

Software-Anforderungen an Messgeräte und Zusatzeinrichtungen gemäß PTB-A 50.7 Geräteklasse 2: Gerät mit Datenübertragung über Kommunikationsnetzwerke	Anhang PTB-A 50.7-2
	April 2002*

Die folgenden Software-Anforderungen sind abgestimmt auf Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme und sind ein Anhang zur PTB-A 50.7. Sie sind abgeleitet aus dem WELMEC-Leitfaden 7.1 „Software“ [1] und beruhen damit auf der →MID, Anhang I und den messgeräte-spezifischen Anforderungen der Anhänge MI-001 bis MI-004 (siehe Vorwort des Hauptteils der PTB-A 50.7).

Die Anforderungen entsprechen den anerkannten Regeln der Technik. Sie wurden in schriftlicher Abstimmung von den Mitgliedern der Vollversammlung für das Eichwesen im April 2002 verabschiedet.

Dieser Anhang zur Anforderung A50.7 gilt für die folgenden im WELMEC-Leitfaden 7.1 definierten eichrechtlichen und technischen Kategorien (**Geräteklasse 2**):

Manipulationsschutz:	<i>mittel/hoch</i>
Prüftiefe:	<i>mittel</i>
Konformität:	<i>mittel</i>
Hardware-Konfiguration:	<i>Messgerät oder Zusatzeinrichtung in geschlossenem Gehäuse mit Schnittstellen, an offenem Datennetz angeschlossen (e), siehe Abb. 1 bis 4</i>
Bedienoberfläche:	<i>Nur eichpflichtige Betriebsart. (f)</i>
Laden von Software:	<i>Nicht vorgesehen. (i)</i>
Software-Struktur:	<i>Gesamte Software wird als eichpflichtig angesehen. (l)</i>
Software-Umgebung:	<i>Nicht variabel, die gesamte Software wurde zum messtechnischen Zweck konstruiert. (o)</i>
Fehlererkennung:	<i>Software-Fehlererkennung notwendig. (r)</i>
Langzeitspeicherung:	<i>Langzeitspeicherung von Messwerten vorgesehen. (t)</i>
Messprinzip:	<i>Kumulative Messungen und nicht-kumulative Messungen zu bestimmten Zeitpunkten. Nicht wiederholbare Messung. Einfache, statische Messung. (u/v, x, y)</i>

(Abkürzungen gemäß WELMEC-Leitfaden 7.1 [1])

Die Bauart eines Messgerätes oder einer Zusatzeinrichtung, die von diesen Anforderungen abweicht, wird zugelassen, wenn die gleiche Messsicherheit auf andere Weise gewährleistet ist. In diesem Fall werden die Anforderungen an die Bauart bei der Zulassung festgelegt (§ 16 Abs. 2 der Eichordnung).

* Ergänzung am 30.04.2010 zu Pkt. 1 auf S. 3

Inhalt

1	Vorbemerkung	3
1.1	Kryptologische Begriffe	3
2	Beschreibung der Geräteklasse 2	4
3	Spezifische Software-Anforderungen für Geräteklasse 2	7
3.1	Anforderungen an Funktionalität und Software-Struktur (A1)	7
3.1.1	Spezifikation der Grundanforderung A1.3	7
3.1.1.1	Software zur Bedienung von Hardware-Schnittstellen	7
3.1.1.2	Software zur Abfrage von Tastaturen und Tasten	8
3.2	Anforderungen zum Schutz gegen zufällige Informationsverfälschungen und Manipulationen und zur Vermeidung von Bedienungsfehlern (A2)	9
3.2.1	Spezifikation der Grundanforderung A2.1	9
3.2.1.1	Physikalische Effekte	9
3.2.1.2	Bedienungsfehler und falsche Messwertzuordnung	9
3.2.2	Spezifikation der Grundanforderung A2.2	10
3.2.2.1	Schutz gegen direkte Verfälschung von im Messgerät gespeicherten Messwerten	10
3.2.2.2	Gesicherte und setzbare Parameter	10
3.2.2.3	Schutz des Programmcodes	11
3.2.2.4	Schutz von übertragenen oder offen gespeicherten Daten	11
3.2.3	Spezifikation der Grundanforderung A2.3	12
3.2.4	Spezifikation der Grundanforderung A2.4	12
3.3	Anforderungen zur Konformität zwischen Bauartmuster und Seriengerät (A3)	13
3.3.1	Spezifikation der Grundanforderung A3.1	13
3.3.2	Spezifikation der Grundanforderung A3.2	13
3.4	Prüfbarkeit (A4)	15
3.4.1	Spezifikation der Grundanforderung A4.1	15
3.5	Geforderte Dokumentation zur Zulassungsprüfung (A5)	16
3.5.1	Spezifikation der Grundanforderung A5.1	16
4	Grundlegende Software-Anforderungen nach WELMEC-Leitfaden 7.1	18
5	Literatur	18

1 Vorbemerkung

Diese PTB-Anforderung ist eine gerätespezifische Interpretation der allgemeinen Software-Anforderungen im WELMEC-Leitfaden 7.1. Dieser Leitfaden enthält „Grundlegende Software-Anforderungen“, die aus dem Anhang I der →MID abgeleitet sind. Für die praktische Anwendung ist es notwendig, diese weiter zu interpretieren und zu detaillieren, wobei die verschiedenen Anwendungsbereiche der betreffenden Messgeräteart und technische Eigenschaften der Hardware und der Software berücksichtigt werden. Für jede Messgeräteart gibt es im Allgemeinen mehrere Varianten dieser Interpretationen.

Zur besseren Handhabung werden die vorkommenden Geräte in Klassen eingeteilt, für die es in Form eines Anhanges zusätzliche spezifische Anforderungen zur PTB-A 50.7 gibt. Der vorliegende Anhang PTB-A 50.7-2 enthält die Anforderungen für die Geräteklasse 2. Er ist anzuwenden, wenn das Messgerät oder die Zusatzeinrichtung die im Deckblatt dieses Anhanges aufgelisteten Eigenschaften aufweist. Die Anforderungen entsprechen weitgehend denjenigen, die an ein „einfaches Gerät“ gestellt werden (siehe Anhang PTB-A 50.7-1); lediglich die Anforderungen in Abschnitt 3.2.2.4 sind unterschiedlich.

Die Anforderungen werden im Folgenden ohne ausführliche Erläuterung aufgeführt. Als Interpretationshilfe steht ein separates Dokument „*Kommentare zu Software-Anforderungen PTB-A 50.7-2, Anhang 2 der PTB-A 50.7*“ zur Verfügung. Es enthält allgemeine Erläuterung zur Systematik des WELMEC-Leitfadens 7.1, Erklärungen der spezifischen Anforderungen für Geräteklasse 2, und Beispiele für technische Lösungen. (**Ergänzung am 30.04.2010: Dieser Kommentar ist leider nicht verfügbar.**)

Erklärungen von Begriffen sind dem WELMEC-Leitfaden 7.1, Abschnitt 2 und dem Hauptteil der PTB-A 50.7, Abschnitt 1 (Kennzeichnung mit „→“), zu entnehmen.

1.1 Kryptologische Begriffe

- Hash-Code** Ein Textblock wird mit einem Transformationsalgorithmus auf eine viel kürzere Zeichenkette abgebildet. Diese Zeichenkette heißt Hash-Code; sie kennzeichnet den Textblock eindeutig. Der Algorithmus ist darauf ausgerichtet, dass verschiedene Textblöcke mit großer Wahrscheinlichkeit einen anderen Hash-Code ergeben.
- Schlüssel** Große Zahl oder lange Zeichenkette, mit der ein Text durch einen Algorithmus verknüpft wird, um ihn für jemanden, der den Schlüssel nicht kennt, unlesbar zu machen.
- Signatur** Verschlüsselung eines →Hash-Codes.
Anmerkung: Meist wird unsymmetrische Verschlüsselung angewandt, das heißt, dass für Verschlüsselung (Signaturbildung) und Entschlüsselung (Signaturprüfung) verschiedene Schlüssel zum Einsatz kommen. Vorteilhaft ist, dass der zur Signaturprüfung beim Empfänger notwendige Schlüssel öffentlich sein darf, also nicht geheim gehalten zu werden braucht.
- Verschlüsselung** Transformation einer lesbaren Zeichenkette (Klartext) in eine nicht lesbare (Chiffre).
Anmerkung: Der Algorithmus, mit dem verschlüsselt wird, ist meist nicht geheim. Der Schlüssel, mit dem der Klartext verknüpft wird, muss jedoch geheim gehalten werden. Bei *symmetrischen Schlüsselssystemen* wird zur Rücktransformation vom Chiffre zum Klartext derselbe →Schlüssel verwendet. Bei *unsymmetrischen Schlüsselssystemen* sind es ein geheimer →Schlüssel und ein davon verschiedener öffentlicher Schlüssel, mit dem die entgegengesetzte Transformation durchgeführt wird.

2 Beschreibung der Geräteklasse 2

Im Folgenden werden typische Geräte, für die die in Abschnitt 3 definierten Anforderungen gelten sollen, beschrieben. Beispiele für derartige Geräte sind „Statische“ Elektrizitätszähler, elektronische →Zusatzeinrichtungen, Mengenumwerter, mikroprozessorgesteuerte Gas-, Wasser- und Wärmezähler usw. Aus Abb. 1 geht hervor, dass der grundsätzliche Aufbau der Geräte bei allen Messgerätearten und Zusatzeinrichtungen gleich ist, nur die Eingangsschaltungen zur Konvertierung der Eingangssignale unterscheiden sich abhängig von den zu messenden Größen oder sind bei Zusatzeinrichtungen überhaupt nicht vorhanden.

So zeigt Abb. 2 einen Impulsgeber mit Reed-Relais, typisch für Messgeräte, bei denen Umdrehungen von mechanischen Messwertaufnehmern gezählt werden. Die Impulse werden auf einen Zählbaustein geführt, der vom Mikrorechner ausgelesen werden kann.

Abb. 3 zeigt eine Kombination aus Impulsgeber und Analog-Digital-Wandlern wie sie bei Wärmezählern anzutreffen ist. Hier müssen zwei Größen gemessen werden, nämlich der Durchfluss des Heizwassers und die Temperaturdifferenz zwischen Vor- und Rücklauf. Man speist die Temperatur-Sensoren mit gepulstem Konstant-Strom und führt die am Sensor abfallende Spannung einem Analog-Digital-Wandler zu. Der Mikroprozessor berechnet aus den gemessenen Größen Volumen bzw. Volumenstrom und Temperaturdifferenz unter Berücksichtigung des Wärmekoeffizienten die thermische Energie und bringt sie zur Anzeige.

Abb. 4 zeigt einen Konverter mit Analog-Digital-Wandlern zur Messung der elektrischen Energie. Die Momentanwerte von Strom und Spannung werden in kurzen Abständen abgetastet und den Wandlern zugeführt. Der Mikroprozessor liest sie aus und berechnet die Spannungsverläufe, die momentane Leistung und die Energie sowie weitere elektrische Größen.

Das Gerät der Klasse 2 lässt sich mit den Begriffen des WELMEC-Leitfadens 7.1 folgendermaßen beschreiben (das Ergebnis dieser Klassifizierung ist auf dem Deckblatt in Kurzform wiedergegeben):

Geschlossenes Gehäuse, alle Komponenten des Gerätes sind innerhalb des Gehäuses, eine eichtechnische Sicherung des Gehäuses ist (falls erforderlich) möglich.

- Die Eingangsschaltungen der Geräte bestehen häufig aus mechanisch angetriebenen Impulsgebern (z. B. bei Elektrizitätszählern mit der Ferrarisscheibe gekoppelte Magnet-Reedrelais-Kombination) oder aus Analog-Digital-Wandlern.
- Der Digitalteil enthält neben dem Mikroprozessor / Mikrocontroller weitere Komponenten wie z.B. Programm- und Arbeitsspeicher, nicht flüchtige Datenspeicher, Timer, Watchdogs, Schnittstellen-Controller, LCD-/LED-Controller, LCD/LED als Anzeige.
- Die Zusatzeinrichtung enthält einen Messwertspeicher, der die Werte auch ohne externe Stromversorgung erhält.
- Die hier behandelte Geräte-Kategorie besitzt eine Schnittstelle zum Anschluss von sowohl eichpflichtigen als auch nicht eichpflichtigen Geräten. In der Anordnung gemäß Abb. 1 werden z.B. die vom Messgerät ermittelten Messwerte über ein Kommunikationsnetzwerk an eine Zusatzeinrichtung übertragen und dort für längere Zeit gespeichert. Anhand dieser gespeicherten Werte kann der Kunde die Rechnung überprüfen, die von der von der Eichpflicht ausgenommenen Zentrale erstellt worden ist. Die Datenübertragung erfolgt nach einem Protokoll entsprechend dem Stand der Technik, das die Möglichkeit bietet, die Anforderungen in Abschnitt 3.2.2.4 zur Sicherung der eichtechnisch relevanten Daten gegen Manipulationen zu erfüllen.

Anmerkung: Werden Messwerte nur zur nicht eichpflichtigen Weiterverarbeitung über die Schnittstelle an andere Geräte übertragen (unter Einhaltung der Bedingungen von §9 EO), so gelten die Anforderungen gemäß Anhang PTB-A 50.7-1.

- Das Gerät kann über die Schnittstelle parametrierbar werden. Die Anforderungen im Hauptteil PTB-A 50.7, Abschnitt 3.1.9 und den Tabellen 7-2 und 7-3 sind zu beachten.
- Die Software ist in nicht-flüchtigen Speichern abgelegt, die zur Programmierung ausgebaut werden müssen ((P)ROM, EPROM) oder deren Programmierung durch eine eichtechnische Sicherung verhindert werden kann.
- Die Software ist komplett für die Messaufgabe konstruiert, es gibt kein universelles Betriebssystem.
- Die gesamte Bedienoberfläche (d.h. die Darstellung von Messwerten und Daten und die Steuerung des Gerätes durch den Bediener z.B. durch Menüs) wird von der eichpflichtigen Software generiert.

- Die Software kann nicht eichpflichtige Teile enthalten. Diese sind in den eichpflichtigen Teil integriert. Die Software wird als Gesamtheit betrachtet und zugelassen. Jede Änderung der Software wird der Zulassungsstelle mitgeteilt.

Anmerkung: Der Hersteller hat die Wahl, die Software so zu konstruieren, dass nicht eichpflichtige Teile von den eichpflichtigen klar getrennt sind und die eichpflichtigen Funktionen und Daten nicht unzulässig beeinflussen. In diesem Fall werden an den nicht eichpflichtigen Software-Teil geringere Konformitätsanforderungen gestellt. Es gelten bei dieser Software-Konzeption die Anforderungen des Anhangs PTB-A 50.7-3.

- Als software-gesteuerte Fehlererkennung sind beispielsweise realisiert: Prüfsummen-Berechnung über Speicherbereiche, Watchdog-Kontrolle des Programm-Ablaufs.

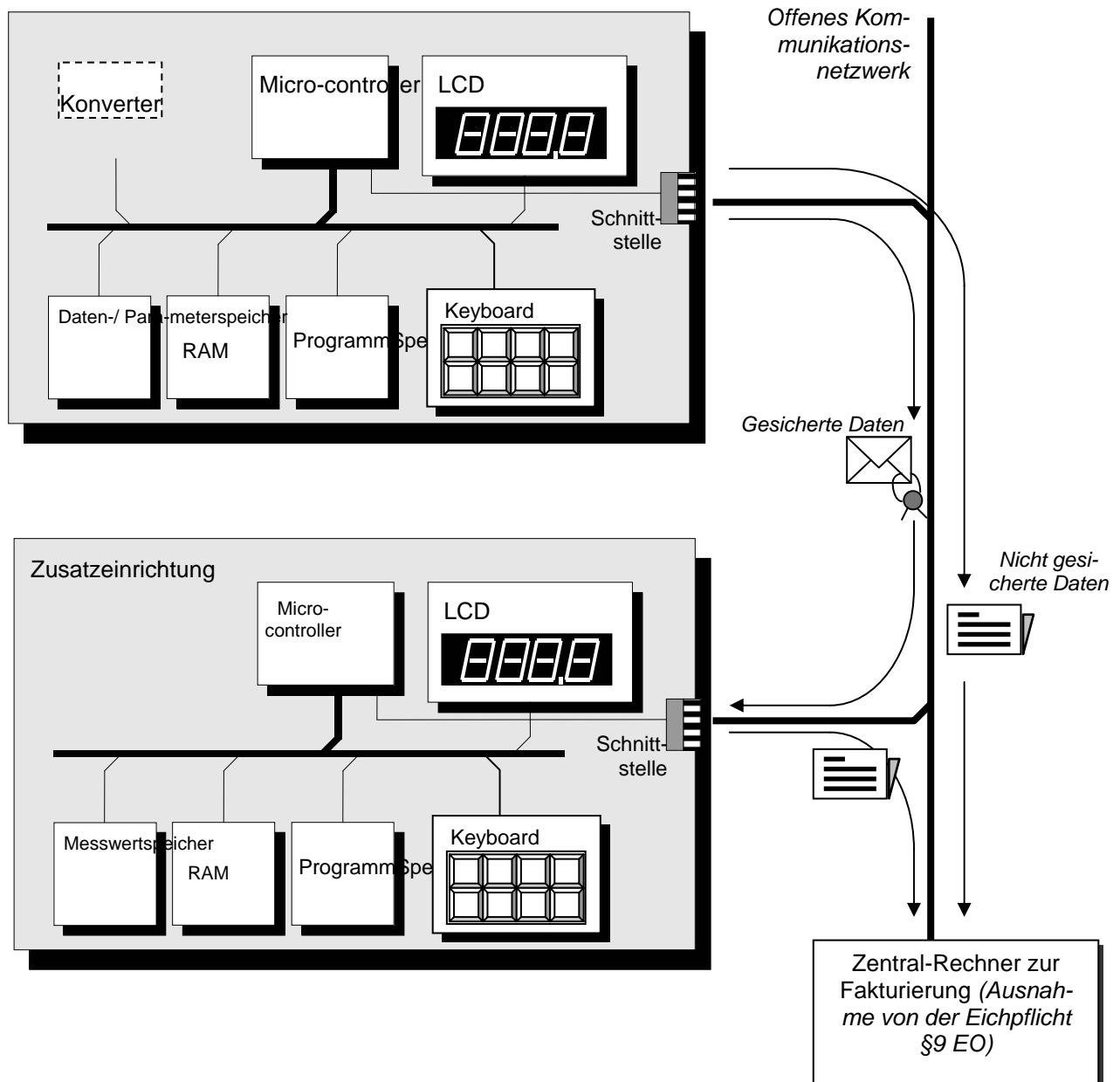


Abbildung 1: Beispiel für typische Hardware-Konfiguration der Geräteklasse 2 (Konverter siehe folgende Abbildungen)

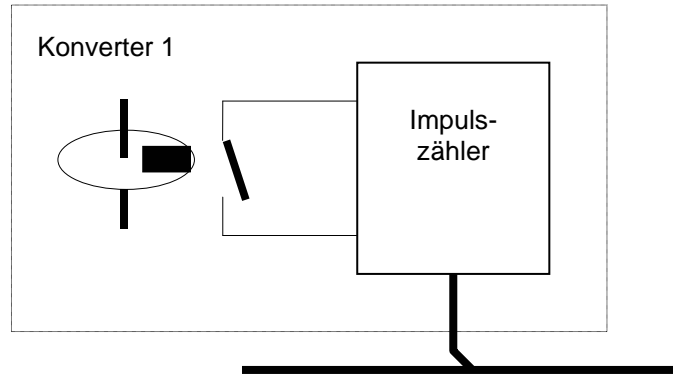


Abbildung 2: Beispiel für Messwertwandler (Konverter in Abb. 1) für Turbinenradzähler und Ferraris-Zähler

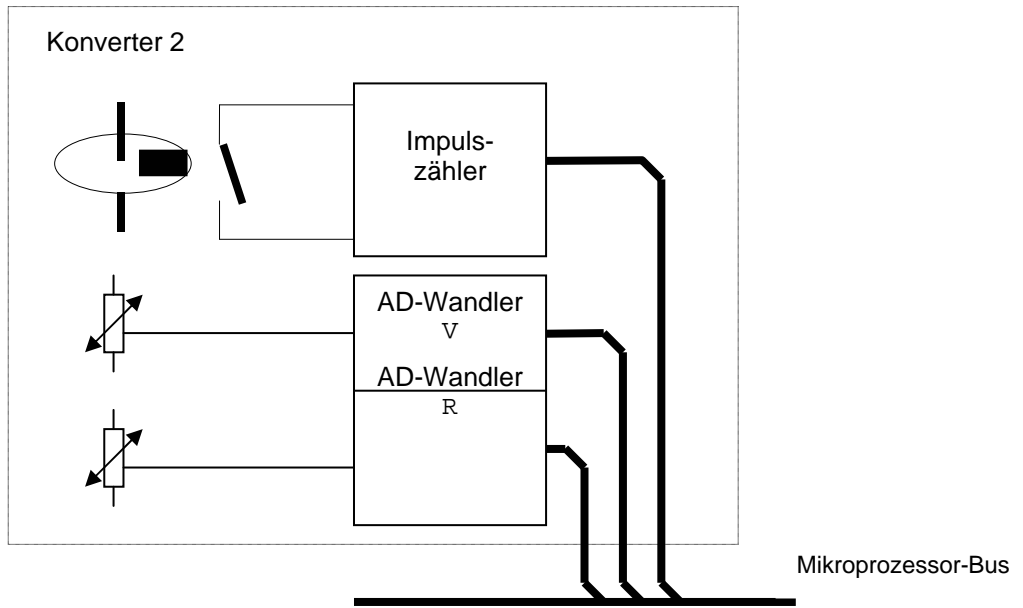


Abbildung 3: Beispiel für Messwertwandler eines Wärmezählers

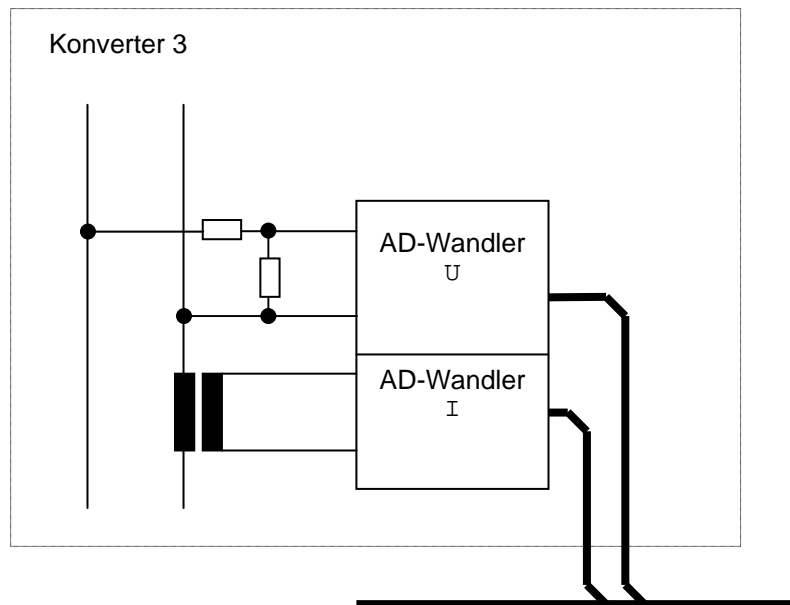


Abbildung 4: Beispiel für Messwertwandler eines elektronischen Elektrizitätszählers

3 Spezifische Software-Anforderungen für Geräteklasse 2

Anmerkung zur Schreibweise: Im Folgenden werden die grundlegenden Anforderungen des WELMEC-Leitfadens (siehe Tabelle 4-1, Seite 18) in doppelt gerahmten Kästen zitiert und die daraus abgeleiteten spezifischen Anforderungen in einfachen Kästen dargestellt. Die Nummerierung der einzelnen spezifischen Anforderungen bezieht sich auf die Nummern der grundlegenden Anforderungen des WELMEC-Leitfadens 7.1.

Aus den grundlegenden Anforderungen wurden neben den spezifischen Anforderungen an die Geräteeigenschaften auch Anforderungen an die Verfahrensweise bei der Zulassungsprüfung (Beispiel VZ1.3-1) und bei der Eichung (Beispiel VE1.3-1) und Anforderungen an den Software-Hersteller (Beispiel VH1.3-1) abgeleitet.

3.1 Anforderungen an Funktionalität und Software-Struktur (A1)

Anmerkung: Die Anforderungen A1.1 und A1.2 (s. Tabelle 4-1, Seite 18) sind bei der hier behandelten Geräteklasse nicht relevant.

3.1.1 Spezifikation der Grundanforderung A1.3

WELMEC 7.1:

A1.3 Die eichpflichtige Software muss so konstruiert sein, dass sie nicht unzulässig über die Schnittstellen des Gerätes beeinflusst werden kann.

Hinsichtlich ihrer Funktionalität sind Software-Teile, die Eingaben über Schnittstellen und die Eingaben über Tastaturen ermöglichen ähnlich. Deshalb wird die Grundanforderung A1.3 nicht nur auf die Bedienung von Hardware-Schnittstellen (Abschnitt 2.1.1.1) sondern sinngemäß auch auf Tasten- bzw. Tastatur-Eingabe (Abschnitt 2.1.1.2) angewandt.

3.1.1.1 Software zur Bedienung von Hardware-Schnittstellen

Nahezu jedes softwaregesteuerte Messgerät ist heute mit Schnittstellen ausgestattet, weil z.B. Messwerte von anderen Geräten verwendet werden um einen Prozess zu steuern oder weil das Messgerät von anderen Geräten gesteuert werden soll. Über Eingangs- und Ausgangsschnittstellen dürfen →eichtechnische relevante Funktionen und Daten nicht unzulässig beeinflusst werden (Hauptteil PTB-A 50.7, Abschnitt 3.1.3). Die Ausgabe-Richtung ist nicht kritisch aber bei der Eingabe ergeben sich zwei Probleme:

- Die Messwerte könnten über die Schnittstelle beeinflusst werden. Manipulationen könnten möglich sein, wenn die Software, die Schnittstellenbefehle empfängt dies zulässt.
- Für den Prüfer ist es nicht möglich, direkt zu prüfen, ob Manipulationen verhindert werden, da sich die Prüfung auf die Dokumentation der Software und nicht auf den Quellcode abstützt.

Deshalb sind folgende spezifische Anforderungen und Anweisungen erforderlich:

A1.3-1 Alle über Schnittstellen des Gerätes empfangenen Befehle dürfen Daten und Funktionen des Gerätes nur in zulässiger Art und Weise beeinflussen:

- Es muss einen Programm-Teil geben, der die empfangenen Befehle interpretiert. Dieser Befehlsinterpreter muss alle möglichen Befehle einteilen in gültige und ungültige. Gültig sind alle, denen er eine Bedeutung zuordnen kann, ungültig ist der Rest.
- Alle ungültigen Befehle dürfen keine Wirkung auf Daten und Funktionen des Gerätes haben.

Anforderung an den Hersteller

Es muss eine detaillierte Dokumentation zur Verfügung gestellt werden, von allen Befehlen und Daten, die über die Schnittstelle übertragen werden können (siehe Anforderung VH5.1-3 in Abschnitt 3.5.1). Zusätzlich ist die folgende Versicherung seitens des Herstellers notwendig:

- | |
|---|
| <p>VH1.3-1</p> <ul style="list-style-type: none">• <i>Der Hersteller muss bestätigen, dass der Befehlsinterpretierer alle gültigen Schnittstellen-Befehle erkennt und andere ausfiltert.</i>• <i>Die Bedeutung und Wirkung aller gültigen Schnittstellen-Befehle muss dokumentiert werden.</i>• <i>Der Hersteller muss bestätigen, dass die Dokumentation gemäß VH5.1-3 vollständig ist.</i> |
|---|

Anforderung zur Zulassungsprüfung

Es ist die Aufgabe des Prüfers zu entscheiden, ob ein gültiger Befehl zulässig ist oder nicht.

- | |
|---|
| <p>VZ1.3-1 <i>Bei der Zulassungsprüfung wird beurteilt, ob alle dokumentierten gültigen Befehle zulässig sind.</i></p> |
|---|

Es ist möglich, dass einige Befehle aufgrund des Ergebnisses der Prüfung von gültig auf ungültig klassifiziert werden müssen, mit der Konsequenz, dass sie nun vom Schnittstellen-Kommandointerpreter ausgefiltert werden müssen.

Wenn das Messgerät oder die Zusatzeinrichtung keine Datenschnittstelle besitzt oder wenn die Schnittstelle eichtechnisch verschlossen werden soll, sind die genannten Anforderungen nicht anzuwenden.

3.1.1.2 Software zur Abfrage von Tastaturen und Tasten

Wie oben erwähnt, wird die Grundanforderung A1.3 auch auf Tasten- bzw. Tastatur-Eingabe angewandt. Es ergeben sich die folgenden spezifischen Anforderungen und Anweisungen:

- | |
|--|
| <p>A1.3-2</p> <p><i>Alle über Schalter, Tasten oder Tastaturen eingebbaren Befehle dürfen Daten und Funktionen des Gerätes nur in zulässiger Art und Weise beeinflussen.</i></p> <ul style="list-style-type: none">• <i>Es muss einen Programm-Teil geben, der die eingegebenen Tastaturbefehle interpretiert. Dieser Befehlsinterpretierer muss alle möglichen Befehle einteilen in gültige und ungültige. Gültig sind alle, denen er eine Bedeutung zuordnen kann, ungültig ist der Rest.</i>• <i>Alle ungültigen Befehle dürfen keine Wirkung auf Daten und Funktionen des Gerätes haben.</i> |
|--|

Anforderung an den Hersteller

Es muss eine detaillierte Dokumentation zur Verfügung gestellt werden, von allen Befehlen und Daten, die eingegeben werden können (siehe Anforderung VH5.1-3 in Abschnitt 3.5.1). Zusätzlich ist die folgende Versicherung seitens des Herstellers notwendig:

- | |
|---|
| <p>VH1.3-2</p> <ul style="list-style-type: none">• <i>Der Hersteller muss bestätigen, dass der Befehlsinterpretierer alle gültigen Tastaturbefehle erkennt und andere ausfiltert.</i>• <i>Die Bedeutung und Wirkung aller gültigen Tastaturbefehle muss dokumentiert werden.</i>• <i>Der Hersteller muss bestätigen, dass die Dokumentation vollständig ist.</i> |
|---|

Anforderung zur Zulassungsprüfung

Es ist die Aufgabe des Prüfers zu entscheiden, ob ein gültiger Befehl zulässig ist oder nicht.

VZ1.3-2 *Bei der Zulassungsprüfung wird beurteilt, ob alle dokumentierten gültigen Befehle zulässig sind.*

Es ist möglich, dass einige Befehle aufgrund des Ergebnisses der Prüfung von gültig auf ungültig klassifiziert werden müssen, mit der Konsequenz, dass sie nun vom Kommandointerpreter ausgefiltert werden müssen.

Wenn das Messgerät oder die Zusatzeinrichtung keine Vorrichtung zur manuellen Eingabe besitzt oder wenn diese eichtechnisch gesichert werden soll, sind die genannten Anforderungen nicht anzuwenden.

3.2 Anforderungen zum Schutz gegen zufällige Informationsverfälschungen und Manipulationen und zur Vermeidung von Bedienungsfehlern (A2)

3.2.1 Spezifikation der Grundanforderung A2.1

WELMEC 7.1:
A2.1 *Eichpflichtige Programme und Daten müssen gegen zufällige und unabsichtliche Veränderungen geschützt werden.*

Es gibt drei Gründe für unzulässige Änderungen der Software im Sinne dieser Anforderung: physikalische Effekte, Fehlbedienung und - im weiteren Sinne - falsche Zuordnung eines Messwertes zu einer bestimmten Messung.

3.2.1.1 Physikalische Effekte

Wenn das betreffende Gerät entsprechend den einschlägigen Vorschriften auf Verträglichkeit mit den Umgebungsbedingungen getestet worden ist (elektromagnetische Verträglichkeit, Temperatur, Feuchte usw.) brauchen physikalische Effekte als Ursache für Informationsverfälschungen grundsätzlich nicht angenommen zu werden (Ausnahme: siehe Anforderung A2.4).

3.2.1.2 Bedienungsfehler und falsche Messwertzuordnung

Die folgende Definition der spezifischen Anforderung A2.1-1 deckt Verfälschungen von Daten und falsche Zuordnung von selbst unverfälschten eichtechnisch relevanten Daten ab. Es ist möglich, dass der Kunde gespeicherte Messwerte, die Basis der Abrechnung sind, wegen der Komplexität des Messgerätes nicht überprüfen kann:

A2.1-1 *Die Software muss so konstruiert sein, dass die Gefahr von (unabsichtlichen) Bedienungsfehlern gering ist und dass Fehlbedienungen nicht zu einer Verfälschung oder falschen Zuordnung von Messwerten führen (§ 40 EO). Insbesondere muss eine Anzeige der verrechnungsrelevanten Werte und die eindeutige Zuordnung zum jeweiligen Posten in einer Rechnung mit einfachen Mitteln möglich sein.*

Verfälschungen von →eichtechnisch relevanten Daten sind bei der gegebenen Geräteklassifizierung (geschlossenes Gehäuse, kein Laden von Software, kein Betriebssystem mit Bedienoberfläche) nur möglich durch das eichpflichtige Programm des Messgerätes oder der →Zusatzeinrichtung. Wenn aber Anforderungen A1.3-1 und A1.3-2 vom eichpflichtigen Programm erfüllt werden, kann die *Verfälschung* von →eichtechnisch relevanten Daten durch Bedienungsfehler ausgeschlossen werden.

Das Gerät soll die unabsichtliche falsche *Zuordnung* eines Messwertes zu einer Messung durch den →Kunden bei dem Versuch, die in Rechnung gestellten Messwerte an Messgerät oder →Zusatzeinrichtung zu verifizieren, verhindern. Das Gerät muss alle →eichrechtlich relevanten Werte aus dem Langzeitspei-

cher lesen und zur Anzeige bringen können. Die Messwerte müssen durch einen Zeitstempel und falls erforderlich durch zusätzliche Kennzeichnungen - z.B. eine laufende Nummer - identifizierbar gemacht werden. Die Kennzeichnungen müssen in der Rechnung wiederzufinden sein. (Vergleiche hierzu Abschnitt 3.1.1.3 im Hauptteil der PTB-A 50.7).

3.2.2 Spezifikation der Grundanforderung A2.2

WELMEC 7.1:

A2.2 *Eichpflichtige Programme und Daten müssen gegen absichtliche Veränderungen durch nicht autorisierte Personen geschützt werden.*

Verfälschungen von Messwerten mit Betrugsabsicht können versucht oder erzielt werden durch:

- direkten Zugriff auf im Messgerät gespeicherte Messwerte
- direkten Zugriff auf Messwerte, die übertragen oder offen gespeichert werden
- indirekt durch Änderung der Parameter des Messgerätes
- indirekt durch Änderung des Programmcodes.

3.2.2.1 Schutz gegen direkte Verfälschung von im Messgerät gespeicherten Messwerten

Bei der hier behandelten Geräteklasse (geschlossenes Gehäuse, kein Laden von Software, kein Betriebssystem mit Bedienoberfläche) ist der direkte Zugriff auf im Messgerät gespeicherte Daten (Messwerte, Parameter) nur dem implementierten Programm möglich. Wenn die spezifischen Anforderungen A1.3-1 und A1.3-2 erfüllt werden, kann die direkte Manipulation von Messwerten und Parametern ausgeschlossen werden. Eine zusätzliche spezifische Anforderung ist nicht notwendig.

3.2.2.2 Gesicherte und setzbare Parameter

Es ist typisch für softwaregesteuerte Zähler und →Zusatzeinrichtungen, dass die Eigenschaften durch eine große Zahl von Parametern eingestellt werden können. Parameter werden eingeteilt in solche, die bei der Eichung gesichert werden müssen, und solche, die vom →Messgerätebesitzer nach der Eichung eingestellt werden können („→ungesicherte Parameter“, siehe Tabellen 7-2 und 7-3 im Hauptteil der PTB-A 50.7). Der →Messgerätebesitzer kann eine eigene Sicherung gegen Missbrauch vorsehen. Weitere Anforderungen zu Parametern sind in den Abschnitten 3.3.1 und 3.3.2 zu finden).

- A2.2-1**
- →Gesichert parametrierbare Größen müssen durch eichtechnische Sicherung gegen Veränderungen geschützt werden können und/oder durch einen Eintrag in das →eichtechnische Logbuch nachvollziehbar gemacht werden.
 - Dagegen können eichtechnisch nicht relevante Größen ungesichert sein (siehe VZ3.2-1). Ungesicherte Größen brauchen nicht durch eine eichtechnische Sicherung geschützt bzw. durch Logbuch-Eintrag nachvollziehbar gemacht zu werden.
 - Ausgewählte, bei der Zulassung freigegebene Größen dürfen auch per Datenfernübertragung gesetzt werden (siehe VZ3.2-1).

Anforderung an die Durchführung der Eichung

VE2.2-1 *Bei der Eichung müssen Parameter, die nicht durch Anforderung VZ3.2-1 ausgeschlossen sind, eichtechnisch gegen Veränderung geschützt werden und / oder die Einträge im →eichtechnischen Logbuch sind zu prüfen.*

3.2.2.3 Schutz des Programmcodes

Das Ändern des Programmcodes des geeichten Messgeräts bzw. der geeichten →Zusatzeinrichtung ist unzulässig. Die Eigenschaften der hier behandelten Geräteklasse (geschlossenes Gehäuse, kein Laden von Software, kein Betriebssystem mit Bedienoberfläche) erlaubt nicht die direkte Änderung des Programmcodes z.B. über die Tastatur oder das Laden von Code über eine Schnittstelle, wenn die Software entsprechend den Anforderungen A1.3-1 und A1.3-2 realisiert ist. Ein anderer Weg die Programme des Messgerätes oder der →Zusatzeinrichtung unzulässig zu verändern wäre der Austausch des Programm-Speichers. Die folgende Anforderung soll unzulässige Programm-Änderungen ausschließen:

A2.2-2 *Programcode muss gegen unzulässige Veränderung oder Laden durch eine eichtechnische Sicherung geschützt werden. Das Laden über Schnittstellen oder Einbringen von Programcode über austauschbare Speichermedien ist nicht zulässig.*

Anforderung an die Durchführung der Eichung

VE2.2-2 *Bei der Eichung muss der Programm-Speicher gesichert werden.*

(Abhängig von der technischen Lösung und praktischen Ausführung muss das Gehäuse, der Speicher selbst oder eine Schreibschutz-Vorrichtung des Speicher-Schaltkreises eichtechnisch gesichert werden.)

3.2.2.4 Schutz von übertragenen oder offen gespeicherten Daten

Wenn Messwerte über offene Kommunikationsnetzwerke übertragen oder offen gespeichert werden mit dem Ziel, sie später weiter für gesetzlich geregelte Zwecke zu verwenden, müssen die Daten gegen zwei Arten von Verfälschungen geschützt werden:

- a) Empfangene Daten können während Übertragung oder Speicherung verfälscht worden sein, d.h. die *Daten-Integrität* kann verletzt sein.
- b) Empfangene Daten können von einem unbekanntem oder nicht autorisiertem Absender stammen. Das empfangende Gerät muss in die Lage versetzt werden, die *Authentizität* einer Nachricht zu überprüfen und das empfangende Gerät muss in die Lage versetzt werden, zu erkennen, ob die empfangene Nachricht bereits früher einmal gesendet, von einem nicht berechtigten Teilnehmer empfangen und zwischengespeichert und anschließend unverfälscht noch einmal gesendet worden ist (Prüfung der *Daten-Aktualität*).

Die spezifischen Anforderungen A2.2-3 bis A2.2-7 verlangen Schutzmaßnahmen gegen diese Verfälschungen.

A2.2-3 *Über offene Kommunikationsnetzwerke übertragene oder auf frei zugänglichen Speichern gespeicherte eichpflichtige Daten müssen gegen Verfälschungen geschützt werden:*

- *Die Manipulation der Daten muss erkennbar sein.*
- *Bewusste Fehlleitung oder Verzögerung und nicht autorisiertes Einspeisen der Daten in das System muss verhindert werden oder für das empfangende Gerät erkennbar sein.*
- *Die übertragenen Messwerte müssen eindeutig einer Messung zugeordnet werden können.*
- *Die einer Messung zugeordneten eichtechnisch relevanten Daten müssen zu einer Datenstruktur zusammengefasst werden („Eichtechnischer Datensatz“).*

Der Schutz der Daten wird typischerweise durch Berechnung von →Signaturen oder durch →Verschlüsselung realisiert. Vom eichtechnischen Standpunkt ist eine →Verschlüsselung der Messwerte normalerweise nicht notwendig; es ist ausreichend, wenn der Empfänger oder Verwender der Messwerte Verfälschungen *erkennen kann*: Es braucht nur eine →Signatur über die Daten gebildet zu werden und die Daten selbst können in einem lesbaren Format übertragen werden.

Für zwei Manipulationsschutz-Niveaus wurden unterschiedliche Anforderungen definiert (mittleres Niveau: A2.2-4, hohes Niveau: A2.2-5). Das hohe Niveau wird bei Übertragung über das Internet verlangt, das mittlere Niveau kann ausreichen, wenn andere Schutzmaßnahmen im System realisiert sind.

A2.2-4 (mittleres Schutz-Niveau) Über alle Daten eines eichtechnischen Datensatzes muss eine Prüfzahl berechnet werden, mit einem Algorithmus, der sicherstellt, dass sich keine gleiche Prüfzahl für unterschiedliche Datensätze ergibt¹. Die minimale Schlüssellänge beträgt 2 Bytes.

A2.2-5 (hohes Schutz-Niveau) Über alle Daten eines eichtechnischen Datensatzes muss eine Prüfzahl berechnet werden, mit einem Algorithmus, der dem Stand der Technik entspricht². Die minimale Schlüssellänge beträgt 20 Bytes.

A2.2-6 Kryptografische →Schlüssel, Algorithmen usw. müssen gegen Verfälschung geschützt werden.

A2.2-7 Kryptografische Daten und Algorithmen, auf denen die Sicherheit beruht, müssen geheim gehalten und gegen unbefugtes Ausspähen geschützt werden.

Anforderung an den Hersteller

Je nach vorausgesetztem Schutzniveau muss sich der Hersteller an Anforderung VH2.2-1 (mittleres Niveau) oder VH2.2-2 (hohes Niveau) halten.

VH2.2-1 (mittleres Schutz-Niveau) Der Hersteller ist verpflichtet, Algorithmen, →Schlüssel usw., auf denen die Sicherheit von übertragenen oder gespeicherten Daten beruht, geheim zu halten.

VH2.2-2 (hohes Schutz-Niveau) Das Schlüsselmanagement muss entsprechend dem Stand der Technik realisiert werden.

Um die Anforderung VH2.2-2 erfüllen zu können, muss ein unabhängiges Trust Centre zur Schlüsselverwaltung und –Vergabe (*Schlüsselmanagement*) eingeschaltet werden, sofern ein unsymmetrisches Schlüssel-System zum Einsatz kommt.

3.2.3 Spezifikation der Grundanforderung A2.3

WELMEC 7.1:
A2.3 Nur die zugelassene und geeichte Software darf für gesetzlich geregelte Zwecke verwendet werden. Es muss klar und eindeutig sein, dass eine Messwert-Darstellung von einem zugelassenen Programm erzeugt wird.

Diese Anforderung wird durch Abschnitt 3.1 im Hauptteil der PTB-A 50.7 abgedeckt.

3.2.4 Spezifikation der Grundanforderung A2.4

WELMEC 7.1:
A2.4 Funktionsfehler in softwaregesteuerter Hardware, die Messwerte verfälschen können, müssen erkannt werden und auf den Fehler muss eine Reaktion zur Fehlerbehandlung erfolgen.

Wenn Daten oder Programmcode für lange Zeit (mehrere Monate oder Jahre) gespeichert werden, ist die Wahrscheinlichkeit für eine Verfälschung durch physikalische Effekte nicht mehr vernachlässigbar. Deshalb müssen Fehler aufgrund zufälliger Effekte in der Hardware von Langzeitspeichern erkannt werden:

¹⁾ Z.B. CRC-Algorithmus [2]

²⁾ Z.B. Hash-Algorithmus SHA-1 [3,4] + Verschlüsselungsalgorithmus IDEA [5]

A2.4-1 Bei eichpflichtigen Programmen und Daten in Langzeitspeichern müssen Informationsverfälschungen durch zyklische automatische Prüfungen erkennbar gemacht werden.

3.3 Anforderungen zur Konformität zwischen Bauartmuster und Seriengerät (A3)

3.3.1 Spezifikation der Grundanforderung A3.1

WELMEC 7.1:

A3.1 Die Software darf nach der Zulassung nicht unzulässig verändert werden.

Die folgenden spezifische Anforderungen und Anweisungen setzen diese Grundanforderung in das verlangte Konformitätsniveau um:

A3.1-1 Die implementierte Software jedes Seriengerätes muss identisch mit der des Bauartmusters sein.

Anforderung an den Hersteller

Der Hersteller muss die folgende Anforderung beachten:

VH3.1-1 Die Zulassungsstelle muss über jede Änderung der Software informiert werden. Geänderte Software darf nicht installiert werden, bevor die Zulassungsstelle zugestimmt hat. Wenn Änderungen vorgenommen worden sind, muss die Software-Dokumentation aktualisiert werden.

Anforderung zur Zulassungsprüfung

Die Zulassungsstelle muss die folgende Anforderung beachten:

VZ3.1-1 Die zugelassene Dokumentation und der vollständige ausführbare Programmcode des Bauartmusters werden bei der Zulassungsstelle in einer Form hinterlegt, die einen Vergleich der Software der Seriengeräte mit der des Baumusters ermöglicht. Bei der Zulassung wird ferner festgelegt, ob der Quellcode ebenfalls hinterlegt werden muss.

Anmerkung: Wenn Funktionen der Software über (->gesicherte) Parameter eingestellt werden können, legt die Zulassungsstelle fest, welche einstellbaren Funktionen (Varianten), geprüft und zugelassen werden müssen.

3.3.2 Spezifikation der Grundanforderung A3.2

WELMEC 7.1:

A3.2 Für die Durchführung der Eichung der eichpflichtigen Software müssen geeignete Anweisungen zur Verfügung stehen.

Das Problem bei der Eichung von softwaregesteuerten Geräten ist, dass viele der Eigenschaften nicht unmittelbar geprüft werden können. Die Eichung muss sich auf die Ergebnisse der Zulassungsprüfung und die Annahme abstützen, dass der Hersteller die Konformitätsanforderungen befolgt. Die Beschaffenheitsprüfung bei der Eichung beschränkt sich deshalb im Normalfall auf die Überprüfung der Software-Identität und die richtige Einstellung von Parametern. Die folgenden spezifischen Anforderungen und Anweisungen sollen eine effektive und sichere eichtechnische Prüfung möglich machen (siehe auch Hauptteil PTB-A 50.7, Abschnitt 3.1.9).

A3.2-1 a) *Die Software-Identifikation muss automatisch unmittelbar vor der Anzeige aus dem ausführbaren Programmcode berechnet werden.*

ODER

b) *Als Software-Identifikation wird die Software-Versionsnummer verwendet. In diesem Fall muss genau dokumentiert sein, wie die Versionsnummer aufgebaut ist. Jede Änderung der Software muss zu einer Änderung der Versionsnummer führen.*

Anmerkung: Grundsätzlich besteht nach WELMEC Leitfaden 7.1 bei Konformitätsniveau „mittel“ die Forderung der **Identität** zwischen Software des Baumusters und des Seriengerätes. Bei der Zulassung wird festgelegt, welche Form der Software-Identifikation notwendig ist.

A3.2-3 *Können Funktionen der Programme über Parameter eingestellt werden, so muss jede Parametrier-Variante (siehe unten) identifizierbar sein. Die Identifikation besteht entweder aus*

a) *einer berechneten Prüfzahl (→Signatur) über die relevanten Parameterwerte.*

ODER

b) *einer Versionsnummer für den Parametersatz. In diesem Fall muss genau dokumentiert sein, wie die Versionsnummer aufgebaut ist. Jede Änderung eines Parameters muss zu einer Änderung der Versionsnummer führen.*

Wenn es sich nur um wenige Parameter handelt, ist keine spezielle Identifikation erforderlich. Anforderung A3.2-4 (Anzeige) gilt dann für jeden einzelnen Parameter-Wert.

Anmerkung: Eine **Parametrier-Variante** ist ein Satz von Parameterwerten. Dabei handelt es sich um Parameter, mit denen sich eichrechtlich relevante Eigenschaften und Funktionen des Gerätes definieren lassen. Mit den Werten der Parameter werden die Eigenschaften und Funktionalitäten des Gerätes festgeschrieben.

Im Allgemeinen sind hier andere, sehr von der programm-technischen Lösung abhängige Parameter gemeint, als die in den Tabellen 7-2 und 7-3 im Hauptteil genannten. Bei großem Umfang der Parametrier-Möglichkeiten entspricht die „Parametrierung“ eines Gerätes eher einer Programmierung, so dass Parametrier-Varianten eichrechtlich wie unterschiedliche Programm-Versionen behandelt werden müssen.

Die Anmerkung zu A3.2-1 gilt hier sinngemäß.

A3.2-4 *Die Software- bzw. Parameter-Identifikation muss*

a) *auf Anforderung (z.B. über die Tastatur des Messgerätes) oder automatisch zyklisch angezeigt werden*

ODER

b) *wenn es technisch nicht möglich ist, auf dem Typenschild angebracht werden.*

Anforderung zur Zulassungsprüfung

Die Zulassungsstelle muss die folgenden Anweisungen beachten:

VZ3.2-1 Die Liste der Parameter (siehe VH5.1-5) muss geprüft werden. Alle Parameter müssen klassifiziert werden in solche, die eichtechnisch →gesichert werden müssen und solche, die nach der Eichung ohne Verletzung einer eichtechnischen Sicherung bzw. ohne Logbuch-Eintrag eingestellt werden dürfen („→ungesicherte Parameter“, siehe Hauptteil PTB-A 50.7, Abschnitt 3.1.9). Von den ungesicherten Parametern können aufgrund des Prüfergebnisses einzelne ausgewählt werden, die auch „→fernparametrierbar“, d.h. über die Schnittstelle und Datenfernübertragung ohne Anwesenheit eines Monteurs einstellbar sein dürfen.

VZ3.2-2 Die Zulassungsstelle muss eine Anleitung zur eichtechnischen Prüfung erstellen, sofern diese nicht in der Prüfregel beschrieben ist. Diese Anleitung enthält im Allgemeinen die folgenden Punkte:

- eine Liste der Schnittstellen, die gesichert werden müssen und eine Liste der Schnittstellen, die ungesichert bleiben dürfen
- eine Liste der Programm-Speicher, die gegen Austausch gesichert werden müssen
- eine Beschreibung der Schreibschutz-Vorrichtung für Programm- und Parameter-Speicher, die gesichert werden müssen
- eine Liste aller Parameter und ihrer Sollwerte, die bei der Eichung überprüft und gesichert werden müssen
- den Sollwert der Software-Identifikation
- eine Schritt-für-Schritt-Anleitung auf der Basis der Hersteller-Dokumentation, die angibt, wie die Software-Identifikation und Parameter-Werte und ggf. das Logbuch zur Anzeige gebracht werden können.

Anforderung an die Durchführung der Eichung

Bei der Beschaffenheitsprüfung im Rahmen der Eichung bzw. Befundprüfung sind die folgenden Anweisungen einzuhalten:

VE3.2-1 Die Beschaffenheitsprüfung ist auf der Basis der Anforderung VZ3.2-2 durchzuführen.

VE3.2-2 Schnittstellen, Programm- oder Parameter-Speicher usw. die in der Anforderung VZ3.2-2 nicht erwähnt sind, müssen eichtechnisch gesichert werden. Im Zweifelsfall darf das Gerät nicht geeicht werden.

3.4 Prüfbarkeit (A4)

3.4.1 Spezifikation der Grundanforderung A4.1

WELMEC 7.1:

A4.1 Die Funktionalität des Messgerätes muss prüfbar sein.

Für Zähler und Zusatzeinrichtungen, die z.B. Lastgänge speichern oder Maxima im Abrechnungsintervall berechnen leitet sich die folgende Anforderung an den Hersteller aus der Grundanforderung A4.1 ab:

VH4.1-1 Wenn die Software neue Messwerte ermittelt, die es erforderlich machen, das Gerät über große Zeiträume zu beobachten, müssen Hilfsmittel zur Verfügung gestellt oder im Gerät implementiert werden, die es erlauben, Algorithmen innerhalb einer vertretbaren Zeit zu prüfen.

VH4.1-2 Wenn eine große Anzahl von Parametern zu prüfen ist, muss die Software eine Prüfzahl über die eichtechnisch relevanten Parameter bilden oder es muss eine Versionsnummer für diese Parametrier-Variante geben (vergleiche Anforderung A3.2-3). Prüfzahl oder Versionsnummer müssen am Gerät anzeigbar sein, so dass ein Soll-Ist-Vergleich einer einzigen Zahl erforderlich ist, um den gesamten Parametersatz zu überprüfen.

VH4.1-3 Wenn am Gerät eine Schnittstelle zum Parametrieren vorhanden ist, muss entweder zusätzlich zu den aktuell eingestellten eichtechnisch relevanten Parametern die Soll-Merkmalisliste mit der Ur-Parametrierung im Gerät abgespeichert sein

ODER

die ursprüngliche Parametrierung muss anhand eines →eichtechnischen Logbuches lückenlos nachvollziehbar sein

ODER

die Urparametrierung muss dem Gerät in Papierform beigegeben werden (vergleiche Hauptteil Abschnitt 3.1.9.2).

3.5 Geforderte Dokumentation zur Zulassungsprüfung (A5)

3.5.1 Spezifikation der Grundanforderung A5.1

WELMEC 7.1:

A5.1 Die eichpflichtige Software muss einschließlich ihrer Hardware- und Software-Umgebung in geeigneter Weise dokumentiert sein.

Anforderung an den Hersteller

Diese Grundanforderung richtet sich an den Hersteller. Die Dokumentation soll die folgenden Punkte beinhalten (einige sind in bestimmten Fällen nicht relevant):

VH5.1-1 Beschreibung der Software-Umgebung

- Block-Schaltbild der Hardware des Messgerätes oder der →Zusatzeinrichtung

VH5.1-2 Beschreibung der Software-Struktur und –Funktionen

Diese Beschreibung soll den Prüfer in die Lage versetzen, die Struktur der Software, den Ablauf der Datenverarbeitung, die Funktionen der einzelnen Software-Teile und die Bedeutung von Daten zu verstehen. Die Beschreibung kann aus den folgenden Dokumenten bestehen (siehe Kommentar zu dieser Anforderung [8]):

- Beschreibung der in Software realisierten Funktionen
- Beschreibung der Software-Struktur, wenn möglich in grafischer Form z.B. als Nassi-Shneidermann-Diagramm, Aufruf-Hierarchie-Plan ...
- Zeitdiagramm von (quasi-)parallelen Prozessen / Funktionen

VH5.1-3 Beschreibung von Kommando-Interpretern

Für Module, die Kommandos von Tastaturen, Schnittstellen usw. empfangen und interpretieren (siehe Kommentar zu dieser Anforderung [8]):

- Liste aller Kommandos und Beschreibung ihrer Bedeutung und Wirkung auf Funktionen und Daten des Messgerätes oder der →Zusatzeinrichtung (= gültige Kommandos)
- Darstellung, welche Datenflüsse über den betreffenden Interpreter laufen, d.h. welcher Schnittstelle oder Tastatur der Interpreter zugeordnet ist.

VH5.1-4 Beschreibung von Datensätzen

Wenn Datenübertragung über offene Kommunikationsnetzwerke oder offene Speicherung realisiert wird, müssen Messwerte und andere relevante Daten in Datensätzen organisiert sein. Es ist zu beschreiben:

- alle Felder des Datensatzes, ihre Bedeutung, ihr Typ, gegebenenfalls zulässige Wertebereiche
- Signatur-Algorithmus und Schlüssellänge
- Sicherungsmaßnahmen im Gerät um das Ausspähen von geheimen Informationen (z.B. Schlüssel) zu verhindern

VH5.1-5 Beschreibung der Parameter (siehe Hauptteil PTB-A 50.7, Tabellen 7.2 und 7.3)

- Alle Parameter, die eingestellt werden können, müssen zusammen mit einer Erklärung der Bedeutung aufgelistet werden. Falls erforderlich können zulässige Wertebereiche angegeben werden.
- Parameter, deren Veränderung nach der Eichung möglich sein soll, können vom Hersteller genannt werden („→ungesicherte Parameter“).
- Parameter, deren Veränderung per Datenfernübertragung über eine Schnittstelle nach der Eichung möglich sein soll, können vom Hersteller genannt werden („→fernparametrieren“).
- Falls ein →eichtechnisches Logbuch realisiert ist, muss die Struktur und Bedeutung der Einträge beschrieben sein. Eine Anleitung zum Auslesen muss gegeben werden und ein Probeausdruck des Logbuches ist beizufügen.

VH5.1-6 Beschreibung der Bedienoberfläche

- Bedienungsanleitung
- Beschreibung von Menüs und Dialogen, bei komplizierten Eingabe-Prozeduren sollte ein grafischer Dialog-Plan erstellt werden.
(Zur Dokumentation des Kommando-Interpreters siehe VH5.1-3)

VH5.1-7 Bestätigungen, Versicherungen

- Bestätigung, dass die Dokumentation von Hardware- und Software-Schnittstellen und Tastatur-Kommandos vollständig ist und dass alle Kommandos, die nicht in der Dokumentation erwähnt wurden ungültige Kommandos sind.
- Bestätigung, dass alle über Schnittstellen und Tastaturen empfangenen ungültigen Kommandos ausgefiltert werden und keine Wirkung auf Funktionen und Daten des Gerätes haben.

VH5.1-8 Allgemeines

- Bezug auf die Punkte dieser Anforderungen in der Dokumentation.
- Nennung des Sollwertes der Software-Identifikation.

4 Grundlegende Software-Anforderungen nach WELMEC-Leitfaden 7.1

Anforderungs-Nr.	Grundlegende Software-Anforderungen
Software-Funktionalität und -Struktur	
A1.1	Die Software eines Messgerätes muss so konstruiert sein, dass eine einfache Auswertung bezüglich der Übereinstimmung mit den folgenden Software-Anforderungen möglich ist.
A1.2	Die eichpflichtige Software muss so konstruiert sein, dass sie nicht unzulässig von anderer Software beeinflusst werden kann.
A1.3	Die eichpflichtige Software muss so konstruiert sein, dass sie nicht unzulässig über die Schnittstellen des Gerätes beeinflusst werden kann.
Software-Schutz	
A2.1	Eichpflichtige Programme und Daten müssen gegen zufällige und unabsichtliche Veränderungen geschützt werden.
A2.2	Eichpflichtige Programme und Daten müssen gegen absichtliche Veränderungen durch nicht autorisierte Personen geschützt werden.
A2.3	Nur die zugelassene und geeichte Software darf für gesetzlich geregelte Zwecke verwendet werden. Es muss klar und eindeutig sein, dass eine Messwert-Darstellung von einem zugelassenen Programm erzeugt wird.
A2.4	Funktionsfehler in softwaregesteuerter Hardware, die Messwerte verfälschen können, müssen erkannt werden und auf den Fehler muss eine Reaktion erfolgen.
Software Konformität	
A3.1	Die Software darf nach der Zulassung nicht unzulässig verändert werden.
A3.2	Für die Durchführung der Eichung der eichpflichtigen Software müssen geeignete Anweisungen zur Verfügung stehen.
Prüfbarkeit	
A4.1	Die Funktionalität des Messgerätes muss prüfbar sein.
Dokumentation für die Zulassungsprüfung	
A5.1	Die eichpflichtige Software muss einschließlich ihrer Hardware- und Software-Umgebung in geeigneter Weise dokumentiert sein.

Tabelle 4-1: Grundlegende Software-Anforderungen (WELMEC 7.1)

5 Literatur

- [1] WELMEC Guide 7.1 „Software Requirements on the Basis of the Measuring Instruments Directive“, 1999 – <http://www.welmec.org/publicat.htm>
- [2] ISO 3309, CCITT X.25
- [3] National Institute of Standards and Technology (NIST). FIPS PUB 180-1: Secure Hash Standard SHA-1, April 1995 – <http://csrc.nist.gov/fips/fip180-1.txt> (ascii)
- [4] H. Dobbertin, A. Bosselaers, B. Preneel; RIPEMD-160 – A strengthened Version of RIPEMD, BSI, Bonn; Katholische Universität, Leuven, 1996
- [5] IDEA – X. Lai, J. Massey, S. Murphy, Markov Ciphers and Differential Cryptanalysis, Proceedings of Eurocrypt'91, LNCS 547, Springer Verlag, Berlin
- [6] CC – Common Criteria ISO/IEC 15408 – Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik
- [7] ITSEC – Information Technology Security Evaluation Criteria 1991
- [8] Kommentare zu Software-Anforderungen PTB-A 50.7-2, Anhang 2 der PTB-A 50.7, PTB, 2002