungen A, B und C erfüllt sind:

A Die Nutzerschnittstelle hat keinerlei Steuerungsfähigkeiten, um den Wert der Prüfsumme oder eine alternative Anzeige der Softwaremodifikation auf dem Display zu aktivieren, oder das Display gestattet die Anzeige dieser Werte aus technischen Gründen nicht (mechanischer Zähler).

B. *Das Messgerät hat keine Schnittstelle, um den Software-Identifikator zu übermitteln.*

C. Nach der Fertigung eines Zählers ist eine Änderung der Software nicht mehr möglich oder nur dann möglich, wenn auch die Hardware oder eine Hardwarekomponente, die die Software enthält, geändert wird.

Detaillierende Anmerkungen:

- Der Hersteller ist dafür verantwortlich, dass die Prüfsumme oder eine Alternativanzeige der Softwaremodifikationen ordnungsgemäß auf der betroffenen Hardware angegeben ist.
- Es gelten alle anderen detaillierenden Anmerkungen von P6.

Erforderliche Dokumentation:

Gemäß P6.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- Gemäß P6.

Funktionsprüfungen:

- Gemäß P6.

Beispiel einer akzeptablen Lösung:

Aufprägen der Prüfsumme oder einer alternativen Anzeige der Softwaremodifikation auf das Typenschild des Messgeräts.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I3-9: MID, Anhang V Elektrizitätszähler für Wirkverbrauch (MI-003), 5.2 Anzahl der Ziffernstellen Die Anzeige der Gesamtmenge muss über eine ausreichende Zahl an Ziffernstellen verfügen, damit sichergestellt ist, dass die Anzeige bei 4 000 Stunden Volllastbetrieb (I = I max , U = U n und PF = 1) nicht auf den Ausgangswert zurückspringt.		
Detaillierende Anmerkungen:		
Erforderliche Dokumentation: Dokumentation der internen Darstellung des Energieregisters und der Hilfsgrößen.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob die Anzahl der Ziffernstellen ausreichend ist (intern und auf der Anzeige).		
Beispiel einer akzeptablen Lösung: Typische Werte für Dreiphasen-Stromzähler sind: E_{max} (4000h) = 3*60A * 230V * 4000h / 1000 = 165600 kWh. Dies erfordert eine Darstellung von mindestens 6 Ziffern.		

11.4.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Der Zugang zu Mitteln für die Modifizierung der Software, der Einstellungen und/oder Parameter, die die Bestimmung der Messergebnisse beeinflussen, muss gesichert werden[11].

Parameter	***Geschützt***	***Einstellbar***	***Anmerkung***
Kalibrierfaktor	***x***		
Linearisierungsfaktor	***x***		
Rechtlich relevante Konfiguration der Register	***x***		
Einstellungen von zum Beispiel: • ***rechtlich relevanten Parametern einer Korrektureinrichtung, z. B. Parameter, die auf der Fehlerkurve eines Elektrizitätszählers für Wirkverbrauch beruhen*** • ***Stromwandlerverhältnis***	***x***		
Sonstige relevante Parameter, die das Messergebnis beeinflussen könnten	***x***		
Software-Download der rechtlich relevanten Software	***x***		

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

11.4.5 Einstufung in Risikoklassen

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

– Risikoklasse C für Messgeräte vom Typ P und U.

11.5 Wärmezähler

11.5.1 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 VI (MI-004) der MID.

11.5.2 Technische Beschreibung

11.5.2.1 Hardwarekonfiguration

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

11.5.2.2 Softwarekonfiguration

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

11.5.2.3 Messprinzip

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

11.5.2.4 Fehlererkennung und -reaktion

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

Nach der Einwirkung einer elektromagnetischen Störgröße muss der Wasserzähler

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

11.5.3 Spezifische Softwareanforderungen

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-1: Fehlerbehebung *Die Software muss nach einer Störung wieder zur normalen Verarbeitung zurückkehren.*		
Detaillierende Anmerkungen: Datumstempel-Flags zur Unterstützung der Protokollierung von Zeiträumen im Fehlbetrieb müssen eingerichtet werden.		
Erforderliche Dokumentation: • Kurze Beschreibung der Fehlerbehebungsmechanismen und Erklärung, wann sie aktiviert werden. • Kurze Beschreibung der diesbezüglichen vom Hersteller durchgeführten Tests.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob die Umsetzung der Fehlerbehebung geeignet ist. *Funktionsprüfungen:* • Bestätigen der korrekten Funktion bei Vorhandensein definierter Einflussgrößen und provozierter Fehler.		
Beispiel einer akzeptablen Lösung: Ein Hardware-Watchdog wird von einem zyklisch ausgeführten Mikroprozessor-Unterprogramm zurückgesetzt, um das Auslösen des Watchdogs zu verhindern. Wurde irgendeine Funktion nicht ausgeführt oder – im schlimmsten Fall – befindet sich der Mikroprozessor in einer willkürlichen Endlosschleife, wird der Watchdog nicht zurückgesetzt. In diesem Fall löst der Watchdog nach einer bestimmten Zeitspanne aus und setzt den Mikroprozessor zurück.		

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

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-3: Zusätzliche Funktionalität [12] *Die zusätzliche Funktionalität, beispielsweise die Vorauszahlung oder Intervallmessung[13], sollte die rechtlich relevanten Messfunktionen nicht beeinflussen (wie im MID Anhang VI Wärmezähler (MI-004) spezifiziert).*		
Detaillierende Anmerkungen: Zusätzliche Funktionalität ist zugelassen, wenn sie die in der MID, Anhang VI Elektrizitätszähler für Wirkverbrauch (MI-004) genannten rechtlich relevanten Messfunktionen nicht beeinflusst.		
Erforderliche Dokumentation: Siehe S1 bis S3.		
Validierungsanleitung: Siehe S1 bis S3.		
Beispiel einer akzeptablen Lösung: Siehe S1 bis S3.		

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

[12] Der Hersteller sollte immer die nationalen Anforderungen bezüglich der zusätzlichen Funktionalität berücksichtigen.

[13] Bezüglich der Intervallmessung sind zusätzliche Anweisungen im WELMEC-Leitfaden 11.2 enthalten.

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

Risikoklasse B	Risikoklasse C	Risikoklasse D
I4-6: MID-Anhang I, 8.5 Rücksetzen kumulierter Messdaten 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.*		
Detaillierende Anmerkungen: • Kumulative Register eines Messgeräts sind vor dem anwendbaren Konformitätsbewertungsverfahren zurückzusetzen. Während eines Konformitätsbewertungsverfahrens nach Anhang D, F oder H1 müssen die Wärmezähler vom Hersteller mit sämtlichen Sicherungs- und Schutzvorrichtungen gemäß TEC versehen werden, wonach eine Rückstellung der kumulierten Messdaten ohne Nachweis eines Eingriffs nicht mehr möglich sein darf. • Totalisatoren der kumulativen Register eines Messgeräts müssen zurückgesetzt werden, bevor das betreffende Konformitätsbewertungsverfahren beendet ist. Während des Konformitätsbewertungsverfahrens nach Anhang D, F oder H1 müssen die Wärmezähler mit allen Sicherheitsvorrichtungen gemäß TEC ausgestattet sein, die den Nachweis eines Eingriffs in die Zählerregister nach der Rückstellung der kumulierten Messdaten gewährleisten sollen. Kumulative Register dürfen nicht während der Verwendung im Verteilernetz zurückgesetzt werden. Anmerkung: festgelegt in der EN 1434-1:2015 unter 5.10 – Spezifische Anforderungen an Registriergeräte.		
Erforderliche Dokumentation: Dokumentation der Schutzmaßnahmen gegen das Rücksetzen der Energieregister.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob das Rücksetzen der kumulierten, rechtlich relevanten Messwerte gesichert ist und ob die vorgesehenen Schutzmaßnahmen den Nachweis eines Eingriffs ermöglichen. *Funktionsprüfungen:* • Bestätigung der korrekten Funktion der vorgesehenen Schutzmaßnahmen, siehe auch P3/U3 und P4/U4.		
Beispiel einer akzeptablen Lösung: Das Register für die gemessene Gesamtmenge muss durch eine Hardware-Versiegelung geschützt sein. Andere Register, zum Beispiel Tages- oder Nachttarifregister, müssen mit denselben Mitteln geschützt werden wie Parameter (siehe P7/U7), vorausgesetzt, dass ein Gesamtregister (insgesamt kumulativ) verfügbar ist, welches von einer Hardware-Versiegelung geschützt ist. Zusätzliche Anweisungen sind im WELMEC-Leitfaden 13.1 enthalten.		

Risikoklasse B	Risikoklasse C	Risikoklasse D

I4-7: MID Anhang I, 10.5 Ablesen der Messergebnisse

Die Messergebnisse, die als Grundlage für den zu zahlenden Preis dienen, können Ergebnisse verschiedener Register sein, die durch eine Fernbedienung, Uhr oder andere Vorrichtungen aktiviert werden. Jedes Register steht für die Gesamtmenge, die mit einem Tarif im Fakturierungsprozess verbunden ist. Die Ergebnisse müssen auf verschiedenen Anzeigen periodisch oder auf Anfrage mit Hilfe der Nutzerschnittstelle dargestellt werden können.

Detaillierende Anmerkungen:

Kumulative Register eines Messgeräts können vor dem anwendbaren Konformitätsbewertungsverfahren zurückgesetzt werden. Während eines Konformitätsbewertungsverfahrens nach Anhang D, F oder H1 müssen die Verbrauchszähler vom Hersteller mit sämtlichen Sicherungs- und Schutzvorrichtungen gemäß TEC versehen werden, wonach eine Rückstellung der kumulierten Messdaten ohne Nachweis eines Eingriffs nicht mehr möglich sein darf.

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

Erforderliche Dokumentation:

Dokumentation der Erzielung der Messergebnisse, die als Grundlage für den zu zahlenden Preis dienen.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob die Messergebnisse korrekt bearbeitet wurden.

Funktionsprüfungen:

- Bestätigen der korrekten Funktion der Bearbeitung der Messergebnisse.

Beispiel einer akzeptablen Lösung:

Wenn ein Zähler für die Zählung der Mengen, die in MID Anhang VI Wärmezähler (MI-004) definiert sind, in verschiedenen Registern ausgelegt ist, muss ein Zähler die Gesamtmengen jedes Registers auf der Anzeige mit Hilfe der Nutzerschnittstelle (siehe P3/U3, z. B.: Tasten auf Geräten) sowie die derzeit aktiven Tarifregister darstellen können. Die Ergebnisse dürfen periodisch oder auf Anfrage durch die Nutzerschnittstelle auf verschiedenen Anzeigen dargestellt werden. Bei der Anzeige verschiedener Messergebnisse muss jedoch klar sein, welche Anzeige zu welchem Register gehört; es darf diesbezüglich keine Unklarheiten geben.

Falls notwendig, können zusätzliche Beschriftungen auf dem Wasserzähler angebracht werden, die die verschiedenen Register oder die Anzeige des Testmodus benennen (siehe I1-9).

Risikoklasse B	Risikoklasse C	Risikoklasse D

I4-8: MID Anhang I Schutz gegen absichtliche Änderungen bei Wärmezählern vom Typ P (mit mechanischem Zähler)

Die berechnete Prüfsumme oder eine Alternativanzeige, um den Nachweis der Softwaremodifikation zu unterstützen, ist auf Befehl für Kontrollzwecke sichtbar zu machen, siehe P6. Für Wärmezähler vom Typ P mit einem mechanischen Zähler wäre als Ausnahme ein Aufprägen der Prüfsumme oder einer Alternativanzeige der Softwaremodifikation auf das Typenschild eines Messgeräts eine akzeptable Lösung, wenn die folgenden Bedingungen A, B und C erfüllt sind:

A. Die Nutzerschnittstelle hat keinerlei Steuerungsfähigkeiten, um die Anzeige des Prüfsummenwertes oder eine Alternativanzeige der Softwaremodifikation auf dem Display zu aktivieren, oder das Display gestattet die Anzeige der Werte aus technischen Gründen nicht (mechanischer Zähler).

B. Das Messgerät hat keine Schnittstelle, um den Software-Identifikator zu übermitteln.

C. Nach der Fertigung eines Zählers ist eine Änderung der Software nicht mehr möglich oder nur dann möglich, wenn auch die Hardware oder eine Hardwarekomponente, die die Software enthält, geändert wird.

Detaillierende Anmerkungen:

- Der Hersteller ist dafür verantwortlich, dass die Prüfsumme oder eine Alternativanzeige der Softwaremodifikation ordnungsgemäß auf der betroffenen Hardware angegeben ist.
- Es gelten alle anderen detaillierenden Anmerkungen von P6.

Erforderliche Dokumentation:
Gemäß P6.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- Gemäß P6.

Funktionsprüfungen:

- Gemäß P6.

Beispiel einer akzeptablen Lösung:
Aufprägen der Prüfsumme oder einer alternativen Anzeige der Softwaremodifikation auf das Typenschild des Messgeräts.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I4-9: Anzahl der Ziffernstellen

Gemäß EN1434-1:2015 Paragraf 6.3.7:
Die Anzeige der Wärmemenge muss in der Lage sein, ohne Überlauf eine Wärmemenge zu registrieren, die mindestens der Energieübertragung entspricht, die bei einem Dauerbetrieb von 3 000 Stunden an der oberen Grenze der Wärmeleistung des Wärmezählers erfolgt. Die von einem Wärmezähler gemessene Wärmemenge, welcher 1h lang bei Obergrenze der Wärmeleistung betrieben wird, muss mindestens einer Ziffer der niedrigsten Signifikanz der Anzeige entsprechen.

Eignung gemäß Absatz 7.6 und 10.5 von Anhang I der Richtlinie 2014/32/EU (MID):
Ein Messgerät ist so auszulegen, dass die Messvorgänge kontrolliert werden können, nachdem das Messgerät in Verkehr gebracht und in Betrieb genommen wurde. Erforderlichenfalls muss das Messgerät eine spezielle Ausrüstung oder Software für diese Kontrolle besitzen. Darüber hinaus muss ein Messgerät, das fernabgelesen werden kann, auf jeden Fall mit einer der messtechnischen Kontrolle unterliegenden Anzeige ausgestattet sein, die für den Verbraucher ohne Hilfsmittel zugänglich ist.

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

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

Detaillierende Anmerkungen:

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

Erforderliche Dokumentation:

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

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

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

Funktionsprüfungen:

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

Beispiel einer akzeptablen Lösung:
Auf der Anzeige des Wärmezählers gibt es eine ausreichende Ziffernstellenanzahl, die sowohl die Anforderung an die anzeigbare Gesamtmenge sowie an die erforderliche Auflösung erfüllt.

Umschalten von Anzeigemodi auf der Anzeigevorrichtung, um die Werte für die Gesamtmenge mit der korrekten Auflösung sowie den "Prüfmodus" mit den zusätzlichen Prüfelementen anzuzeigen. Diese Anzeigemodi müssen mit Hilfe folgender Elemente angezeigt werden können:
- der Nutzerschnittstelle (siehe P3/U3, z. B.: Tasten auf Geräten) oder
- beim Durchlaufen der verschiedenen Anzeigemodi.

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

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

Risikoklasse B	Risikoklasse C	Risikoklasse D

I4-10: Anzeigetest

Zur Verifikation der korrekten Funktion aller Segmente der elektronischen Anzeige muss ein Anzeigetest durchgeführt werden können.

Detaillierende Anmerkungen:
Der Anzeigetest lautet wie folgt:
- Der Zähler muss eine Sichtprüfung der gesamten Anzeigeeinrichtung mit folgendem Verlauf erlauben:
  1) bei Siebensegmentanzeigen: Anzeige aller Elemente (z. B. ein sogenannter "8er-Test");
  2) bei Siebensegmentanzeigen: Abschalten aller Elemente ("Abschalt"-Test).
  3) bei grafischen Anzeigen: äquivalenter Test, der aufzeigt, dass Anzeigefehler nicht dazu führen können, dass irgendeine Ziffer fehlinterpretiert wird.
- Jeder Schritt dieses Verfahrens muss mindestens 1 Sekunde dauern.

Erforderliche Dokumentation:
Eine Beschreibung des elektronischen Anzeigetests und eine Erklärung, wie ein solcher Test gestartet wird.

Validierungsanleitung:
Starten des Anzeigetests und prüfen, ob eine visuelle Prüfung der gesamten Anzeige möglich ist.

Beispiel einer akzeptablen Lösung:
Ein Anzeigetest wird auf Sonderbefehl durch die Nutzerschnittstelle gestartet (siehe P3/U3, z. B.: Tasten auf Geräten) oder ist Teil des Durchlaufverfahrens, welches die verschiedenen Anzeigemodi zeigt.

11.5.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Der Zugang zu Mitteln für die Modifizierung der Software, der Einstellungen und/oder Parameter, die die Bestimmung der Messergebnisse beeinflussen, muss gesichert werden[14].

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

11.5.5 Einstufung in Risikoklassen

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

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

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

11.6 Messsysteme zur kontinuierlichen und dynamischen Mengenmessung von Flüssigkeiten außer Wasser

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

11.6.1 Spezifische Vorschriften, Normen und andere normative Dokumente

Die spezifischen Anforderungen dieses Kapitels basieren auf der MID, Anhang VII und der OIML-R117-1 Ausgabe 2019.

11.6.2 Technische Beschreibung

11.6.2.1 Hardwarekonfiguration

Messsysteme zur kontinuierlichen und dynamischen Mengenmessung von Flüssigkeiten außer Wasser sind entweder Geräte mit zweckgebundener Hard- und Software (Typ P in diesem Dokument) oder können aus mehreren Teilen bestehen, einschließlich Universalgeräten (Typ U in diesem Dokument).

Das Messsystem muss mindestens umfassen:

- einen Zähler,
- einen Übergabepunkt und
- einen hydraulischen Weg.

Für den korrekten Betrieb ist es häufig erforderlich, Folgendes hinzuzufügen:

- eine Vorrichtung zur Gasbeseitigung,
- einen Filter,
- eine Pumpe und
- Korrekturgeräte.

Das Messsystem kann mit weiteren Zusatzeinrichtungen und zusätzlichen Geräten ausgestattet sein.

Zusatzeinrichtungen und zusätzlichen Geräte können sein:

- Nullstellgerät;
- Wiederholanzeigegerät;
- Druckgerät;
- Speichergerät;
- Preisanzeigegerät;
- Summierungsanzeigegerät;
- Korrekturgerät;
- Konvertierungsgerät;
- Voreinstellgerät;
- Selbstbedienungsanordnung und
- Selbstbedienungsgerät.

Wenn Zusatzeinrichtungen und zusätzliche Geräte als separate Geräte Teil von Messsystemen zur kontinuierlichen und dynamischen Mengenmessung von Flüssigkeiten außer Wasser sind, die ohne Brechen der Siegel abgenommen werden kön-

nen und rechtlich relevante Software enthalten, dann muss die Erweiterung T angewendet werden.

Sind mehrere Zähler für einen einzigen Messvorgang vorgesehen, gelten die Zähler als ein einziges Messsystem.

Wenn mehrere Messgeräte, die für getrennte Messvorgänge vorgesehen sind, über gemeinsame Elemente verfügen (Rechner, Filter, Vorrichtung zur Gasbeseitigung, Umwerter usw.), wird jedes Messgerät als ein separates Messsystem betrachtet, das die gemeinsamen Elemente teilt.

11.6.2.2 Softwarekonfiguration

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

11.6.2.3 Messprinzip

Die Menge der Flüssigkeit wird mittels Messsensors eines Volumen- oder Massendurchflusssensors gemessen, der nach unterschiedlichen Prinzipien arbeiten kann. Die gemessene Größe wird im Sender in ein Signal (z. B. Impulse) umgewandelt und an das Rechen- und Anzeigegerät gesendet. Sie bilden zusammen einen Zähler. An das Messgerät können zusätzliche Geräte zur Messung der Flüssigkeitseigenschaften angeschlossen werden, z. B. Temperatursensor, Drucksensor. Die Messgröße kann auf die Grundbedingungen umgerechnet werden, z. B. mit einer ATC-Funktion (Automatic Temperature Compensation) zur Umrechnung auf 15 °C. Die abgemessene Menge muss in Millilitern, Kubikzentimetern, Litern, Kubikmetern, Gramm, Kilogramm oder Tonnen angegeben werden.

11.6.2.4 Fehlererkennung und -reaktion

Die Anforderung von Anhang VII (MI-005) Artikel 3.1 befasst sich mit elektromagnetischen Störgrößen. Es besteht die Notwendigkeit, diese Anforderungen für softwaregesteuerte Geräte zu interpretieren, da die Entdeckung einer Störgröße (eines Fehlers) sowie die nachfolgende Behebung nur durch das Zusammenwirken spezieller Hardwareteile und spezieller Software möglich sind. Aus Softwaresicht macht es keinen Unterschied, was der Grund für eine Störgröße war (elektromagnetisch, elektrisch, mechanisch usw.): die Verfahren zur Wiederaufnahme des Normalbetriebs sind immer gleich.

11.6.3 Spezifische Softwareanforderungen

Risikoklasse B	Risikoklasse C	Risikoklasse D

I5-1: Fehlerbehebung

Messsysteme für nicht unterbrechbare Messungen müssen so entworfen und hergestellt sein, dass keine signifikanten Fehler auftreten, wenn sie Störgrößen ausgesetzt sind. Prüfeinrichtungen für Unstimmigkeiten in der Bildung, Übertragung, Verarbeitung und/oder Anzeige der Messdaten müssen im Fehlerfalle eine angemessene Reaktion auslösen.

Elektronische Messsysteme für nicht unterbrechbare Messungen müssen so entworfen und hergestellt sein, dass im Falle, dass sie einer Störgröße ausgesetzt sind, entweder:

a) die Anzeige des Messergebnisses eine momentane Änderung anzeigt, die nicht als Messergebnis interpretiert, gespeichert oder übertragen werden kann. Weiterhin kann dies im Fall einer unterbrechbaren Messung bedeuten, dass keine Messung möglich ist; oder

b) die Änderung im Messergebnis größer als der kritische Änderungswert ist. In diesem Fall muss das Messsystem das Auslesen des letzten Messergebnisses vor Auftreten des kritischen Änderungswerts ermöglichen und den Fluss unterbrechen.

Detaillierende Anmerkungen:

Bei nicht unterbrechbaren Messsystemen muss die Erkennung von Fehlern bei der Erzeugung, Übertragung, Verarbeitung und/oder Anzeige von Messdaten durch die Prüfeinrichtungen folgende Maßnahmen zur Folge haben:

- automatische Korrektur der Störung; oder
- Anhalten nur des fehlerhaften Geräts, wenn das Messsystem ohne dieses Gerät weiterhin den Vorschriften entspricht.

Stellen die Prüfeinrichtungen eines unterbrechbaren elektronischen Messsystems signifikante Defekte oder Unrichtigkeiten bei der Erzeugung, Übertragung, Verarbeitung oder Anzeige der Messdaten fest, müssen sie entsprechend handeln:

- automatische Korrektur der Störung; oder
- Anhalten nur des fehlerhaften Geräts, wenn das Messsystem ohne dieses Gerät weiterhin den Vorschriften entspricht; oder
- das Messsystem muss das Auslesen des letzten Messergebnisses vor Auftreten des kritischen Änderungswerts ermöglichen und den Fluss unterbrechen.

Zusätzliche Anforderungen sind in OIML R117-1:2019 Abschnitt A.1.5 bezüglich Fehlergenerierungsparametern aufgeführt.

Erforderliche Dokumentation:

Eine kurze Beschreibung dessen, was überprüft wird, was erforderlich ist, um den Fehlererkennungsprozess auszulösen, und welche Maßnahmen bei der Erkennung eines Fehlers ergriffen werden.

Eine Liste der Parameter und ihrer gültigen und kontrollierten Bereiche, die Fehler erzeugen können und von der Software erkannt werden, einschließlich der erwarteten Reaktion und, falls für das Verständnis des Erkennungsalgorithmus erforderlich, seiner Beschreibung.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob die Umsetzung der Fehlerbehebung geeignet ist.

Funktionsprüfungen:

- Funktionsprüfungen bei Vorhandensein definierter Einflussgrößen und provozierter Fehler.

Beispiel einer akzeptablen Lösung:

Ein Hardware-Watchdog wird von einem zyklisch ausgeführten Mikroprozessor-Unterprogramm zurückgesetzt, um das Auslösen des Watchdogs zu verhindern. Wurde irgendeine Funktion nicht ausgeführt oder – im schlimmsten Fall – befindet sich der Mikroprozessor in einer willkürlichen Endlosschleife, wird der Watchdog nicht zurückgesetzt. In diesem Fall löst der Watchdog nach einer bestimmten Zeitspanne aus und setzt den Mikroprozessor zurück.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I5-2: Nicht rechtlich relevante Software und dynamisches Verhalten *Die nicht rechtlich relevante Software darf das dynamische Verhalten eines Messprozesses nicht unzulässig beeinflussen.*		
Detaillierende Anmerkungen: Diese Anforderung stellt sicher, dass das dynamische Verhalten der rechtlich relevanten Software bei Echtzeitanwendungen von Zählern nicht in unzulässiger Weise durch nicht rechtlich relevante Software beeinflusst wird, d. h., dass die Ressourcen der rechtlich relevanten Software nicht in unzulässiger Weise vom nicht rechtlich relevanten Teil gemindert werden.		
Erforderliche Dokumentation: • Beschreibung der Interrupt-Hierarchie. • Zeitdiagramm der Softwareaufgaben. Grenzen der anteiligen Laufzeit der nicht rechtlich relevanten Aufgaben.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob die Dokumentation der Grenzen der anteiligen Laufzeit der nicht rechtlich relevanten Aufgaben dem Programmierer des nicht rechtlich relevanten Softwareteils zur Verfügung steht. *Funktionsprüfungen:* • Bestätigen der korrekten Funktion bei Vorhandensein definierter Einflussgrößen und provozierter Fehler.		
Beispiel einer akzeptablen Lösung: Die Interrupt-Hierarchie ist so entworfen, dass nachteilige Einflüsse vermieden werden.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I5-3: Zusätzliche Funktionalität[15] *Zusätzliche Funktionalität sollte die rechtlich relevanten Messfunktionen nicht beeinflussen, wie in der MID, Anhang VII (MI-005), spezifiziert.*		
Detaillierende Anmerkungen: Zusätzliche Funktionalität ist zugelassen, wenn sie die rechtlich relevanten Messfunktionen, wie in der MID, Anhang VII (MI-005), spezifiziert, nicht beeinflusst.		
Erforderliche Dokumentation: Siehe P8, U8 und S1 bis S3.		
Validierungsanleitung: Siehe P8, U8 und S1 bis S3.		
Beispiel einer akzeptablen Lösung: Siehe P8, U8 und S1 bis S3.		

[15] Der Hersteller sollte immer die nationalen Anforderungen bezüglich der zusätzlichen Funktionalität berücksichtigen.

Risikoklasse B	Risikoklasse C	Risikoklasse D

I5-4: Backup-Einrichtungen

Im Falle von nicht unterbrechbaren Messsystemen kann eine Einrichtung vorhanden sein, die für ein regelmäßiges Backup von Messdaten (wie z. B. Messwerte und der aktuelle Prozessstatus) sorgt. Diese Daten müssen in einem nichtflüchtigen Speicher gehalten werden.

Das Messsystem muss mit einer Backup-Spannungsquelle ausgestattet sein, um sicherzustellen, dass alle Messfunktionen bei Ausfall der Hauptstromversorgung ausgeführt werden können. Oder es muss mit Mitteln zur Speicherung und Anzeige der Daten ausgestattet sein, sodass der laufende Geschäftsvorgang beendet werden kann.

Detaillierende Anmerkungen:

Das Speicherintervall muss so kurz sein, dass die Differenz zwischen aktuellen und gespeicherten Messdaten gering ist.

Erforderliche Dokumentation:

- Eine kurze Beschreibung, welche Daten gesichert werden und wann dies geschieht.
- Berechnung des maximalen Fehlers, der auftreten kann, wenn kumulierte Messdaten von der Backup-Einrichtung gespeichert werden.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- ob Messdaten im nichtflüchtigen Speicher gesichert werden und wiederhergestellt werden können.

Funktionsprüfungen:

- Funktionsprüfungen bei Vorhandensein definierter Einflussgrößen und provozierter Fehler.

Beispiel einer akzeptablen Lösung:

- Die Messdaten werden regelmäßig (Häufigkeit abhängig von der Anwendung) auf einem nichtflüchtigen Speicher auf einem Speichergerät gesichert.
- Ein Hardware-Watchdog wird ausgelöst, wenn er nicht in regelmäßigen Abständen zurückgesetzt wird. Dieser Alarm erzeugt eine Unterbrechung im Mikroprozessor. Die zugewiesene Unterbrechungsroutine sammelt sofort Messwerte, Zustandswerte und andere relevante Daten und speichert sie in einem nichtflüchtigen Speicher, z. B. in einem EEPROM oder in einem anderen geeigneten Speicher.

Hinweis: Es wird davon ausgegangen, dass die Watchdog-Unterbrechung höchste Unterbrechungspriorität hat und jede normale Verarbeitung oder jede willkürliche Endlosschleife unterbrechen kann, d. h., die Ablaufsteuerung springt immer zur Unterbrechungsroutine, wenn der Watchdog ausgelöst wird.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I5-5: Software-Download *Während der Software-Installation muss der Messvorgang unterbunden sein oder eine korrekte Messung muss angemessen gewährleistet werden.*		
Detaillierende Anmerkungen: • Diese Anforderung gilt zusätzlich zu D1, D2, D3 und D4, wenn ein Software-Download durchgeführt wurde. • Die zusätzliche Anforderung stellt sicher, dass für Echtzeit-Anwendungen des Zählers Messungen nicht unterbrochen werden.		
Erforderliche Dokumentation: Siehe D1, D2, D3 und D4.		
Validierungsanleitung: Siehe D1, D2, D3 und D4.		
Beispiel einer akzeptablen Lösung: Siehe D1, D2, D3 und D4.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I5-6: Aufgeprägter Software-Identifikator *Der Software-Identifikator wird normalerweise auf einem Display angezeigt. Für Messsysteme für Flüssigkeiten außer Wasser wäre als Ausnahme ein Aufprägen des Software-Identifikators auf das Typenschild eines Messgeräts eine akzeptable Lösung, wenn die folgenden Bedingungen A, B und C erfüllt sind:* *A. Die Nutzerschnittstelle hat keinerlei Steuerungsfähigkeiten, um die Anzeige des Prüfsummenwertes oder eine Alternativanzeige der Softwaremodifikation auf dem Display zu aktivieren, oder das Display gestattet die Anzeige dieser Werte aus technischen Gründen nicht (mechanischer Zähler).* *B. Das Messgerät hat keine Schnittstelle, um den Software-Identifikator zu übermitteln.* *C. Nach der Fertigung eines Zählers ist eine Änderung der Software nicht mehr möglich oder nur dann möglich, wenn auch die Hardware oder eine Hardwarekomponente geändert wird.*		
Detaillierende Anmerkungen: • Die Kennzeichnung, die den Software-Identifikator aufweist, darf weder löschbar noch übertragbar sein. • Der Hersteller der Hardware bzw. der betroffenen Hardwarekomponenten ist dafür verantwortlich, dass der Software-Identifikator ordnungsgemäß auf der betroffenen Hardware angegeben ist. • Es gelten alle anderen detaillierenden Anmerkungen von P6.		
Erforderliche Dokumentation: • Gemäß P2/U2.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • Gemäß P2/U2. *Funktionsprüfungen:* • Gemäß P2/U2.		
Beispiel einer akzeptablen Lösung: Aufprägen des Software-Identifikators auf das Typenschild des Messgeräts.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I5-7: Parametereinstellungen *Zum Zweck der Verifizierung eines Messgeräts muss es möglich sein, die aktuellen Parametereinstellungen, die die rechtlich relevanten Charakteristiken des Messsystems festlegen, anzuzeigen oder auszudrucken.* *Die Parameter müssen geschützt sein, siehe P7 und U7. Im Falle eines Audit Trails muss der Zeitstempel von der Uhr des Geräts abgelesen werden. Die Einstellung von Zeit und Datum muss geschützt sein.*		
Detaillierende Anmerkungen: Diese Anforderungen sind in OIML R117-1:2019 Abschnitt A.1.3.3 zu finden.		
Erforderliche Dokumentation: Informationen bezüglich der Parametereinstellungen und Verifizierungsmöglichkeiten.		
Validierungsanleitung: Die Parametereinstellungen und Verifizierungsmöglichkeiten des Messgeräts sind zu überprüfen.		
Beispiel einer akzeptablen Lösung: Die obengenannten Anforderungen müssen erfüllt sein.		

Risikoklasse B	Risikoklasse C	Risikoklasse D
I5-8: Zusatzeinrichtungen und zusätzliche Geräte (ZZG) *Wenn Zusatzeinrichtungen oder zusätzliche Geräte Teil eines Messgerätes sind und von diesem getrennt werden können, muss Anhang T angewandt werden.*		
Detaillierende Anmerkungen: In Fällen, in denen Messgeräte ZZG ohne rechtlich relevante Software enthalten, müssen Daten aus ZZG mit nicht rechtlich relevanter Software klar von Daten aus ZZG mit rechtlich relevanter Software unterscheidbar sein. In Fällen, in denen ZZG mit rechtlich relevanter Software abgetrennt werden können, ohne ein Siegel zu brechen, das die Verbindung zum Messgerät schützt, ist Anhang T anzuwenden.		
Erforderliche Dokumentation: • Liste der ZZG, die rechtlich relevante Software enthalten, zzgl. einer Beschreibung. • Gemäß Anhang T. • Gemäß Anhang S (falls zutreffend).		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • Gemäß Anhang T. • Gemäß Anhang S (falls zutreffend). • ob die Dokumentation eine vollständige Liste von ZZG mit rechtlich relevanter Software enthält. *Funktionsprüfungen:* • Gemäß Anhang T. • Gemäß Anhang S (falls zutreffend).		
Beispiel einer akzeptablen Lösung:		

11.6.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten[16]

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

Parameter	Geschützt	Einstellbar	Anmerkung

[16] Siehe auch WELMEC-Leitfaden 10.6: Guide for Securing of Fuel Dispensers

Kalibrierfaktor	x		
Linearisierungsfaktor	x		
Rechtlich relevante Konfiguration der Register	x		
Sonstige relevante Parameter, die das Messergebnis beeinflussen könnten, bspw., aber nicht beschränkt auf: • Anzahl der Ziffernstellen für die Mengenangabe • Abschaltung bei geringem Durchfluss • Servicebefehle (Speichern der Peripheriegeräte-IDs, Zurücksetzen elektronischer Summen, vollständige Initialisierung des Speichers – elektronische Zusammenfassungen, Statistiken und Historie sowie Übergang von Parametern auf Werkseinstellungen) • Mit Massemesser gemessener Wert – Einstellung L/kg • Unterdrückung der Ausgabeschlauchdehnung – Einstellung der versteckten Menge bei Ausgabebeginn • Korrekturfaktor des Messgeräts • Messzeit nach dem Aufhängen der Düse • Puls / L, Puls / kg • Aktivierung der automatischen Temperaturkompensation für einzelne Düsen (ATC) und Kalibrierung von Temperatursensoren • Kraftstofftyp oder -dichte • Zuordnung der Temperatursensoren zu einzelnen Düsen • Konfiguration des Massemessers • Nullpunkt des Massemessers einstellen	x		
Software-Download der rechtlich relevanten Software	x		
Softwareeinstellung/-konfiguration im Falle von Pulssignalen	x		

Softwareeinstellung/-konfiguration im Falle von digitalen Signalen	x		

11.6.5 Einstufung in Risikoklassen

Die folgende Risikoklasse wird als angemessen befunden und sollte angewendet werden, wenn Softwareprüfungen für (softwaregesteuerte) Messsysteme von Flüssigkeiten außer Wasser durchgeführt werden:

– **Risikoklasse C für Messgeräte vom Typ P und U**

11.7 Waagen

Waagen werden in zwei Hauptkategorien unterteilt:

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

Während die meisten selbsttätigen Waagen durch die MID geregelt sind, gilt dies nicht für NSW; diese werden immer noch durch die EU-Richtlinie 90/384/EEC geregelt. **Daher gilt der Softwareleitfaden WELMEC 7.5 für NSW, während der vorliegende Softwareleitfaden für SW gilt.**

Die spezifischen 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.

11.7.1 Spezifische Vorschriften, Normen und andere normative Dokumente

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

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

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

Eine Kategorie der SW ist nicht in der MID geregelt:

- selbsttätige Waagen für Straßenfahrzeuge in Bewegung (R134)

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

Von diesen sechs Kategorien wurde jedoch nur für die Kategorien *selbsttätige Waagen zum* ***diskontinuierlichen Totalisieren*** und *selbsttätige Waagen zum* ***kontinuierlichen Totalisieren*** *(Förderbandwaagen)* die Notwendigkeit ausgemacht, instrumentenspezifische Softwareanforderungen aufzustellen (siehe 11.7.3). Der Grund hierfür ist, dass die Messung über einen relativ langen Zeitraum kumulativ ist und nicht wiederholt werden kann, wenn ein signifikanter Fehler auftritt.

11.7.2 Technische Beschreibung

11.7.2.1 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 auf Wägezellen gestützten Behältern, Stromversorgung, Steuerelektronik und Anzeigevorrichtung.

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, einem auf Wägezellen gestützten Lastaufnehmer, Energieversorgung, Steuerelektronik und Anzeigevorrichtung. Es gibt Mittel zum Anpassen der Förderbandspannung.

11.7.2.2 Softwarekonfiguration

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

11.7.2.3 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. Es gibt keine gezielte Unterteilung des Produkts oder Unterbrechung des Förderbands, wie es bei einer selbsttätigen Waage zum diskontinuierlichen Totalisieren der Fall ist. Die Gesamtmasse ist eine Integration der einzelnen Messungen. Es ist anzumerken, dass für den Lastaufnehmer Dehnungsmessstreifen-Wägezellen oder andere Techniken, z. B. Schwingende Saite, verwendet werden können.

11.7.2.4 Defekte

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

11.7.3 Spezifische Softwareanforderungen (Selbsttätige Waagen zum diskontinuierlichen und zum kontinuierlichen Totalisieren)

MID Anhang MI-006 Kapitel IV Abschnitt 8 und Kapitel V Abschnitt 6 behandeln elektromagnetische Störgrößen. Es ist notwendig, diese Anforderungen für softwaregesteuerte Geräte zu interpretieren, da das Entdecken einer Störgröße (eines Fehlers) sowie das nachfolgende Beheben nur durch das Zusammenwirken spezieller Hardwareteile und spezieller Software möglich sind. Aus Softwaresicht macht es keinen Unterschied, was der Grund für eine Störgröße war (elektromagnetisch, elektrisch, mechanisch usw.); die Verfahren zur Wiederaufnahme des Normalbetriebs sind immer gleich.

Risikoklasse B	Risikoklasse C	Risikoklasse D
I6-1: Fehlererkennung *Die Software muss erkennen, dass die normale Verarbeitung gestört ist.*		
Detaillierende Anmerkungen: Bei Entdeckung eines Fehlers: a. Die kumulierten Messwerte und andere rechtlich relevante Daten müssen automatisch in einem nichtflüchtigen Speicher gesichert 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 ergriffen wird. 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 behandelt oder richtig berücksichtigt wird.		
Validierungsanleitung: *Auf Basis der Dokumentation ist zu prüfen:* • ob die Umsetzung der Fehlererkennung angemessen 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 Hardware-Watchdog wird von einem zyklisch ausgeführten Mikroprozessor-Unterprogramm zurückgesetzt, um das Auslösen des Watchdogs zu verhindern. Vor dem Zurücksetzen prüft das Unterprogramm den Zustand des Systems, z. B., ob alle rechtlich relevanten Unterprogramme während des letzten Intervalls ausgeführt wurden. Wurde irgendeine Funktion nicht ausgeführt oder – im schlimmsten Fall – befindet sich der Mikroprozessor in einer willkürlichen 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 im Falle einer Störung für ein Backup von Messdaten (wie z. B. Messwerte und aktueller Prozessstatus) sorgt.

Detaillierende Anmerkungen:

a. Die Zustandsmerkmale und wichtige Daten müssen in einem nichtflüchtigen Speicher gespeichert werden.

b. Diese Anforderung impliziert normalerweise eine kontrollierte Speichermöglichkeit, die im Falle einer Störung ein automatisches Backup gestattet. Periodisches Backup ist nur dann zulässig, wenn aufgrund von Hardware- oder Funktionsbeschränkungen keine kontrollierte Speichermöglichkeit vorhanden ist. In diesem Ausnahmefall müssen die Abstände zwischen den einzelnen Backups ausreichend klein sein, d. h., die größtmögliche Diskrepanz zwischen den laufenden und den gespeicherten Werten muss innerhalb eines festgelegten Bruchteils des höchstzulässigen Fehlers liegen (siehe Erforderliche Dokumentation).

c. Die Backup-Einrichtungen sollten normalerweise geeignete Wake-Up-Einrichtungen 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 kumulierten Werten auftreten kann, wenn ein zyklisches (periodisches) Backup durchgeführt wird.

Validierungsanleitung:

Auf Basis der Dokumentation ist zu prüfen:

- Sicherungsmöglichkeiten

Funktionsprüfungen:

- Durch Simulierung einer Störung überprüfen, ob der Backupmechanismus so wie in der Dokumentation beschrieben funktioniert.

Beispiel einer akzeptablen Lösung:

Ein Hardware-Watchdog wird ausgelöst, wenn er nicht in regelmäßigen Abständen zurückgesetzt wird. Dieser Alarm erzeugt eine Unterbrechung im Mikroprozessor. Die zugewiesene Unterbrechungsroutine sammelt sofort Messwerte, Zustandswerte und andere relevante Daten und speichert sie in einem nichtflüchtigen Speicher, z. B. in einem EEPROM oder in einem anderen geeigneten Speicher.

Hinweis: Es wird davon ausgegangen, dass die Watchdog-Unterbrechung höchste Unterbrechungspriorität hat und jede normale Verarbeitung oder jede willkürliche Endlosschleife unterbrechen kann, d. h., die Ablaufsteuerung springt immer zur Unterbrechungsroutine, wenn der Watchdog ausgelöst wird.

11.7.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Tabelle 11-1: Beispiele für rechtlich relevante, gerätespezifische und bauartspezifische 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 der Stabilität des 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
Aufwärmzeit	TF (TD)	X	X	X	X	X	X	X
(Wechselseitige) Verriegelung von Funktionen	TF		X	X				
z. B. Nulleinstellung/Tara			X	X	X	X		
Betrieb automat./nicht automat.							X	
Nullstellung/Totalisieren		X						X
Log für Änderung der dynamischen Justierung	TF (VV)		X	X				
Maximaler Durchsatz/Geschwindigkeitsbereich (dynamisches Wiegen)	DD (TD)	X	X	X	X		X	X
(Produktspezifische) Parameter für die dynamische Gewichtsberechnung	VV		X	X			X	
Voreingestellter Gewichtswert	VV		X		X			
Breite des Einstellbereichs	DD (TD)		X	X				
Kriterium für automat. Nullstellung (z. B. Zeitintervall, Ende des Wägezyklus)	DD (TD)		X	X	X		X	X
Minimale Entnahmemenge, minimale Nennfüllung	DD				X			X
Grenzwert für Annahme eines signifikanten Defekts	DD (TD)	X			X			

(wenn nicht 1e oder 1d) Grenzwert für die Batterieleistung	DD (TD)	X	X	X	X	X	X	X

Tabelle 11-1: Beispiele für rechtlich relevante, gerätespezifische und bauartspezifische 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.

11.7.5 Weitere Aspekte

Keine

11.7.6 Einstufung in Risikoklassen

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

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

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

11.8 Taxameter

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

11.8.1 Spezifische Vorschriften, Normen und normative Dokumente

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

11.8.2 Technische Beschreibung

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

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

11.8.3 Spezifische Softwareanforderungen

MID Anhang IX, 4:

> Ein Taxameter muss über eine (oder mehrere) geeignete rückwirkungsfreie Schnittstelle(n) folgende Daten übertragen können:
>
> - Betriebseinstellung: "Frei", "Besetzt" oder "Kasse";
>
> - Zählwerksdaten gemäß Nummer 15.1;
>
> - allgemeine Daten: Konstante des Wegstreckensignalgebers, Datum der Sicherung, Taxikennung, Echtzeit, Tarifkennung;
>
> - Preisdaten einer Fahrt: in Rechnung gestellte Gesamtsumme, Fahrpreis, Berechnung des Fahrpreises, Zuschlag, Datum, Fahrtbeginn, Fahrtende, zurückgelegte Strecke;
>
> - Tarifdaten: Parameter des bzw. der Tarife.
>
> Aufgrund nationaler Rechtsvorschriften besteht möglicherweise die Pflicht, bestimmte Geräte an die Schnittstelle(n) eines Taxameters anzuschließen. In diesem Fall muss es möglich sein, mittels einer Sicherheitseinstellung den Betrieb des Taxameters automatisch zu verhindern, wenn das erforderliche Gerät nicht vorhanden ist oder nicht vorschriftsmäßig funktioniert.

MID Anhang IX, 9:

Bei Abfall der Stromversorgung unter den vom Hersteller angegebenen unteren Betriebsgrenzwert muss das Taxameter:

– ordnungsgemäß weiterarbeiten oder den ordnungsgemäßen Betrieb ohne Verlust der vor dem Spannungsabfall verfügbaren Daten wieder aufneh-

men, wenn der Spannungsabfall vorübergehend auftritt, d. h. durch das Wiederanlassen des Motors verursacht ist;
– einen laufenden Messvorgang abbrechen und zur Betriebsstellung „Frei“ zurückkehren, wenn der Spannungsabfall länger andauert.

MID Anhang IX, 15.2:

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

MID Anhang IX, 19:

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

Risikoklasse B	Risikoklasse C	Risikoklasse D
I7-1: Backup-Einrichtungen *Es muss eine Einrichtung vorhanden sein, die automatisch für wesentliche Daten (wie z. B. Messdaten oder den aktuellen Prozessstatus) ein Backup erzeugt, wenn die Spannung für längere Zeit abfällt.*		
Detaillierende Anmerkungen: 1) Diese Daten sollten normalerweise in einem nichtflüchtigen Speicher gespeichert werden. 2) Ein Spannungsdetektor ist notwendig, um zu erkennen, wann Messdaten gespeichert werden müssen. 3) Die Backup-Einrichtungen müssen geeignete Wake-Up-Funktionen 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 prüfen:* • ob im Falle einer Störung alle rechtlich relevanten Daten gespeichert sind. *Funktionsprüfungen:* • Funktionsprüfungen bei Vorhandensein definierter Einflussgrößen und provozierter Fehler.		
Beispiel einer akzeptablen Lösung: Der Spannungspegeldetektor löst eine Unterbrechung aus, wenn die Spannung für die Dauer von 15 s abfällt. Die zugehörige Unterbrechungsroutine sammelt Messdaten, Statuswerte und andere relevante Daten und speichert sie in einem nichtflüchtigen Speicher, z. B. EEPROM. Wenn der Spannungspegel wieder steigt, werden die Daten wiederhergestellt und die Funktion läuft weiter oder wird gestoppt (siehe MI-007, 9.) *Hinweis:* Es wird davon ausgegangen, dass die Spannungsunterbrechung eine hohe Unterbrechungspriorität hat und jede normale Verarbeitung oder jede willkürliche Endlosschleife unterbrechen kann, d. h., die Programmsteuerung springt immer zu der Unterbrechungsroutine, wenn die Spannung abfällt.		

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

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

11.8.4 Beispiele für rechtlich relevante Parameter, Funktionen und Daten

Zusätzlich zu den unter 11.8.2 genannten Funktionen, können die folgenden typischen Parameter von Taxametern betrachtet werden.

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

Mindestens die Tarife müssen separat gesichert werden.

Die folgenden Daten können ebenfalls berücksichtigt werden:

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

11.8.5 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…

11.8.6 Einstufung in Risikoklassen

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

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

11.9 Maßverkörperungen

Maßverkörperungen unterliegen den Regelungen der MID. Die spezifischen Anforderungen befinden sich in Anhang MI-008.

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

11.10 Längenmessgeräte

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

Fehlende Kapitel werden eingetragen, wenn dies in Zukunft für notwendig erachtet wird.

11.10.1 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**

11.11 Abgasanalysatoren

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

Fehlende Kapitel werden eingetragen, wenn dies in Zukunft für notwendig erachtet wird.

11.11.1 Einstufung in Risikoklassen

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

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

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 spezifischen 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 die Baumusterprüfbescheinigung benötigten Informationen im letzten Unterkapitel dieses Kapitels aufgelistet.

12.1 In die Baumusterprüfbescheinigung einzubeziehende Informationen

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

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

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

Abbildung 12-1: Anzeige des gewählten Typs, der Risikoklasse sowie der entsprechenden Anhänge

2. **Software-Identifikation**
   - Anzeige der validierten Werte des Software-Identifikators bzw. der -Identifikatoren der rechtlich relevanten Software.
   - Beschreibung, wie der Software-Identifikator bzw. die Software-Identifikatoren der rechtlich relevanten Software angezeigt werden.

3. **Software-Integritätsprüfung**
   - Bei den Risikoklassen C und höher, Angabe der Prüfsumme oder alternativen Methode mit dem gleichen Schutzniveau.
   - Bei den Risikoklassen C und höher, genaue Angabe, wie die Prüfsumme oder alternative Methode mit dem gleichen Schutzniveau zu prüfen ist.
   - Hinweis: Verweis auf ein Dokument (z. B. Benutzerhandbuch) ist ungeeignet.
   - Beschreibung, wie die Audit Trails zu prüfen sind, falls zutreffend.

- Beschreibung der Hardware-Siegelung(en) und ggf. anderer Siegelungstypen hinsichtlich der Software.
- Gegebenenfalls andere Mittel zum Schutz der Integrität.

4. Kurze Beschreibung der Softwareumgebung

- Anzeige der relevanten Information hinsichtlich:
- Softwareumgebung, die für die Betreibung der Software notwendig ist (z. B. Betriebssystem).
- Module unter rechtlicher Kontrolle (sofern Softwaretrennung implementiert ist).
- Hardware- und Softwareschnittstellen (z. B. Infrarot, Bluetooth, Wireless LAN…).
- Elektronische (Hardware-) Teilereferenzen und ihre Positionen im Messgerät einschließlich ihrer Sicherung und ihres Schutzes, falls erforderlich.

12.2 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 WELMEC-Leitfaden 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. Die Grundfunktionen des Geräts sind:

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

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

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

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

Seite 1 / 4

Softwaretyp

Risikoklasse [A-E]	P	U	O	L	T	S	D	Ix [1-6]
C	x			x				I1

Die eingebettete Software des Messgeräts wurde entwickelt von

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

Software-Identifikation

Die Version der überprüften Software lautet **V1.2c.** Die Prüfsumme ist 0xA07GT… (CRC32). Softwareversion und Prüfsumme können auf dem LCD-Display durch einen Knopfdruck bei eingeschaltetem Messgerät überprüft werden.

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 DF100
- Wartungshandbuch DF100
- 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.

Software-Integritätsprüfung

- Für Risikoklassen C und höher ist die Prüfsumme bzw. alternative Methode mit gleicher Anforderung anzugeben.
- Präzise Beschreibung bei Risikoklasse C und höher, wie die Prüfsumme bzw. Alternativmethode bei gleichem Anforderungsniveau angesehen werden kann.
- Hinweis: Ein Verweis auf ein Dokument (z. B. Benutzerhandbuch) ist nicht geeignet.
- ggf. Beschreibung, wie die Audit Trails angezeigt werden.
- Beschreibung der Hardware-Siegelung(en) und anderer Siegelungsarten im Zusammenhang mit der Software, sofern zutreffend.
- Ggf. andere Mittel zum Integritätsschutz.

Kurze Beschreibung der Softwareumgebung

- Angabe relevanter Informationen bzgl.:
- Software-Ausführungsumgebung, die zum Betrieb der Software erforderlich ist (z. B. Betriebssystem).
- Softwaremodule unter rechtlicher Kontrolle (sofern Softwaretrennung implementiert ist).
- Hardware- und Softwareschnittstellen (z. B. Infrarot, Bluetooth, Wireless LAN…).
- Verweise auf elektronische (Hardware-)Teile und deren Positionen im Messgerät sowie deren Sicherung, wenn benötigt.

Ablauf der Prüfung

Die Validierung wurde gemäß WELMEC 7.2 Softwareleitfaden 2022 durchgeführt (Download von www.welmec.org).

Die Validierung wurde zwischen dem 1. November und dem 23. Dezember 2021 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 von Messdaten

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

Für dieses Gerät wurde die Risikoklasse C angewandt.

Folgende Validierungsmethoden wurden angewandt:

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

Ergebnis

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

– P1, P2, P3, P5, P6, P7, P8
(Anforderung P4 wird als nicht anwendbar angesehen.)

– L1, L2, L3, L4, L5, L6, L7, L8

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

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

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

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

Die Software des Dynaflow DF100 V1.2c erfüllt die wesentlichen Anforderungen der Messgeräterichtlinie.

Das Ergebnis bezieht sich nur auf die geprüfte Einheit.

National Testing & Measurement Lab
Software-Abteilung

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

M. S.A.N.S Problème
Technical Officer

Datum: 23. Dezember 2003

Seite 4 / 4

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

Die erste Checkliste unterstützt den Nutzer bei der Entscheidung, ob die Grundkonfiguration P oder U für das zu prüfende Gerät anzuwenden ist.

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

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

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

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

12.4 Anhang 2 des Prüfberichts: Spezifische Checklisten für die entsprechenden technischen Teile

12.4.1 Checkliste für die Grundanforderungen an ein Gerät vom Typ P

Checkliste für Anforderungen vom Typ P						
Anforderung	**Prüfverfahren**		**Bestanden**	**Durchgefallen**	**Entfällt**	**Anmerkungen***
P1		Erfüllt die erforderliche Herstellerdokumentation die Anforderung P1 (a-f)?				
P2		Wird die Software-Identifikation, wie in P2 gefordert, umgesetzt und dargestellt?				
P3		Wird bei der Befehlseingabe über die Nutzerschnittstelle die unzulässige Einflussnahme von rechtlich relevanter Software, gerätespezifischen Parametern und Messdaten verhindert?				
P4		Beeinflussen die über Kommunikationsschnittstellen des Geräts eingegebenen Befehle die rechtlich relevante Software, gerätespezifischen Parameter und Messdaten nicht unzulässig?				
P5		Sind rechtlich relevante Software, gerätespezifische Parameter und Messdaten gegen zufällige oder unbeabsichtigte Änderungen geschützt?				
P6		Ist die rechtlich relevante Software gegen unzulässige absichtliche Modifizierung, unzulässiges Laden oder Austauschen des Hardwarespeichers gesichert?				
P7		Sind die gerätespezifischen Parameter, wie in P7 gefordert, geschützt?				
P8		Ist die Authentizität der dargestellten Messdaten gewährleistet?				
** Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.*						

12.4.2 Checkliste für die Grundanforderungen für ein Gerät vom Typ U

Checkliste für Anforderungen vom Typ U						
Anforderung	**Prüfverfahren**		**Bestanden**	**Durchgefallen**	**Entfällt**	**Anmerkungen***
U1		Erfüllt die geforderte Herstellerdokumentation die Anforderung U1 (a-g)?				
U2		Wird die Software-Identifikation, wie in U2 gefordert, umgesetzt und dargestellt?				
U3		Wird bei der Befehlseingabe über die Nutzerschnittstelle unzulässige Einflussnahme auf die rechtlich relevante Software und die Messdaten verhindert?				
U4		Wird bei der Befehlseingabe über Kommunikationsschnittstellen des Gerätes unzulässige Einflussnahme auf die rechtlich relevante Software, die gerätespezifischen Parameter und die Messdaten verhindert?				

U5		Sind rechtlich relevante Software, gerätespezifische Parameter und Messdaten gegen zufälligen oder unbeabsichtigten Änderungen geschützt?				
U6		Sind rechtlich relevante Software und Messdaten gegen unzulässige absichtliche Modifizierungen oder Austausch geschützt?				
U7		Sind die gerätespezifischen Parameter, wie in U7 gefordert, geschützt?				
U8		Ist die Authentizität der dargestellten Messdaten gewährleistet?				
** Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.*						

12.4.3 Checkliste für spezifische Anforderungen aus Anhang O

Checkliste für Anforderungen von Anhang O						
Anforderung	**Prüfverfahren**		**Bestanden**	**Durchgefallen**	**Entfällt**	**Anmerkungen***
O1		Ist der Hardwareteil, auf dem das rechtlich relevante Betriebssystem läuft, gegen absichtliche Änderungen geschützt?				
O2		Für Komponenten der Kategorie 1 und komplette Geräte: Bietet der Bootvorgang die gleiche konfigurierte Umgebung für die Ausführung der rechtlich relevanten Software?				
O3		Stellt die Konfiguration des Betriebssystems sicher, dass genügend Ressourcen für den Betrieb der rechtlich relevanten Anwendung vorhanden sind?				
O4		Ist das Betriebssystem so konfiguriert, dass die rechtlich relevante Softwareanwendung nicht unzulässig durch Funktionen des Betriebssystems oder anderer Software beeinflusst werden kann?				
O5		Beeinflussen die über offene Schnittstellen zugänglichen Betriebssystemfunktionen nicht unzulässigerweise die rechtlich relevante Software, rechtlich relevante Parameter oder Messdaten?				
O6		Sind das Betriebssystem und die Konfiguration des Betriebssystems identifizierbar? Werden die Identifikation des Betriebssystems und die Identifikation der Konfiguration des Betriebssystems auf Befehl oder im Betrieb angezeigt?				
O7		Ist das Betriebssystem gegen absichtliche Modifizierungen geschützt?				
** Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.*						

12.4.4 Checkliste für spezifische Anforderungen aus Anhang L

Checkliste für Anforderungen von Anhang L						
Anforderung	**Prüfverfahren**		**Bestanden**	**Durchgefallen**	**Entfällt**	**Anmerkungen***
L1		Enthalten die gespeicherten Messdaten alle Informationen, die für rechtlich relevante Zwecke erforderlich sind?				

L2		Sind die gespeicherten Daten gegen zufällige und unbeabsichtigte Änderungen geschützt?				
L3		Sind die gespeicherten Daten gegen absichtliche Änderungen geschützt?				
L4		Sind die gespeicherten Messdaten auf die Messung und das Messgerät, das sie erzeugt hat, rückführbar?				
L5		Werden vertrauliche Informationen gegen Änderungen geschützt, geheim gehalten sowie vor Kompromittierung geschützt?				
L6		Gibt es ein rechtlich relevantes Modul oder eine Komponente für das Lesen, die Überprüfung, die Handhabung und die Anzeige gespeicherter Messdaten?				
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.*						

12.4.5 Checkliste für spezifische 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 gegen zufällige und unbeabsichtigte Änderungen geschützt?				
T3		Sind die übertragenen Daten gegen absichtliche Änderungen geschützt?				
T4		Sind die übertragenen Messdaten auf die Messung und die rechtlich relevante Komponente oder das Modul oder Messgerät rückführbar, die die Daten erzeugt haben?				
T5		Werden die vertraulichen Informationen gegen Änderungen geschützt und Kompromittierung geschützt sowie geheim gehalten?				
T6		Gibt es eine rechtlich relevante Komponente oder ein Modul für das Empfangen, Überprüfen, die Handhabung und Anzeige übertragener Messdaten?				
T7		Ist sichergestellt, dass die Messung durch eine Übertragungsverzögerung nicht unzulässig beeinflusst wird?				
T8		Ist sichergestellt, dass keine Messdaten verloren gehen, wenn Netzwerkdienste nicht mehr verfügbar sind?				
** Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.*						

12.4.6 Checkliste für spezifische Anforderungen aus Anhang S

Checkliste für Anforderungen aus Anhang S

Anforderung	Prüfverfahren		Bestanden	Durchgefallen	Entfällt	Anmerkungen*
S1		Gibt es einen Softwareteil, der die gesamte rechtlich relevante Software sowie sämtliche Parameter enthält und eindeutig von anderen Softwareteilen getrennt ist?				
S2		Wird die rechtlich relevante Anzeige von der rechtlich relevanten Software generiert und ist sie von der nicht rechtlich relevanten Anzeige klar unterscheidbar?				
S3		Erfolgen die Interaktion und der Datenaustausch zwischen der rechtlich relevanten und der nicht rechtlich relevanten Software über eine rückwirkungsfreie Schnittstelle?				
** Es sind Erklärungen erforderlich, wenn es Abweichungen von den Softwareanforderungen gibt.*						

12.4.7 Checkliste für spezifische Anforderungen aus Anhang D

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

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

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

13.1 Softwareanforderungen und ihr Bezug zur MID

Anforderung		MID	
Nr.	**Bezeichnung**	**Artikel / Anhang Nr.** (AI = Anhang I)	**Bezeichnung**
	Basis-Typ P		
P1	Dokumentation	AI-9.3 AI-12 Artikel 18	Am Gerät anzubringende bzw. dem Gerät beizulegende Informationen Konformitätsbewertung Technische Unterlagen
P2	Software-Identifikation	AI-7.6 AI-8.3	Eignung Schutz gegen Verfälschungen
P3	Einflussnahme über die Nutzerschnittstellen	AI-7.1	Eignung
P4	Einflussnahme über die Kommunikationsschnittstellen	AI-7.1 AI-8.1	Eignung Schutz gegen Verfälschungen
P5	Sicherung und Schutz der rechtlich relevanten Software und der gerätespezifischen Parameter	AI-7.1, AI-7.2 AI-8.4	Eignung Schutz gegen Verfälschungen
P6	Schutz von Software und Messdaten	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Eignung[16] Schutz gegen Verfälschungen
P7	Parameterschutz	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Eignung Schutz gegen Verfälschungen
P8	Dargestellte Messdaten	AI-7.1, AI-7.2, AI-7.6 AI-8.3 AI-10.2, AI-10.3, AI-10.4	Eignung Schutz gegen Verfälschungen Anzeige des Ergebnisses
	Basis-Typ U		
U1	Dokumentation	AI-9.3 AI-12 Artikel 18	Am Gerät anzubringende bzw. dem Gerät beizulegende Informationen Konformitätsbewertung Technische Unterlagen
U2	Software-Identifikation	AI-7.6 AI-8.3	Eignung Schutz gegen Verfälschungen
U3	Einflussnahme über die Nutzerschnittstellen	AI-7.1	Eignung
U4	Einflussnahme über die Kommunikationsschnittstellen	AI-7.1 AI-8.1	Eignung Schutz gegen Verfälschungen
U5	Sicherung und Schutz der rechtlich relevanten Software und der gerätespezifischen Parameter	AI-7.1, AI-7.2 AI-8.4	Eignung Schutz gegen Verfälschungen
U6	Schutz von Software und Messdaten	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Eignung Schutz gegen Verfälschungen
U7	Parameterschutz	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Eignung Schutz gegen Verfälschungen

[16] Anmerkung: Was den Inhalt betrifft, so handelt es sich bei Absatz 7.1 des MID-Anhangs I nicht um "Eignung", sondern um “Schutz gegen Verfälschungen" (Absatz 8)

Anforderung		MID	
Nr.	**Bezeichnung**	**Artikel / Anhang Nr.** (AI = Anhang I)	**Bezeichnung**
U8	Dargestellte Messdaten	AI-7.1, AI-7.2, AI-7.6 AI-8.3 AI-10.2, AI-10.3, AI-10.4	Eignung Schutz gegen Verfälschungen Anzeige des Ergebnisses
	Anhang O		
	Anhang L		
L1	Vollständigkeit der gespeicherten Messdaten	AI-7.1 AI-8.4 AI-10.2	Eignung Schutz gegen Verfälschungen Anzeige des Ergebnisses
L2	Sicherung und Schutz gespeicherter Messdaten	AI-7.1, AI-7.2 AI-8.4	Eignung Schutz gegen Verfälschungen
L3	Schutz gespeicherter Messdaten	AI-7.1 AI-8.4	Eignung Schutz gegen Verfälschungen
L4	Rückführbarkeit der gespeicherten Messdaten	AI-7.1 AI-8.4 AI-10.2	Eignung Schutz gegen Verfälschungen Anzeige des Ergebnisses
L5	Schutz vertraulicher Informationen	AI-7.1 AI-8.4	Eignung Schutz gegen Verfälschungen
L6	Abruf, Verifizierung und Anzeige gespeicherter Messdaten	AI-7.2 AI-10.1, AI-10.2, AI-10.3, AI-10.4	Eignung Anzeige des Ergebnisses
L7	Automatisches Speichern	AI-7.1 AI-8.4	Eignung Schutz gegen Verfälschungen
L8	Speicherkapazität und -dauer	AI-7.1	Eignung
Lx	Gesamter Anhang L	AI-11.1	Weiterverarbeitung von Daten zum Abschluss des Geschäftsvorgangs
	Anhang T		
T1	Vollständigkeit der übertragenen Messdaten	AI-7.1 AI-8.4	Eignung Schutz gegen Verfälschungen
T2	Sicherung und Schutz übertragener Messdaten	AI-7.1, AI-7.2 AI-8.4	Eignung Schutz gegen Verfälschungen
T3	Schutz übertragener Messdaten	AI-7.1 AI-8.4	Eignung Schutz gegen Verfälschungen
T4	Rückführbarkeit der übertragenen Messdaten	AI-7.1 AI-8.4	Eignung Schutz gegen Verfälschungen
T5	Schutz vertraulicher Informationen	AI-7.1 AI-8.4	Eignung Schutz gegen Verfälschungen
T6	Empfang, Verifizierung und Handhabung übertragener Messdaten	AI-7.1 AI-8.4	Eignung Schutz gegen Verfälschungen
T7	Übertragungsverzögerung	AI-7.1 AI-8.4	Eignung Schutz gegen Verfälschungen
T8	Verfügbarkeit von Übertragungsdiensten	AI-7.1 AI-8.4	Eignung Schutz gegen Verfälschungen
	Anhang S		
S1	Umsetzung der Softwaretrennung	AI-7.6 AI-10.1	Eignung Anzeige des Ergebnisses
S2	Gemischte Anzeige	AI-7.1, AI-7.2, AI-7.6 AI-10.2	Eignung Anzeige des Ergebnisses
S3	Rückwirkungsfreie Softwareschnittstelle	AI-7.6	Eignung
	Anhang D		
D1	Download-Mechanismus	AI-8.2, AI-8.4	Schutz gegen Verfälschungen

Anforderung		MID	
Nr.	**Bezeichnung**	**Artikel / Anhang Nr.** (AI = Anhang I)	**Bezeichnung**
D2	Authentifizierung der übertragenen Software	AI-7.6 AI-8.3, AI-8.4 AI-12	Eignung Schutz gegen Verfälschungen Konformitätsbewertung
D3	Schutz der heruntergeladenen Software	AI-7.1 AI-8.4	Eignung Schutz gegen Verfälschungen
D4	Rückführbarkeit des Downloads rechtlich relevanter Software	AI-7.1, AI-7.6 AI-8.2, AI-8.3 AI-12	Eignung Schutz gegen Verfälschungen Konformitätsbewertung
	Anhang I (Instrumentenspezifische Softwareanforderungen)		
I1-1, I2-1, I3-1, I4-1 I5-1	Fehlerbehebung	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Zuverlässigkeit Spezifische Anforderungen für Verbrauchszähler
I1-4, I2-3, I3-4, I4-4, I5-4	Backup-Einrichtungen	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Zuverlässigkeit Spezifische Anforderungen für Verbrauchszähler
I1-9, I2-9, I3-9, I4-9	Anzahl der Ziffernstellen	MI-002-5.3, MI-003-5.2	Spezifische Anforderungen für Verbrauchszähler
I1-6, I2-6, I3-6, I4-6	Rücksetzen kumulierter Messdaten verhindern	AI-8.5	Schutz gegen Verfälschungen
I1-2, I2-2, I3-2, I4-2. I5-2	Nicht rechtlich relevante Software und dynamisches Verhalten	AI-7.6	Eignung Schutz gegen Verfälschungen
I2-10	Lebensdauer der Energiequelle	MI-002-5.2	Spezifische Anforderungen für Gaszähler
I2-12	Elektronischer Mengenumwerter	MI-002-9.1	Spezifische Anforderungen für Gaszähler
I2-11	Prüfelement des Gaszählers	MI-002-5.5	Spezifische 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 Nummer**
	Artikel-Teil		
1, 2, 3		Keine besondere Softwarerelevanz	
4(b)	Definitionen, Anordnung von Teilgeräten	Übertragung der Messdaten… Grundleitfäden anwendbar auf Teilgeräte	T P, U
5 bis 9		Keine besondere Softwarerelevanz	
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, allgemeinen Software-Informationen. Anbringungsstelle für Siegel und Kennzeichnungen. Bedingungen für die Kompatibilität mit Schnittstellen und Teilgeräten.	P1, U1
11 bis 27		Keine besondere Softwarerelevanz	
	Anhang I		
AI-1 bis AI-5		Keine besondere Softwarerelevanz	
AI-6	Zuverlässigkeit	Fehlererkennung, Backup, Wiederherstellen, Neustart	I1-1, I1-2, I2-1, I2-2, I3-1, I3-2, I4-1, I4-2, I6-1, I6-2
AI-7	Eignung	Keine Merkmale zum Erleichtern betrügerischer Verwendung; minimale Möglichkeiten für unbeabsichtigte Fehlnutzung.	P3 – P8, U3 - U8, L1 – L5, L7, L8, T1 – T8, S2, D3, D4, I1-4, I2-8, I3-5, I4-4
AI-8	Schutz gegen Verfälschungen		
AI-8.1		Keine Beeinflussung durch den Anschluss von anderen Geräten.	P4, U4
AI-8.2		Schutz; Nachweis von Eingriffen	P6, P7, U6, U7, D1, D4
AI-8.3		Identifikation der Software; Nachweis von Eingriffen	P2, P6, P7, P8 U2, U6, U7, U8, D2, D4
AI-8.4		Schutz von gespeicherten oder übertragenen Daten	P5 - P7, U5 - U7, L1 - L5, T1 - T8 D1 - D3
AI-8.5		Kein Rücksetzen von kumulativen Registern	I1-3, I2-4, I3-4, I4-3
AI-9	Informationen, die auf dem Gerät angegeben oder mit ihm zusammen geliefert werden		

MID			Softwareleit-faden
Artikel / Anhang Nr. (AI = Anhang I)	**Bezeichnung**	**Anmerkung**	**Anforderung Nummer**
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	Anzeige des Ergebnisses		
AI-10.1		Anzeige mittels Displays oder Ausdrucks.	U8, L6, S2
AI-10.2		Bedeutung des Ergebnisses, keine Verwechslung mit zusätzlichen Anzeigen.	P8, U8, L1, L4, L6, S2
AI-10.3		Abdruck oder Aufzeichnung leicht leserlich und nicht löschbar.	P8, U8, L6, S2
AI-10.4		Für Direktverkäufe: Ergebnisanzeige für beide Parteien.	P8, U8, S2
AI-10.5		Für Verbrauchszähler: Display für den Kunden.	I1-3, I2-3, I3-3/4, I4-3
AI-11	Weiterverarbeitung von Daten zum Abschluss des Geschäftsvorgangs		
AI-11.1		Dauerhafte Aufzeichnung der Messergebnisse.	L1 - L8
AI-11.2		Dauerhafter Nachweis des Messergebnisses und Information zur Identifikation eines Geschäftsvorgangs.	L1, L6
AI-12	Konformitätsbewertung	Sofort mögliche 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 Wake-Up-Einrichtungen und Wiederherstellung	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	

MID			Softwareleit-faden
Artikel / Anhang Nr. (AI = Anhang I)	**Bezeichnung**	**Anmerkung**	**Anforderung Nummer**
MI-002-3.1	Elektromagnetische Störfes-tigkeit	Fehlerbehebung Backup-Einrichtungen Wake-Up-Einrichtungen und Wieder-herstellung	I2-1, I2-2
MI-002-3.1.3 bis MI-002-5.1		Keine besondere Softwarerelevanz	
MI-002-5.2	Eignung	Akzeptable Lösung zur Überwachung der Batterie-Lebensdauer	I2-5
MI-002-5.3	Eignung	Interne Auflösung	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	Zulässige Lösung für die Überwa-chung des Gasmengenumwerters	I2-6
MI-002-9.2 bis MI-002-10		Keine besondere Softwarerelevanz	
	Anhang MI-003		
MI-003-1 bis MI-003-4.2		Keine besondere Softwarerelevanz	
MI-003-4.3	Zulässige Auswirkung tran-sienter elektromagnetischer Phänomene	Fehlerbehebung Backup-Einrichtungen Wake-Up-Einrichtungen und Wieder-herstellung	I3-1, I3-2
MI-003-5.1		Keine besondere Softwarerelevanz	
MI-003-5.2	Eignung	Interne Auflösung	I3-3
MI-003-5.3 bis MI-003-7		Keine besondere Softwarerelevanz	
	Anhang MI-004		
MI-004-1 bis MI-004-4.1		Keine besondere Softwarerelevanz	
MI-004-4.2	Zulässige Einflüsse von elektromagnetischen Stör-größen	Fehlerbehebung Backup-Einrichtungen Wake-Up-Einrichtungen und Wieder-herstellung	I4-1, I4-2
MI-004-4.3 bis MI-004-7		Keine besondere Softwarerelevanz	
	Anhang MI-005		
	Anhang MI-006		

MID			Softwareleit-faden
Artikel / Anhang Nr. (AI = Anhang I)	**Bezeichnung**	**Anmerkung**	**Anforderung Nummer**
MI-006-IV, MI-006-V	Selbsttätige Waagen zum diskontinuierlichen und zum kontinuierlichen Totalisieren	Fehlererkennung Backup-Einrichtungen	I6-1, I6-2
	Anhang MI-007		
MI-007-8	Zulässige Einflüsse von elektromagnetischen Stör-größen	Backup-Einrichtungen	I7-1
	Anhang MI-008		
	Anhang MI-009		
	Anhang MI-010		

14 Bemerkungen zur Terminologie von Messungen

Anmerkung: Dieser informative Anhang soll die Begriffe und Definitionen im Zusammenhang mit dem Messprozess und deren Verwendung in diesem OIML-Dokument veranschaulichen.

In diesem Dokument ist die Definition von *Messergebnis* ein „Satz von Mengenwerten, die zusammen mit anderen relevanten Daten einer Messgröße zugeordnet werden“ (d. h. für das Messergebnis relevante Daten). Dies wird in Abbildung A.1 als gemessener Mengenwert (MQV) und messergebnisrelevante Daten (MRRD) dargestellt, die beide Teil des Messergebnisses sind.

Zusammen mit den Messprozessdaten (MPD) bilden diese die Messdaten.

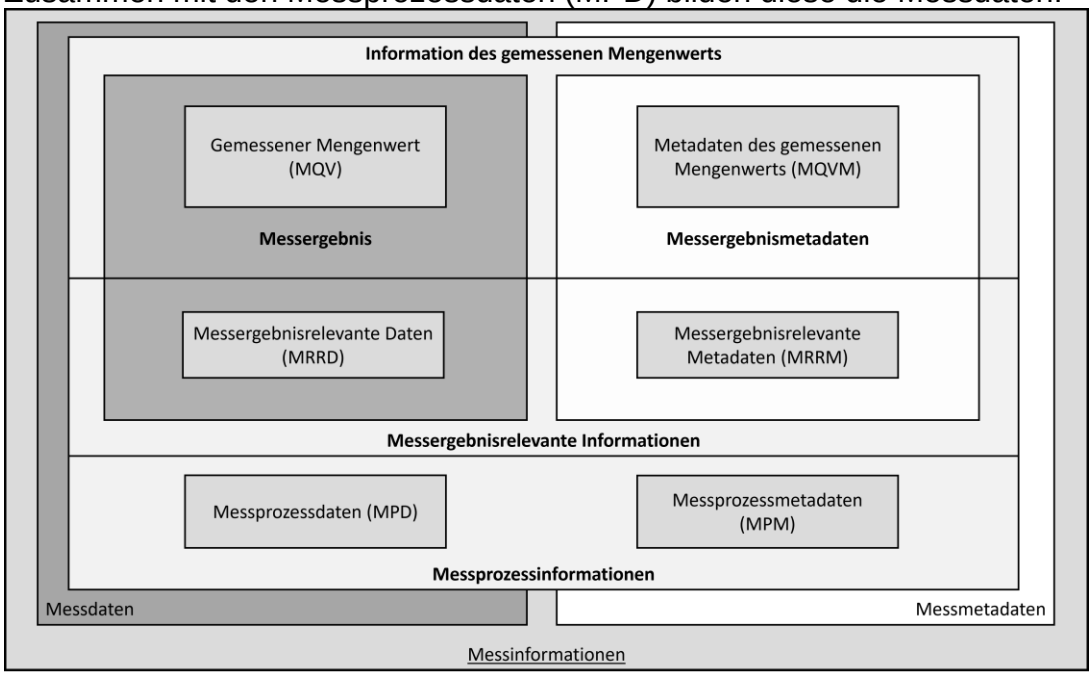


Abbildung A.1 – Visuelle Darstellung der Messinformationen

Im Allgemeinen wird in diesem OIML-Dokument zwischen Messdaten und Messmetadaten unterschieden. Werden beide zusammen verwendet, werden Messdaten in einen Kontext gesetzt; daher sind Messdaten plus Messmetadaten gleich Messinformationen.
Dieses OIML-Dokument unterscheidet außerdem zwischen messergebnisrelevanten Informationen und Messprozessinformationen.

Abbildung A.2 enthält ein Flussdiagramm zur Veranschaulichung der Unterscheidung zwischen den für das Messergebnis relevanten Daten und den für den Messprozess relevanten Daten.

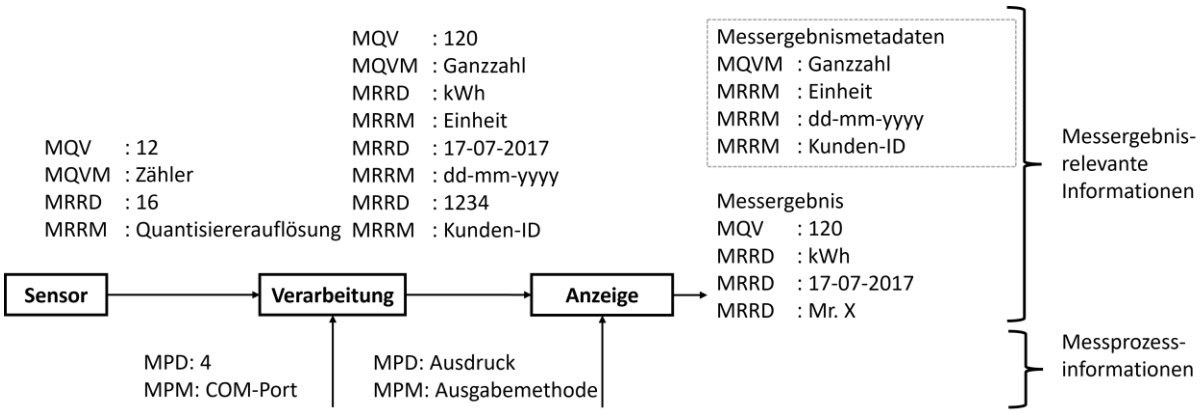


Abbildung A.2 – Flussdiagramm des Messprozesses, das Beispiele für verschiedene für das Messergebnis oder den Messprozess relevante Daten angibt

Abbildung A.2 illustriert außerdem die Daten, aus denen sich das Messergebnis zusammensetzt: gemessener Mengenwert (MQV) und für das Messergebnis relevante Daten (MRRD), während sich die entsprechenden Messergebnis-Metadaten, die für die korrekte Interpretation des Ergebnisses erforderlich sind, in einem gerahmten, gestrichelten Rechteck befinden.

Abbildung A.2 zeigt ein einfaches Beispiel für einen Messvorgang. Für jeden logischen Schritt (von der Datenerfassung durch den Sensor bis zur Anzeige des Ergebnisses) werden folgende Bestandteile notiert:

- der gemessene Mengenwert (MQV) und die Metadaten des gemessenen Mengenwerts (MQVM);
- die messergebnisrelevanten Daten (MRRD) und die messergebnisrelevanten Metadaten (MRRM);
- die Messprozessdaten (MPD) und die Messprozessmetadaten (MPM).

Ein Strang der Messinformationen bezieht sich auf die für das Messergebnis relevanten Informationen.

Die Datenerfassung durch den Sensor liefert einen rohen Zählerwert von 12 (MQV), wobei „Zähler“ das gemessene Mengenwert-Metadatum (MQVM) ist, welches zur Interpretation der Daten benötigt wird.

Die für das Messergebnis relevante Information (MRRI) ist die 16-Bit-Auflösung des Quantisierers des ADC.

- wobei 16 die für das Messergebnis relevanten Daten (MRRD) darstellt,
- während „Quantisiererauflösung“ das für das Messergebnis relevante Metadatum (MRRM) ist, das zur Interpretation der Daten benötigt wird.

Bei der Verarbeitung wird dem gemessenen Mengenwert (MQV) (mit „Ganzzahlwert“ als gemessene Mengenwert-Metadaten (MQVM)) „kWh“ als messergebnisrelevante Daten (MRRD) mit „Einheit“ als messergebnisrelevante Metadaten (MRRM) zugewiesen. Zusätzlich erhält der gemessene Mengenwert einen Zeitstempel „17.07.2017“ (MRRD) im Format „Tag-Monat-Jahr“ (MRRM) und Mister X (MRRD) als Kunden-ID (MRRM).

Sowohl bei der Erfassung durch den Sensor als auch während der Verarbeitung bilden die gemessenen Mengenwerte (MQV) und die für das Messergebnis relevanten Daten (MRRD) einen Teil des Messergebnisses, während die Metadaten für die korrekte Interpretation des Messergebnisses benötigt werden.

Ein weiterer Strang an Messinformationen hängt mit dem Messvorgang zusammen: Zur Erfassung des Messwerts (MQV) vom Sensor wird COM-Port Nummer 4 verwendet, wobei

- die Zahl „4“ die Messprozessdaten (MPD) darstellt und
- es sich beim „COM-Port“ um die Messprozess-Metadaten (MPM) handelt, die zum Verständnis des Datenelements erforderlich sind.

Die Anzeige des Ergebnisses kann durch eine Anzeige oder durch Ausdrucken erfolgen.

Das Messprozessdatum (MPD) „Drucken“ und die entsprechende „Anzeigemethode“ als Messprozessmetadatum (MPM) sind beide für den Messprozess erforderlich, werden jedoch weder Teil des Messergebnisses noch der Messergebnismetadaten.

Die Entscheidung darüber, was messergebnisrelevante Daten sind, obliegt den technischen Arbeitsgruppen, denn unter bestimmten Umständen können Messprozessdaten (MPD) zu messergebnisrelevanten Daten (MRRD) werden.

In dem in Abbildung A.2 gezeigten Beispiel verknüpft der COM-Port Nummer 4 den gemessenen Mengenwert (MQV) mit einem Kunden Herrn X und wandelt so während des Verarbeitungsschrittes die Messprozessdaten (MPD) in messergebnisrelevante Daten (MRRD) um.

15 Rechtlich relevante Eigenschaften

Ein rechtlich relevantes Messgerät kann über rechtlich relevante Software und unter bestimmten Voraussetzungen über nicht rechtlich relevante Software verfügen. Gleiches gilt für Parameter, Daten, Beschriftungen und Anzeigen. Sie können entweder rechtlich relevant oder unter bestimmten Voraussetzungen nicht rechtlich relevant sein.

Mit der obigen Definition kann festgestellt werden, ob Software, Parameter, Daten, Beschriftungen und Hinweise im Hinblick auf MID und NAWID rechtlich relevant sind. Im Folgenden werden einige Beispiele im Hinblick auf die Anwendung der Definition gegeben.

- Die Kennzeichnungen und Aufschriften, die den wesentlichen Anforderungen unterliegen, sind im Sinne der Definition rechtlich relevant.
- Die zur Sicherung von Messgeräten, Software, Parametern, Messdaten, Beschriftungen und Anzeigen eingesetzten Sicherungs- und Schutzeinrichtungen müssen den wesentlichen Anforderungen genügen und sind daher rechtlich relevant.
- Daten, ob gespeichert, übermittelt und/oder angezeigt, die zur Generierung des Messergebnisses verwendet werden, müssen die wesentlichen Anforderungen erfüllen und sind daher rechtlich relevant.

Hinweis: Rechtlich relevante Daten werden als Messdaten bezeichnet.

- Wenn eine Komponente zur Generierung, Speicherung und/oder Übertragung von Messdaten und/oder zur Anzeige des Messergebnisses verwendet wird, kann diese Komponente das Messergebnis beeinflussen und hat daher Einfluss auf die Einhaltung der Anforderungen und ist daher rechtlich relevant.
  - Zu den Komponenten zur Generierung der Messdaten gehören beispielsweise der Sensor, die analoge Datenverarbeitungseinheit und die digitale Datenverarbeitungseinheit;
  - Zu den Komponenten zum Speichern oder Übertragen von Messdaten gehören beispielsweise eine Festplatte und eine Netzwerkschnittstellenkarte;
  - Zu den Komponenten zur Anzeige der Messergebnisse gehören beispielsweise Display und Drucker.

Wenn ein Modul zur Generierung, Speicherung und/oder Übertragung von Messdaten und/oder zur Anzeige des Messergebnisses verwendet wird, kann dieses Modul das Messergebnis beeinflussen und somit einen Einfluss auf die Einhaltung der Anforderungen haben, daher ist es rechtlich relevant.

16 Verweise und Literatur

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

[2] RICHTLINIE 2014/32/EU DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 26. Februar 2014 zur Harmonisierung der Rechtsvorschriften der Mitgliedstaaten über die Bereitstellung von Messgeräten auf dem Markt (Neufassung). Amtsblatt der Europäischen Union L 96/149), 29.3.2014

[3] Richtlinie 2004/22/EG des Europäischen Parlaments und des Rates vom 31. März 2004 über Messgeräte. Amtsblatt der Europäischen Union L 135/1, 30.4.2004

[4] Internet Security Glossary, http://www.ietf.org/rfc/rfc2828.txt

[5] ISO/IEC JTC1/SC7 3941, 2008-03-14, http://pef.czu.cz/~papik/doc/MHJS/pdf/IT-VOCABULARY.pdf

17 Revisionshistorie

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

		satz widersprechen, wurden entfernt. Adressaten des Leitfadens: Der Leitfaden ist für Softwareentwickler und -prüfer bestimmt, kann jedoch auch von anderen Parteien verwendet werden, insbesondere von Marktaufsichtsbehörden, wo und wann immer es angebracht ist. Es hat sich herausgestellt, dass die Umsetzung der beiden vorherigen Aktualisierungen im Einzelnen viel redaktionelle Arbeit erfordert. Diese Änderungen führen zu einer besseren Lesbarkeit des Leitfadens, bedeuten jedoch keine technischen Spezifikationen. Software-Identifizierung (P2/U2): Im Leitfaden 7.2 wird nicht mehr gefordert, dass der Software-Identifikator von der Software selbst zur Verfügung gestellt wird. Es genügt, wenn gefordert wird, dass der Software-Identifikator gesichert vom Gerät zur Verfügung gestellt wird. Unterscheidung zwischen Identifikation und Integrität (P2/U2, P6/U6): MID Anhang 1 unterscheidet zwischen Identifikation der Software (Anhang 1, 7.6) und Integrität, z. B. Schutz der Software (Anhang 1, 8.4). Die Unterscheidung hat keine weniger strengen Anforderungen zur Folge. Unterstützung der Konformität mit der Bauart: Die für die Softwareintegrität erforderlichen technischen Mittel werden als geeignet für die Verwendung für Prüfung der Konformität mit der Bauart angesehen. Die erforderlichen Mittel sind z. B. Prüfsummen oder gleichwertige Mittel auf verschiedenen Ebenen für sämtliche Geräte der Risikoklasse C und höher. Risikoklassen: Risikoklasse C wurde geändert, so dass nun die gesamte rechtlich relevante Software für Geräte in Risikoklasse C als festgelegt gelten. Auf diese Weise wurden Unstimmigkeiten darüber beseitigt, welcher Softwareteil als festgelegt gilt. In Risikoklasse C und höher muss die Softwareidentität auf der Bit-Ebene (z. B. durch Prüfsummen) umgesetzt werden. Risikoklassifikation von Messgeräten mit Universalgeräten (Geräte vom Typ U): Aufgrund eines grundsätzlich höheren Risikos bei Geräten vom Typ U wird ihre Einteilung in Risikoklasse B als ungeeignet angesehen. Geräte vom Typ U können nur in Risikoklasse C und höher eingestuft werden. Akzeptable Sicherheitsmaßnahmen für höhere Risikoklassen (D und höher): Was Algorithmen und minimale Schlüssellängen anbetrifft, so müssen die Anforderungen oder Empfehlungen der nationalen und internationalen Institute, die für die Datensicherheit verantwortlich sind, berücksichtigt werden (z. B. NIST (USA), DCSSI (Frankreich), CESG (Vereinigtes Königreich), CCN (Spanien), NCSC (Niederlande), BSI (Deutschland)). Rechtlich relevante Software: Es scheint nicht mehr notwendig zu sein, zwischen rechtlich relevanter Software und fester rechtlich relevanter Software zu unterscheiden. Sämtliche in Anhang I aufgeführten Schutzanforderungen gelten für rechtlich relevante Software.
7	März 2018	Ergänzung von P7 um eine akzeptable Lösung, die sicherstellt, dass der Inhalt des Audit Trails auf der Anzeige dargestellt wird,

		wird hinzugefügt. Ergänzung von U8 und Einbindung der entsprechenden P8 zur allgemeineren Beschreibung von Kopplung und Handshake-Betrieb zwischen Einheiten. Verbesserte Anschaulichkeit von Anhang S mittels Streichung der Definition der Low-Level-/High-Level-Softwaretrennung.
8	April 2019	Redaktionelle Änderungen hinsichtlich des Übersetzungsabgleichs, Datenbereinigung, Erläuterung der Anwendung von Anhang T, Korrekturen in P6, U6, T2, T6 und L2 Umstrukturierung zwischen “Akzeptable Lösungen” and “Detaillierende Anmerkungen” für jede Anforderung. Die beiden instrumentenspezifischen Anhänge 10.2 Gaszähler und Mengenumwerter sowie 10.3 Elektrizitätszähler für Wirkverbrauch wurden vollständig überarbeitet. Kapitel 11.1 "In die Baumusterprüfbescheinigung einzubeziehende Informationen" wurde angepasst.
9	Oktober 2020	Revision der Anhänge 10.1 Wasserzähler, 10.4 Wärmezähler, 10.5 Messsysteme zur kontinuierlichen und dynamischen Mengenmessung von Flüssigkeiten außer Wasser und 10.7 Taxameter.
10	Juli 2021	Implementierung der Änderungen der Subgroup Terminologie, die im WG7 Meeting 2021 vorgestellt wurden. Umformulierung der Validierungsanleitung für Risikoklasse E („angemessen“ -> „korrekt“), wie beim WB7 Meeting 2019 vorgestellt.
11	März 2022	Ergänzung des „Anhang O“, der neue Anforderungen an Messgeräte mit Betriebssystemen detailliert beschreibt. Anschließend wurde der gesamte Leitfaden aktualisiert, um die neue Erweiterung zu integrieren. Mehrere Anforderungen im gesamten Dokument wurden präzisiert, um die Lesbarkeit zu verbessern und sie weniger mehrdeutig zu machen. Die technischen Spezifikationen bleiben gleich. Die Vorlage des Prüfberichts wurde aktualisiert.
12	März 2023	Implementierung der D31-Terminologie. Daraus resultierend wurden alle Anforderungen überarbeitet, um mit der neuen Terminologie übereinzustimmen. Weitere Klarstellung bezüglich Anhang O wurden im einleitenden Text vorgenommen. Die Checkliste für Anhang O wurde ebenfalls hinzugefügt.

Tabelle 14-1: Revisionshistorie