

WELMEC-Leitfaden 7.4

Beispielhafte Anwendungen des WELMEC-Leitfadens 7.2

Version 2022

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.



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:
www.welmec.org

Inhalt

Vorwort	4
Einleitung	5
1 Begriffe	6
2 Nutzung dieses Leitfadens	7
2.1 Allgemeine Struktur des Leitfadens	7
2.2 Passende Teile des Leitfadens wählen	7
3 Verallgemeinerte Architektur eines Messgeräts	8
3.1 Abgeleitete verallgemeinerte Architektur eines Messgeräts.....	8
4 Beispielhafte Anwendungen.....	8
4.1 Externe Speichereinheit, verbunden mit einem „Muttergerät“	8
4.1.1 Annahmen zum „Muttergerät“	8
4.1.2 Anwendbare Anforderungen für die externe Speichereinheit	9
4.1.3 Beschreibung der akzeptablen Lösung.....	9
4.1.4 Zuordnung von Anforderungen zu Merkmalen der akzeptablen Lösung	11
4.2 Externe Anzeigeeinheit, verbunden mit einem „Muttergerät“	12
4.2.1 Annahmen zum „Muttergerät“	12
4.2.2 Anwendbare Anforderungen für die Anzeigeeinheit	12
4.2.3 Beschreibung der akzeptablen Lösung.....	12
4.2.4 Zuordnung von Anforderungen zu Merkmalen der akzeptablen Lösung	13
4.3 Anhang D: Download von rechtlich relevanter Software	14
4.3.1 Beschreibung der akzeptablen Lösung.....	14
4.3.2 Zuordnung von Anforderungen zu Merkmalen der akzeptablen Lösung	15
4.4 Anhang O: Komponente der Kategorie 1	16
4.4.1 Annahmen zum Gerät	17
4.4.2 Anwendbare Anforderungen für das Messgerät	17
4.4.3 Beschreibung der akzeptablen Lösung.....	17
4.4.4 Zuordnung von Anforderungen zu Merkmalen der akzeptablen Lösung	17
4.5 Anhang O: Komponente der Kategorie 2.....	18
4.5.1 Annahmen zum Messgerät	18
4.5.2 Anwendbare Anforderungen für das Messgerät	19
4.5.3 Beschreibung der akzeptablen Lösung für den PC	19
4.5.4 Zuordnung von Anforderungen zu Merkmalen der akzeptablen Lösung	19
5 Referenzen und zusätzliche Literatur	20
6 Revisionshistorie	20

Vorwort

Dieser Leitfaden basiert auf dem WELMEC-Leitfaden 7.2: Softwareleitfaden [1].

Dieser Leitfaden spiegelt die aktuelle Position der WELMEC WG 7 Software wider. Da der WELMEC-Leitfaden 7.2 die Struktur der MID widerspiegelt, müssen auch die instrumentenspezifischen Anforderungen berücksichtigt werden. Diesbezüglich können andere WELMEC-Arbeitsgruppen zusätzliche formelle oder technische Anforderungen an einzelne Messgeräteklassen stellen.

Dieser Leitfaden hat rein empfehlenden Charakter und führt seinerseits keinerlei Beschränkungen oder zusätzliche technische Anforderungen ein, die über die in der MID 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 genutzt werden sollte.

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

Anmerkung: Dieser Leitfaden gilt für die Richtlinien 2004/22/EG und 2014/32/EU [2] [3].

Einleitung

Dieses Dokument bietet technische Hilfestellung für die Anwendung der Messgeräterichtlinie (MID).

Es bezieht sich insbesondere auf Messgeräte, die mit Software ausgestattet sind, und kann daher auf eine Vielzahl an Messgeräten angewandt werden.

Der vorliegende Leitfaden ist zur Verwendung in Verbindung mit dem WELMEC-Leitfaden 7.2 bestimmt. Er bietet beispielhafte akzeptable Lösungen für bestimmte Gerätearchitekturen (siehe WELMEC-Leitfaden 7.3 [4]) und zeigt, wie diese akzeptablen Lösungen die Anforderungen des WELMEC-Leitfadens 7.2 erfüllen. Dabei werden auch die Anforderungen des WELMEC-Leitfadens 7.2 auf technischer Ebene dargestellt.

Dieser Leitfaden geht nur auf akzeptable Lösungen auf technischer Ebene, nicht auf die Architekturebene ein (siehe WELMEC-Leitfaden 7.3).

Der Detaillierungsgrad orientiert sich an den Bedürfnissen der Hersteller von Messgeräten und von Benannten Stellen (BS), die Konformitätsbewertungen von Messgeräten nach Modul B durchführen.

Wenn diesem Leitfaden gefolgt wird, kann davon ausgegangen werden, dass die softwarebezogenen Anforderungen der MID erfüllt sind. Es kann ferner davon ausgegangen werden, dass alle Benannten Stellen diesen Leitfaden als konforme Auslegung der MID in Bezug auf Software akzeptieren. Für eine Übersicht, wie die in diesem Leitfaden aufgestellten Anforderungen mit den entsprechenden Anforderungen in der MID zusammenhängen, siehe Querverweise im WELMEC-Leitfaden 7.2 [1]

Aktuelle Informationen zu Leitfäden und der Arbeit der WELMEC-Arbeitsgruppe 7 stehen auf der Webseite www.welmec.org zur Verfügung.

1 Begriffe

Für in diesem Leitfaden genutzte allgemeine softwarebezogene Begriffe, siehe Kapitel „Begriffe“ im WELMEC-Leitfaden 7.2 [1]. Definitionen für alle anderen Begriffe sind unten genannt.

Muttergerät (Mother Unit): Messgerät oder Teil eines Messgeräts, das entsprechende Softwareanforderungen erfüllt. Jedoch sind eine oder mehrere Funktionalitäten, die im WELMEC-Leitfaden 7.2 beschrieben sind, in eine andere Komponente verlagert. Die getrennte Komponente und das Muttergerät erfüllen gemeinsam alle Anforderungen von WELMEC-Leitfaden 7.2.

2 Nutzung dieses Leitfadens

Dieser Leitfaden beschreibt sowohl spezifische Konfigurationen von Messgeräten als auch die Hardwarekomponenten und Softwaremodule, aus denen die Messgeräte zusammengesetzt sind. Jede spezifische Konfiguration, auch als „akzeptable Lösung“ bezeichnet, wird individuell beschrieben. Der Leitfaden bietet außerdem Beschreibungen der damit verbundenen Anforderungen, die für eine bestimmte Konfiguration gelten.

2.1 Allgemeine Struktur des Leitfadens

Der Leitfaden ist wie folgt gegliedert. Zuerst wird in Kapitel 3 kurz das modulare Konzept des WELMEC-Leitfadens 7.2 erläutert und es wird auf die Funktionalität der ausgewählten Module des Konzepts eingegangen. Als zweites werden in Kapitel 4 spezifische technische Realisierungen diskutiert. Aus jeder Realisierung wird eine Liste mit geltenden Anforderungen abgeleitet. Danach wird gezeigt, wie die geltenden Anforderungen durch die beschriebenen Realisierungen erfüllt werden. Kapitel 5 listet die Referenzen sowie zusätzliche Literatur auf.

2.2 Passende Teile des Leitfadens wählen

Wird eine spezifische Konfiguration eines Messgeräts untersucht oder entwickelt, ist es Benannten Stellen sowie Herstellern empfohlen, sich für Anwendungsbeispiele an Kapitel 4 zu orientieren. Nicht alle möglichen Konfigurationen eines Geräts können in diesem Leitfaden vorgestellt werden. Daher sollte die Leserin oder der Leser spezifische Implementierungsdetails aus verschiedenen Beispielen auswählen, um individuellen Modalitäten gerecht zu werden. Da sich alle hier vorgestellten Beispiele auf Messgeräte von Typ U der Risikoklasse C gemäß Definitionen in [1] beziehen (soweit nicht anders angegeben), sollten die meisten Aspekte der akzeptablen Lösungen austausch- oder kombinierbar sein.

3 Verallgemeinerte Architektur eines Messgeräts

3.1 Abgeleitete verallgemeinerte Architektur eines Messgeräts

Mit den allgemeinen Modulen und den spezifischen Begriffen, die im WELMEC-Leitfaden 7.2 [1] definiert werden, kann eine verfeinerte modulare Struktur geschaffen werden, die einer verallgemeinerten Architektur eines Messgeräts gleicht (s. Abbildung 3-1).

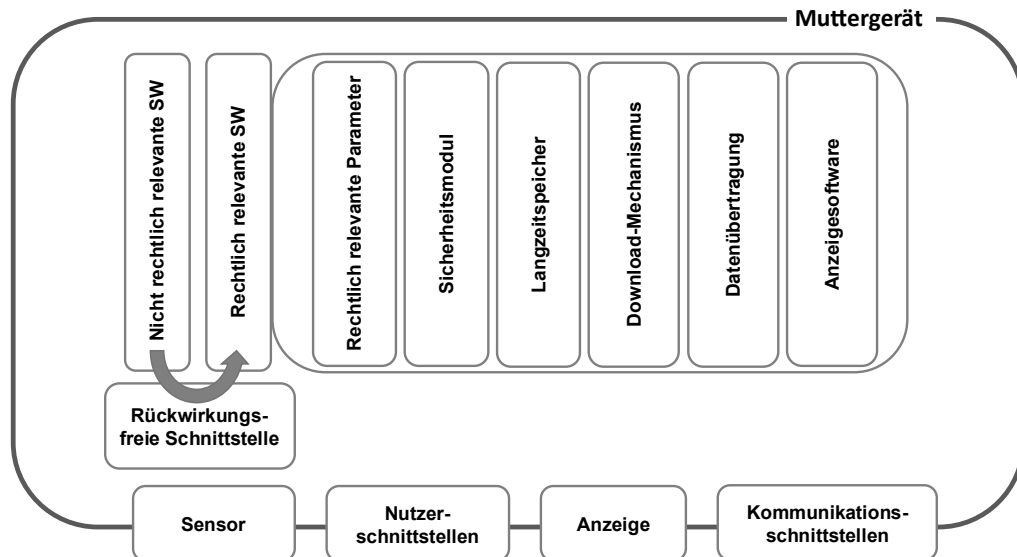


Abbildung 3-1: Allgemeine Architektur, die der verfeinerten modularen Struktur aus WELMEC-Leitfaden 7.2 gleicht

Anmerkung: Das Sicherheitsmodul vereint sämtliche rechtlich relevanten Sicherheitsmerkmale, bspw. für Integrität, Authentizität, Prüfsummenberechnung, Schlüssel- und Zertifikatmanagement, Software-Identifikator, Logbuch/Logdatei etc.

Eine detaillierte Beschreibung der verallgemeinerten Architektur ist in WELMEC-Leitfaden 7.3 „Reference Architectures Based on WELMEC Guide 7.2“ [4] zu finden.

Diese verallgemeinerte Architektur wird hier genutzt, um beispielhafte Konfigurationen von Messgeräten zu identifizieren, für die akzeptable Lösungen vorgestellt werden. Durch diese verallgemeinerte Architektur wird sichergestellt, dass sich die vorgestellten beispielhaften Anwendungen nicht widersprechen und einen einheitlichen Grad an Detailliertheit bieten.

4 Beispielhafte Anwendungen

Anforderung U1 wird durch eine vollständige Dokumentation immer erfüllt. U1 stellt keine zusätzlichen technischen Einschränkungen für das Messgerät dar und wird daher in den folgenden Beispielen nicht berücksichtigt.

4.1 Externe Speichereinheit, verbunden mit einem „Muttergerät“

4.1.1 Annahmen zum „Muttergerät“

- Das „Muttergerät“ ohne externe Speichereinheit muss die Anforderungen U1 bis U9 des WELMEC-Leitfadens 7.2, Ausgabe 2018, erfüllen.

- Die Verbindung zwischen „Muttergerät“ und der externen Speichereinheit ist physisch versiegelt.
- Das „Muttergerät“ und die Speichereinheit müssen zusammen die Anforderungen L1 bis L8 erfüllen. Das „Muttergerät“ muss die Anforderungen L1, L3, L5, L6 und L7 erfüllen.

4.1.2 Anwendbare Anforderungen für die externe Speichereinheit

- „Muttergerät“ und Speichereinheit müssen zusammen die Anforderungen L1 bis L8 erfüllen. Die Speichereinheit muss die Anforderungen L2, L3, L4, L5 und L8 erfüllen.
- Wenn sich rechtlich relevante Software auf der Speichereinheit befindet, um gespeicherte Messdaten anzuzeigen oder zu drucken, muss sie ebenfalls Anforderung L6 erfüllen.
- Falls die externe Speichereinheit eine eigene rechtlich relevante Software besitzt, muss sie die Anforderungen U2, U4, U5, U6, U7, U8 und U9 in Verbindung mit dem „Muttergerät“ erfüllen. (U2: Die Anforderung bezieht sich sowohl auf die Software-Identifikation der externen Speichereinheit als auch auf diejenige des „Muttergeräts“).
- Sollte die externe Speichereinheit eine Nutzerschnittstelle haben (z.B. einen An-/Ausschalter), muss sie U3 in Verbindung mit dem „Muttergerät“ erfüllen.
- Hat die externe Speichereinheit ihre eigene rechtlich relevante Software, müssen Anhänge D und S auf Anwendbarkeit geprüft werden.

4.1.3 Beschreibung der akzeptablen Lösung

Die folgende akzeptable Lösung bezieht sich explizit auf Messgeräte von Typ U der Risikoklasse C. Für eine andere Basiskonfiguration oder Risikoklasse muss die Lösung entsprechend angepasst werden.

Ein mehrdimensionales Messgerät besteht aus zwei Lasersensoren, die die zweidimensionalen Profile von Objekten abtasten, die auf einem Förderband transportiert werden. Die Geschwindigkeit des Bandes wird von einem dritten Sensor gemessen. Die Sensoren sind physisch versiegelt und über ein Kabel mit einer zentralen Prozessoreinheit verbunden, über welches ein serielles Protokoll für die Datenkommunikation genutzt wird. Sämtliche Kabelverbindungen sind gleichsam physisch gegen Manipulation geschützt. Die Prozessoreinheit ist mit einer Echtzeitzuhr und einer eingebauten Anzeige ausgestattet, auf der die berechneten Volumina der vermessenen Objekte angezeigt werden. Jedem neuen Objekt werden von der Prozessoreinheit ein eindeutiger Identifikator sowie ein Zeitstempel zugewiesen. Wurde ein Messwert (Länge, Breite, Höhe des kleinsten Würfels, der in das vermessene Objekt passt) zusammen mit dem eindeutigen Identifikator und dem Zeitstempel angezeigt, wird ein CRC32 mit geheimem Startwert berechnet und an den Messdatensatz angehängt.

Zur Langzeitspeicherung ist eine externe Speichereinheit, welche rechtlich relevante Software enthält, über eine serielle Kommunikationsverbindung an die Prozessoreinheit angeschlossen. Die Verbindung wird versiegelt, wenn beide Komponenten in Betrieb genommen werden. Die Speichereinheit erhält Messdatensätze von der Prozessoreinheit und bestätigt jeden empfangenen Datensatz. Die Speichereinheit meldet der Prozessoreinheit für jeden gespeicherten Datensatz, ob das Speichern erfolgreich war oder ob ein Fehler (Speicherversagen,

Speicher voll, Arbeitsspeicher beschädigt etc.) aufgetreten ist. Die Prozessoreinheit ist ebenfalls dazu in der Lage, der Nutzerin gespeicherte Messergebnisse zur Verfügung zu stellen. Durch Eingabe eines Zeitstempels oder eindeutigen Identifikators über ein Tastenfeld kann sie nach Datensätzen suchen. Nach Anfrage über das serielle Protokoll ruft die Speichereinheit das durch den eindeutigen Identifikator spezifizierte Messergebnis ab und schickt es an die Prozessoreinheit. Die Prozessoreinheit überprüft dann die Integrität des Datensatzes und zeigt der Nutzerin das Ergebnis an. Sollten die Daten beschädigt sein, wird eine Warnmeldung gezeigt. Die Prozessoreinheit ist in der Lage, die Versionsnummer der Software der Speichereinheit (abgefragt über das serielle Protokoll) auf Befehl anzuzeigen.

4.1.4 Zuordnung von Anforderungen zu Merkmalen der akzeptablen Lösung

Nr.	Anforderung	Akzeptable Lösung (Risikoklasse C)
U2	Software-Identifikation	Die Versionsnummer der Software der Prozessoreinheit wird beim Hochfahren angezeigt. Die Softwareversion der Speichereinheit kann über das serielle Protokoll abgefragt werden und wird in einem besonderen Menü angezeigt.
U3	Einfluss über die Nutzerschnittstelle	Die Nutzerschnittstelle der Prozessoreinheit ist so gestaltet, dass kein unzulässiger Einfluss auf Software, Parameter oder Messdaten auftreten kann. Die Speichereinheit hat keine Nutzerschnittstelle.
U4	Einfluss über Kommunikationsschnittstelle	Es sind keine offenen Kommunikationsschnittstellen vorhanden.
U5	Schutz gegen absichtliche oder unbeabsichtigte Änderungen	Einmal pro Tag wird eine CRC32-Prüfsumme mit einem geheimen Startwert von Software und gerätespezifischen Parametern der Prozessoreinheit berechnet und mit einem Referenzwert verglichen. Ein ähnlicher Prozess kann über das serielle Protokoll für die externe Speichereinheit ausgelöst werden. Schlägt eine der Überprüfungen fehl, wird eine Warnung angezeigt und es sind keine weiteren Messungen möglich. Die gerätespezifischen Parameter sind Kalibrierdaten für die Entfernungs- und Geschwindigkeitssensoren. Diese sind in einem extra Flash-Speicher innerhalb der Prozessoreinheit gespeichert. Die Integrität des Flash-Speichers wird einmal pro Tag sowie nach Hochfahren und Neustart durch eine CRC32-Prüfsumme geprüft. Schlägt die Überprüfung fehl, wird eine Warnung angezeigt und es sind keine weiteren Messungen möglich.
U6	Schutz gegen absichtliche Änderungen	Siehe U5. Zusätzlich sind die Gehäuse aller Komponenten und aller Kommunikationsverbindungen versiegelt. Die berechnete CRC32 der rechtlich relevanten Software und der gerätespezifischen Parameter wird auf Befehl auf dem integrierten Display angezeigt.
U7	Parameterschutz	Es gibt keine Befehle, um gerätespezifische Parameter über die Schnittstellen zu modifizieren.
U8	Anzeige der Messdaten	Die Messdaten werden von der rechtlich relevanten Software angezeigt. Es gibt keine nicht rechtlich relevante Software auf dem Gerät.
U9	Einfluss von anderer Software	Es gibt keine nicht rechtlich relevante Software auf dem Gerät.
L1	Vollständigkeit der gespeicherten Messdaten	Gespeicherte Messdatensätze entsprechen immer dem in 4.1.3 spezifizierten Format. Unvollständige Datensätze werden von der Speichereinheit verworfen und es wird eine Fehlermeldung an die Prozessoreinheit geschickt.
L2	Schutz gegen absichtliche oder unbeabsichtigte Änderungen	Jeder Datensatz wird zusammen mit seiner CRC32-Prüfsumme übertragen. Die Prüfsumme wird vor der Abfrage überprüft. Das Ergebnis der Überprüfung wird neben dem abgerufenen Messergebnis angezeigt.
L3	Datenintegrität	Jeder Datensatz wird zusammen mit seiner CRC32-Prüfsumme übertragen. Die Prüfsumme wird vor der Abfrage überprüft. Das Ergebnis der Überprüfung wird neben dem abgerufenen Messergebnis angezeigt.
L4	Authentizität der gespeicherten Messdaten	Da Speicher- und Prozessoreinheit durch ein gesiegeltes Kabel verbunden sind, sind keine weiteren Maßnahmen nötig, um den Ursprung der Messdaten zu verifizieren.
L5	Vertraulichkeit der Schlüssel	Der zur Berechnung der Prüfsumme von Messdaten genutzte geheime Startwert dient als kryptografischer Schlüssel. Er ist im ausführbaren Code der Prozessoreinheit gespeichert. Es gibt keine Befehle, um den Startwert über die Schnittstellen auszulesen oder zu modifizieren.
L6	Abruf, Verifikation und Anzeige von gespeicherten Daten	Die Software auf der Speichereinheit verifiziert jeden Datensatz vor dem Abruf. Die Software auf der Prozessoreinheit zeigt die abgerufenen Messergebnisse an und informiert den Nutzer/die Nutzerin über beschädigte oder modifizierte Datensätze.
L7	Automatisches Speichern	Nach vollständiger Messung wird das Ergebnis ohne Eingriff durch Nutzerin oder Nutzer an die Speichereinheit geschickt. Die nächste Messung kann erst begonnen werden, nachdem der Speichervorgang erfolgreich war.
L8	Speicherkapazität und Kontinuität	Die Speichereinheit verfügt über ausreichend Kapazität, um die Messergebnisse von zwei aufeinanderfolgenden Eichperioden zu speichern. Messergebnisse, die älter als zwei Eichperioden sind, werden automatisch gelöscht. Sollte der Speicher dennoch voll werden, wird eine Warnung angezeigt und es sind keine weiteren Messungen möglich.

Tabelle 4-1: Technische Anforderungen und Beschreibung akzeptabler Lösungen für die externe Speichereinheit.

4.2 Externe Anzeigeeinheit, verbunden mit einem „Muttergerät“

4.2.1 Annahmen zum „Muttergerät“

- Das „Muttergerät“ ohne externe Anzeigeeinheit muss die Anforderungen U1, U2, U3 bis U7 sowie U9 des WELMEC-Leitfadens 7.2, Ausgabe 2018 erfüllen.
- Um die Identifikation des „Muttergeräts“, wie in U2 gefordert, anzuzeigen, besteht eine Schnittstelle zur einer Anzeigeeinheit.
- Sollte die Anzeigeeinheit vom „Muttergerät“ getrennt werden können, ohne ein Siegel zu brechen, muss die Schnittstelle des „Muttergeräts“, die sonst zur Verbindung zur Anzeigeeinheit genutzt wird, Anforderung U4 erfüllen.
- Die Datenübertragung zwischen „Muttergerät“ und Anzeigeeinheit muss die Anforderungen T1 bis T8 erfüllen. Das „Muttergerät“ muss die Anforderungen T1, T2, T3, T4, T5, T7, und T8 erfüllen.

4.2.2 Anwendbare Anforderungen für die Anzeigeeinheit

- „Muttergerät“ und Anzeigeeinheit müssen zusammen die Anforderungen U2 und U8 erfüllen.
- Falls die externe Anzeigeeinheit eine eigene rechtlich relevante Software besitzt, muss sie die Anforderungen U2, U4, U5, U6, U7 und U9 in Verbindung mit dem „Muttergerät“ erfüllen. (U2: Software-Identifikation der externen Anzeigeeinheit, zusätzlich zur Software-Identifikation des „Muttergeräts“).
- Sollte die externe Anzeigeeinheit eine Nutzerschnittstelle haben (z.B. einen An-/Ausschalter), muss sie U3 in Verbindung mit dem „Muttergerät“ erfüllen.
- Anhänge D und S müssen auf Anwendbarkeit geprüft werden.
- Die Datenübertragung zwischen „Muttergerät“ und Anzeigeeinheit muss die Anforderungen T1 bis T8 erfüllen. Die Anzeigeeinheit muss T2, T3, T4, T5, T6, T7 und T8 erfüllen.

4.2.3 Beschreibung der akzeptablen Lösung

Die folgende akzeptable Lösung bezieht sich explizit auf Messgeräte von Typ U der Risikoklasse C. Für eine andere Basiskonfiguration oder Risikoklasse muss die Lösung entsprechend angepasst werden.

Ein Messgerät zum Messen von Flüssigkeiten außer Wasser ist mit drei Ultraschallsensoren ausgestattet, um das Volumen einer Flüssigkeit zu messen, die durch ein Rohr fließt. Die Sensoren sind physisch gesiegelt und über ein Kabel mit einer zentralen Prozessoreinheit verbunden, die ein serielles Protokoll für die Datenkommunikation nutzt. Sämtliche Kabelverbindungen sind gleichsam physisch gegen Manipulation geschützt. Das gemessene Gesamtvolumen wird in einem dedizierten, stetig inkrementierenden Register gespeichert. Einmal installiert, misst das Gerät den Fluss der Flüssigkeit ohne die Notwendigkeit manueller Eingaben. Kalibriereinstellungen für Parameter können nur bei geöffnetem Gehäuse vorgenommen werden. Die Prozessoreinheit hat eine einzelne LED, die anzeigt, dass dem Log ein neuer Fehler hinzugefügt wurde.

Um das aktuelle Messergebnis anzuzeigen, kann eine Sichtanzeige an eine serielle Schnittstelle der Prozessoreinheit angeschlossen werden. Nach dem Anschluss müssen alle Einträge des Fehlerprotokolls durchlaufen werden, indem der Prozessoreinheit Befehle (vorwärts, rückwärts) erteilt werden, die entsprechend antwortet, bevor das Messergebnis angezeigt wird. Die seriellen Schnittstellen von sowohl der Prozessoreinheit als auch der Anzeigeeinheit sind durch ein

Softwarefiltermodul geschützt, das unzulässige Befehle aussortiert/löscht/verwirft. Wenn verbunden, leitet die Prozessoreinheit das aktuelle Volumen und den Zeitstempel an die Anzeige weiter, die das Ergebnis automatisch anzeigt.

4.2.4 Zuordnung von Anforderungen zu Merkmalen der akzeptablen Lösung

Nr.	Anforderung	Akzeptable Lösung (Risikoklasse C)
U2	Software-Identifikation	Die Versionsnummer der Software der Anzeigeeinheit wird beim Hochfahren angezeigt. Die Softwareversion der Prozessoreinheit wird berechnet und an die Anzeigeeinheit geleitet, wenn beide verbunden sind. Die Versionsnummer der Software der Prozessoreinheit wird neben dem Messergebnis angezeigt.
U3	Einfluss über Nutzerschnittstelle	Die Prozessoreinheit hat keine Nutzerschnittstelle. Die Nutzerschnittstelle der Anzeigeeinheit besteht aus zwei Knöpfen, die nur die beiden erlaubten Befehle „vorheriger Eintrag“ und „nächster Eintrag“ auslösen können.
U4	Einfluss über Kommunikationsschnittstelle	Die seriellen Kommunikationsschnittstellen von sowohl der Prozessoreinheit als auch der Anzeigeeinheit sind durch ein Softwarefiltermodul geschützt, das unzulässige Befehle aussortiert/löscht/verwirft.
U5	Schutz gegen zufällige oder unbeabsichtigte Änderungen	Einmal pro Tag wird eine CRC32-Prüfsumme der Software und der gerätespezifischen Parameter der Prozessoreinheit berechnet und mit einem Referenzwert verglichen. Ein ähnlicher Prozess wird für die externe Anzeigeeinheit ausgelöst, wenn sie mit der Prozessoreinheit verbunden wird. Schlägt eine der Überprüfungen fehl, wird dem Fehlerprotokoll ein Eintrag hinzugefügt und die LED an der Außenseite der Prozessoreinheit leuchtet auf. Die LED erlischt erst, wenn der Nutzer bzw. die Nutzerin durch alle Einträge im Fehlerprotokoll gescrollt hat. Die gerätespezifischen Parameter sind Kalibrierdaten für die Ultraschallsensoren. Diese sind in einem extra Flash-Speicher innerhalb der Prozessoreinheit gespeichert. Die Integrität des Flash-Speichers wird einmal pro Tag durch eine CRC32-Prüfsumme überprüft. Schlägt die Überprüfung fehl, wird ebenfalls ein Eintrag im Fehlerprotokoll erzeugt.
U6	Schutz gegen absichtliche Änderungen	Siehe U5. Zusätzlich erfüllen die seriellen Kommunikationsschnittstellen U4.
U7	Parameterschutz	Es gibt keine Befehle, um gerätespezifische Parameter über die Schnittstellen zu modifizieren.
U8	Anzeige von Messdaten.	Die Messdaten werden von der rechtlich relevanten Software angezeigt. Es gibt keine nicht rechtlich relevante Software auf dem Gerät.
U9	Einfluss durch andere Software	Es gibt keine nicht rechtlich relevante Software auf dem Gerät.
T1	Vollständigkeit übertragener Daten	Datensätze, die von der Prozessoreinheit an die Anzeigeeinheit gesendet werden, entsprechen immer dem im letzten Satz von 4.2.3 spezifizierten Format.
T2	Schutz gegen zufällige oder unbeabsichtigte Änderungen	Jeder Datensatz wird zusammen mit seiner CRC32-Prüfsumme übertragen. Die Prüfsumme wird von der Anzeigeeinheit geprüft. Das Ergebnis der Überprüfung wird neben dem abgerufenen Messergebnis angezeigt.
T3	Datenintegrität	Jeder Datensatz wird zusammen mit seiner CRC32-Prüfsumme übertragen. Die Prüfsumme wird von der Anzeigeeinheit geprüft. Das Ergebnis der Überprüfung wird neben dem abgerufenen Messergebnis angezeigt.
T4	Authentizität übertragener Daten	Da die CRC, die zum Schutz übertragener Daten gegen Modifikation genutzt wird, auf einem geheimen Startwert beruht, sichert sie auch die Authentizität übertragener Daten.
T5	Vertraulichkeit der Schlüssel	Der zur Berechnung der Prüfsumme von Messdaten genutzte geheime Startwert dient als kryptografischer Schlüssel. Er ist in den ausführbaren Codes der Prozessoreinheit und der Anzeigeeinheit gespeichert. Es gibt keine Befehle, um den Startwert über die Nutzer- oder Kommunikationsschnittstelle auszulesen oder zu modifizieren.
T6	Umgang mit beschädigten Daten	Wenn die CRC-Prüfung der erhaltenen Daten innerhalb der Anzeigeeinheit fehlschlägt, wird eine Fehlermeldung neben dem

		(möglicherweise unlesbaren) Messergebnis angezeigt.
T7	Übertragungsverzögerung	Ist die Anzeigeeinheit an die Prozessoreinheit angeschlossen, aber Messdaten sind verzögert, wird kein Messergebnis angezeigt. Sie wird eine allgemeine Fehlermeldung anzeigen, das Messergebnis innerhalb der Prozessoreinheit wird von solch einer Verzögerung nicht beeinflusst.
T8	Verfügbarkeit von Übertragungsdiensten	Ist die Anzeigeeinheit an die Prozessoreinheit angeschlossen, aber es werden keine Messdaten empfangen, wird kein Messergebnis angezeigt. Sie wird eine allgemeine Fehlermeldung anzeigen, das Messergebnis innerhalb der Prozessoreinheit wird von einer gestörten Kommunikationsverbindung nicht beeinflusst.

Tabelle 4-2: Technische Anforderungen und Beschreibung akzeptabler Lösungen für die externe Anzeigeeinheit.

4.3 Anhang D: Download von rechtlich relevanter Software

Dieser Anhang von WELMEC-Leitfaden 7.2, Version 2018, muss genutzt werden, wenn Geräte mit Einrichtungen für einen Software-Download ohne Siegelbruch ausgestattet sind. Der Anhang kann auf Messgeräte von Typ P nach Erfüllen der Anforderungen D1-D4 angewandt werden.

4.3.1 Beschreibung der akzeptablen Lösung

Die folgende akzeptable Lösung bezieht sich auf Messgeräte von Typ P der Risikoklasse C. Für eine andere Basiskonfiguration oder Risikoklasse muss die Lösung entsprechend angepasst werden.

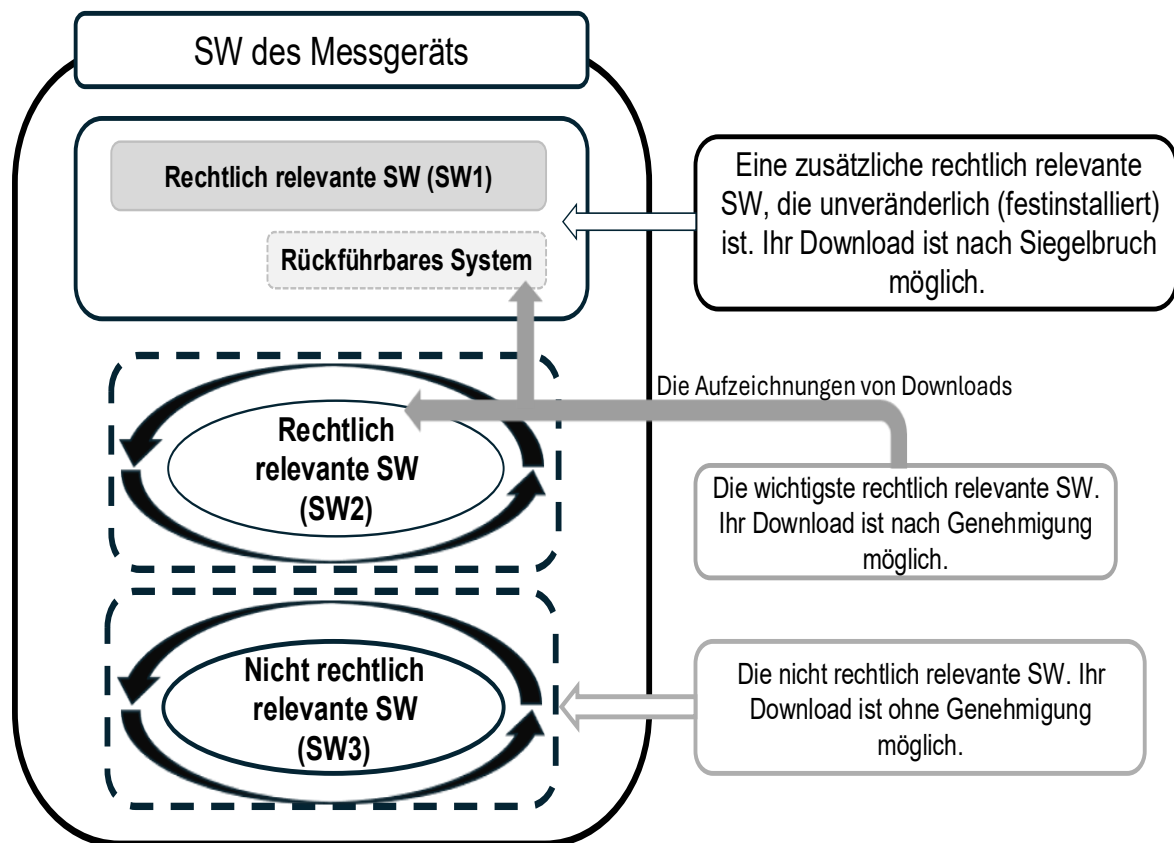


Abbildung 4-3: Software eines Messgeräts

Das Messgerät besteht aus drei verschiedenen Master Control Units (MCU1, MCU2 und MCU3). Die MCU1 beinhaltet feste rechtlich relevante Software (fortan SW1), die

für den gesamten Downloadprozess verantwortlich ist (ohne Möglichkeit, ohne Siegelbruch verändert oder aktualisiert zu werden). Die MCU2 beinhaltet rechtlich relevante Software (fortan SW2), die sämtliche rechtlich relevanten Funktionalitäten liefert, und MCU3 beinhaltet nicht rechtlich relevante Software (fortan SW3). SW1 und SW2 haben jeweils eigene Prüfsummen und Softwareversionen, die ohne zusätzliche Werkzeuge ausgelesen werden können.

Die MCU1 enthält eine versteckte digitale Signatur, Funktionalitäten zur Durchführung von Software-Downloads sowie zwei Eventlogger (EL_1, EL_2). Es ist nicht möglich, Aufzeichnungen in den Eventloggern zu modifizieren oder zu löschen. Die Aufzeichnungen können nur nach einem Siegelbruch gelöscht werden. EL_1 beinhaltet Aufzeichnungen über erfolgreich heruntergeladene SW. Sobald die Anzahl an Aufzeichnungen 50 erreicht, wird die MCU1 elektronisch verschlossen und ab diesem Zeitpunkt ist ein Download von Software nicht mehr möglich. EL_2 beinhaltet Aufzeichnungen über nicht erfolgreich heruntergeladene SW. Die Kapazität für Aufzeichnungen ist 500. Ist einer der Logger voll, wird die MCU1 elektronisch verschlossen und ein weiterer Software-Download ist nicht möglich. Der nächste Download ist erst möglich, nachdem Ereignisse von den Eventloggern gelöscht wurden. Die Aufzeichnungen in den Eventloggern sind gegen Löschen/Modifizieren durch einen gesiegelten Schalter geschützt.

SW1 ist für den gesamten Download-Prozess verantwortlich. Bevor der Downloadprozess beginnt, überprüft SW1, ob die digitale Signatur der neuen heruntergeladenen Version von SW2 korrekt ist. Die digitale Signatur wird zur Überprüfung von Authentizität, Integrität und angemessenem Ursprung genutzt. Fällt die Verifikation der digitalen Signatur negativ aus, wird ein entsprechender Eintrag in EL_2 erstellt. Es kann mehrere Gründe dafür geben, warum ein Downloadprozess nicht erfolgreich abgeschlossen wird, z.B. Verbindungsprobleme, Übertragungsfehler etc.; jeder Problemtyp hat seine eigene Identifikation.

Fällt die Verifikation der digitalen Signatur positiv aus, beginnt der Software-Download. Der erste Schritt ist die Übertragung der aktuellen rechtlich relevanten Software in den temporären Speicher. Tritt während der Übertragung ein Fehler auf, wird ein Eintrag in EL_2 erstellt. Auch für die Integritätsprüfung der neu heruntergeladenen Software SW2 wird eine digitale Signatur genutzt (zur Kontrolle, ob alle Pakete vollständig und fehlerlos übertragen wurden). Fällt die Integritätsprüfung negativ aus, wird ein Eintrag in EL_2 erstellt.

Der zweite Schritt ist die Installation. Der Prozess der Installation beginnt, wenn die Integritätsprüfungen etc. erfolgreich abgeschlossen wurden. Während des Installationsvorgangs wird der Messprozess für maximal 2 Minuten angehalten. War die Installation erfolgreich, erstellt die SW1 einen Eintrag in EL_1, wenn nicht, dann wird ein Eintrag in EL_2 erstellt.

4.3.2 Zuordnung von Anforderungen zu Merkmalen der akzeptablen Lösung

Nr.	Anforderung	Akzeptable Lösung (Risikoklasse C)
D1	Download-Mechanismus	Software auf MCU1 (SW1) ist für den gesamten Download-Mechanismus verantwortlich. Der Downloadprozess besteht aus der Prüfung der digitalen Signatur, dem Download der aktuellen Software in den temporären Speicher, der Integritätsprüfung der neuen Software, dem eigentlichen Installationsvorgang, dem Erstellen von Einträgen in den Eventloggern etc.
D2	Authentifizierung der übertragenen Software	Vor Beginn des Downloadprozesses prüft die SW1, ob die digitale Signatur der neuen heruntergeladenen Version korrekt ist.

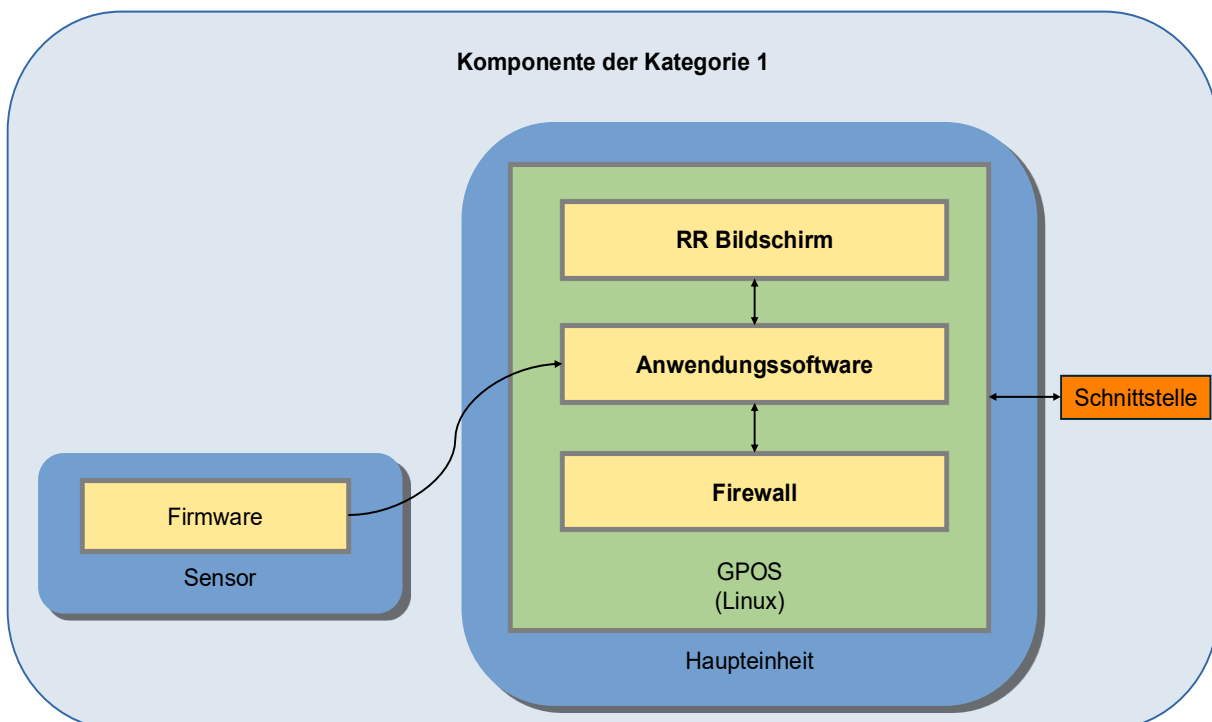
D3	Integrität von heruntergeladener Software	Für die Integritätsprüfung der neu heruntergeladenen Software SW2 wird eine digitale Signatur genutzt (zur Kontrolle, ob alle Pakete vollständig und fehlerlos übertragen wurden). Nach der Integritätsprüfung erstellt die SW einen Eintrag im Eventlogger EL_1 (im Falle eines positiven Ergebnisses) oder im EL_2 (falls an irgendeiner Stelle des Download-Prozesses ein negatives Ergebnis erzielt wird).
D4	Rückführbarkeit des Downloads rechtlich relevanter Software	MCU1 beinhaltet zwei Eventlogger (EL_1 und EL_2). EL_1 beinhaltet Aufzeichnungen über erfolgreich heruntergeladene SW. Sobald die Anzahl an Aufzeichnungen 50 erreicht, wird die MCU1 elektronisch verschlossen und ab diesem Zeitpunkt ist ein Download von Software nicht mehr möglich. EL_2 beinhaltet Aufzeichnungen über nicht erfolgreich heruntergeladene SW. Die Kapazität für Aufzeichnungen ist 500. Ist einer der Logger voll, wird die MCU1 elektronisch verschlossen und ein weiterer Software-Download ist nicht möglich. Der nächste Download ist erst möglich, nachdem Ereignisse von den Eventloggern gelöscht wurden. Die Aufzeichnungen in den Eventloggern sind gegen Löschen/Modifizieren durch einen gesiegelten Schalter geschützt.

Tabelle 4-3: Technische Anforderungen und Beschreibung akzeptabler Lösungen für den Download rechtlich relevanter Software

4.4 Anhang O: Komponente der Kategorie 1

Dieses Beispiel behandelt ein Messgerät mit einem eingebetteten PC und konzentriert sich hauptsächlich auf die Anwendung von Anhang O auf eine Komponente der Kategorie 1.

Abbildung 4-4: Systemüberblick einer Komponente der Kategorie 1.



4.4.1 Annahmen zum Gerät

- Der Sensor erfüllt alle Typ-P-Anforderungen sowie die Anforderungen aus Anhang T für geschlossene Netze bezüglich Messdatenübertragung an den eingebetteten PC.
- Der eingebettete PC erfüllt alle Typ-U-Anforderungen.
- Die Softwareprüfsumme des Sensors wird täglich geprüft und zur Anzeige auf Befehl zusammen mit der Versionsnummer an den eingebetteten PC gesendet.
- Die rechtlich relevante Anzeige wird durch eine Anzeige realisiert, der am eingebetteten PC angebracht wurde. Messdaten, die über die Kommunikationsschnittstelle des Messgeräts abgerufen werden, sind nicht rechtlich relevant.

4.4.2 Anwendbare Anforderungen für das Messgerät

- Typ-P-Anforderungen und Anforderungen aus Anhang T für den Sensor
- Typ-U-Anforderungen und Anhang O für den eingebetteten PC

4.4.3 Beschreibung der akzeptablen Lösung

Die Komponente der Kategorie 1 besteht aus einem Sensor mit digitalem Ausgang, der mit einem kleinen, eingebetteten PC in einem versiegelten Gehäuse verbunden ist. Auf dem eingebetteten PC laufen ein U-Boot-Bootloader und ein Linux-Betriebssystem, auf dem wiederum eine Anwendung zur Visualisierung der Messergebnisse sowie ein Fehlerprotokoll laufen. Das BIOS ist durch ein Zufallspasswort gesichert und durch das versiegelte Gehäuse der Komponente geschützt. Beim Hochfahren verifiziert U-Boot die Integrität des Betriebssystems mithilfe eines SHA256, der über die rechtlich relevanten Teile des Betriebssystems (Bootkonfiguration, /etc, /kernel, /lib) berechnet wird. Nur wenn der Hash mit seinem Referenzwert übereinstimmt, wird das Betriebssystem gestartet. Der Hashwert und die Versionsnummer der Linuxdistribution werden zusammen mit der Kernelversion während des Hochfahrens angezeigt. Dann überprüft ein rechtlich relevantes Startscript, das Teil der Bootkonfiguration ist, die Integrität der rechtlich relevanten Anwendung und fährt das Betriebssystem im Falle einer Diskrepanz herunter. Die Anwendung läuft im Kioskmodus. Für die Abfrage nicht rechtlich relevanter Messdaten vom Gerät sind NFC- und Ethernet-Schnittstellen vorhanden. Beide sind logisch den internen Software-Schnittstellen zugeordnet, die von Seiten des Betriebssystems durch eine Firewall und auf Ebene der Anwendung durch einen Befehlsfilter geschützt sind. Die Prozesspriorität der Anwendung stellt sicher, dass sie immer ausreichend CPU-Zeit hat.

4.4.4 Zuordnung von Anforderungen zu Merkmalen der akzeptablen Lösung

Nr.	Anforderung	Akzeptable Lösung (Risikoklasse C)
O1	Hardware	• Versiegeltes Gehäuse mit offenen NFC- und Ethernet-Schnittstellen.
O2	Bootvorgang	• Passwortschutz des BIOS und Versiegeltes Gehäuse stellen sicher, dass U-Boot nicht umgangen werden kann. • U-Boot prüft die Integrität des Betriebssystems. Das Startscript prüft die Integrität der Anwendung und fährt das Betriebssystem herunter, wenn die Prüfung negativ ausfällt.
O3	Systemressourcen	• Die feste Softwareumgebung und die Prozesspriorität der rechtlich relevanten Anwendung stellen sicher, dass immer ausreichend Ressourcen für die rechtlich relevante Anwendung zur Verfügung stehen.

O4	Schutz in Verwendung	Der Startvorgang stellt sicher, dass der Kioskmodus immer etabliert wird und dass die Nutzerin bzw. der Nutzer keinen Zugriff auf die Funktionen des Betriebssystems erlangen kann.
O5	Rückwirkungsfreie Schnittstellen	Die Firewall-Einstellung stellt sicher, dass nur eine begrenzte Anzahl an Ports für externe Kommunikation geöffnet ist.
O6	Identifikation des Betriebssystems und seiner Konfiguration	Version der Linuxdistribution und ein SHA256 über den rechtlich relevanten Teilen des Betriebssystems werden während des Hochfahrens angezeigt.
O7	Schutz des Betriebssystems	SHA256 über die Bootkonfiguration, /etc, /kernel, /lib.

4.5 Anhang O: Komponente der Kategorie 2

Dieses Beispiel behandelt ein Messgerät mit einem PC und konzentriert sich hauptsächlich auf die Anwendung von Anhang O auf eine Komponente der Kategorie 2.

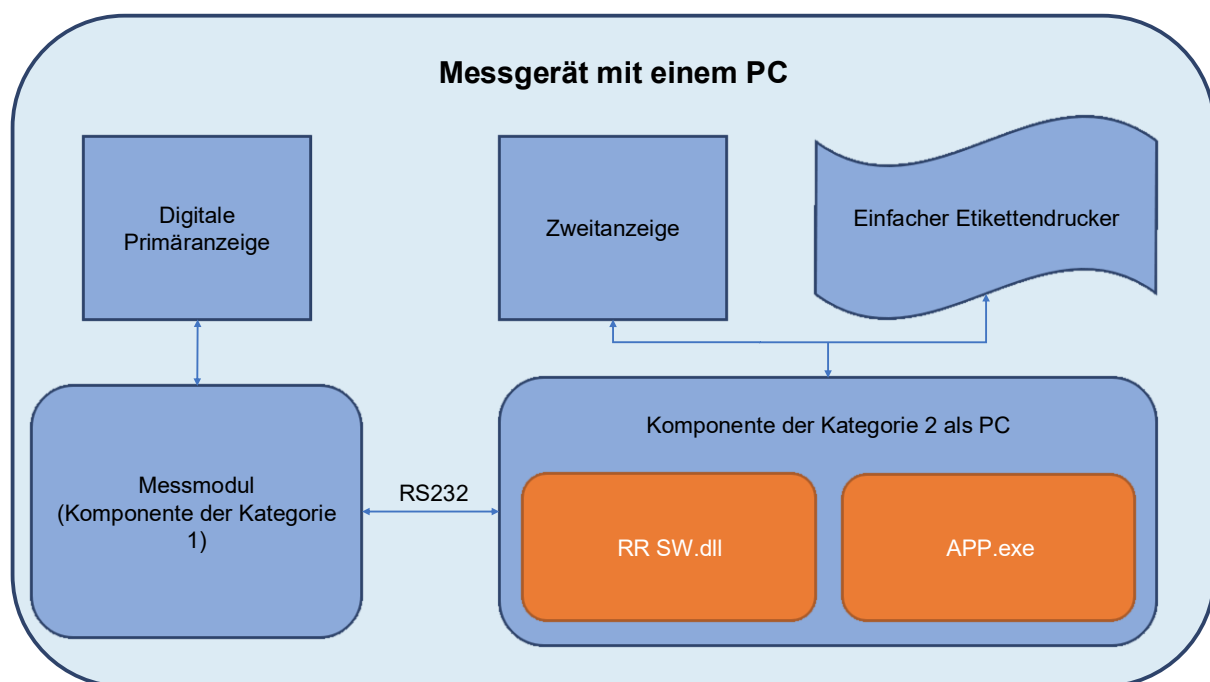


Abbildung 4-5: Systemübersicht eines Messgeräts bestehend aus einer digitalen Primäranzeige, einem Messmodul, einem PC, einer Zweitanzeige und einem einfachen Etikettendrucker.

4.5.1 Annahmen zum Messgerät

- Das Messmodul erfüllt alle Typ-P-Anforderungen vollständig. Auf dem Messmodul läuft keine nicht rechtlich relevante Software. Das Messmodul ist nur über eine serielle Schnittstelle verbunden, die zur Kommunikation mit dem PC genutzt wird. Anforderungen für geschlossene Netze aus Anhang T in Bezug auf die Messdatenübertragung auf den PC sind erfüllt.
- Die Primäranzeige wird durch ein Display realisiert, der an das Messmodul angeschlossen ist (Komponente der Kategorie 1).
- Eine technische Arbeitsgruppe hat den PC der Kategorie 2 zugeordnet. Alle U-Anforderungen sowie Anhänge S, D, L und T für geschlossene Netze werden vom PC erfüllt.
- Über die Kommunikationsschnittstelle des PCs können keine rechtlich relevanten Daten abgefragt werden.

4.5.2 Anwendbare Anforderungen für das Messgerät

- Typ-P-Anforderungen und Anforderungen aus Anhang T für das Messmodul.
- Typ-U-Anforderungen sowie T-, S-, L-, D-Anforderungen und die Erweiterung O Kategorie 2 für den PC unter der Voraussetzung, dass eine technische Arbeitsgruppe die Komponente der Kategorie 2 zugewiesen hat.

4.5.3 Beschreibung der akzeptablen Lösung für den PC

Die Anwendung läuft im Kioskmodus. Die Prozesspriorität der Anwendung stellt sicher, dass sie immer ausreichend Prozessorzeit hat.

Die Softwareprüfsumme der RR SW.dll wird auf der Sekundäranzeige übertragen und kann während des Startvorgangs überprüft und auf Befehl zusammen mit der Versionsnummer angezeigt werden.

Die RR SW.dll besteht aus allen rechtlich relevanten Funktionen. die nicht rechtlich relevante APP.exe wird für andere Zwecke verwendet. Die Schnittstellen, um Peripheriegeräte (z.B. Tastenfeld, Drucker, Maus) anzuschließen oder zur Kommunikation mit dem System der Steuerbehörde, bspw. USB oder Ethernet, sind geschützt. USB-Richtlinien stellen sicher, dass nur vorausgewählte Geräte an den PC angeschlossen werden können. Die Einstellung der Windows Firewall stellt sicher, dass nur eine begrenzte Anzahl an Ports für externe Kommunikation offen sind.

Das Betriebssystem wird durch die Version von Windows 7 Embedded und einen SHA256 über die spezifischen rechtlich relevanten Konfigurationsdateien und Registry-Schlüssel identifiziert. Die Identifikation wird von der RR SW.dll auf Befehl angezeigt. Es gibt keine Schnittstellen mit direktem Zugriff auf den Arbeitsspeicher. Die Anwendung überprüft den Hashwert und fährt das System im Fall einer Diskrepanz herunter.

4.5.4 Zuordnung von Anforderungen zu Merkmalen der akzeptablen Lösung

Nr.	Anforderung	Akzeptable Lösung (Risikoklasse C)
O1	Hardware	• Versiegeltes Gehäuse des PCs mit offenen USB-, Ethernet-Schnittstellen. • Hardwareschnittstellen, die das Betriebssystem beeinflussen können, sind durch das Betriebssystem deaktiviert. • Es gibt keine Schnittstellen mit direktem Zugriff auf den Arbeitsspeicher.
O3	Systemressourcen	• Der Kioskmodus und die Prozesspriorität der rechtlich relevanten Anwendung stellen sicher, dass immer ausreichend Ressourcen für die rechtlich relevante Anwendung zur Verfügung stehen.
O4	Schutz in Verwendung	• Der Startvorgang stellt sicher, dass der Kioskmodus immer etabliert wird und dass die Nutzerin bzw. der Nutzer keinen Zugriff auf die Funktionen des Betriebssystems erlangen kann.
O5	Rückwirkungsfreie Schnittstellen	• Die Einstellung der Windows Firewall stellt sicher, dass nur eine begrenzte Anzahl an Ports für externe Kommunikation offen sind. • USB-Richtlinien stellen sicher, dass nur vorausgewählte Geräte an den PC angeschlossen werden können.
O6	Identifikation des Betriebssystems und seiner Konfiguration	• Version des Windows 7 Embedded Betriebssystems. • SHA256 über die spezifischen rechtlich relevanten Konfigurationsdateien und Registry-Schlüssel.
O7	Schutz des Betriebssystems	• SHA256 über die spezifischen rechtlich relevanten Konfigurationsdateien und Registry-Schlüssel, überprüft von der Anwendung.

5 Referenzen und zusätzliche Literatur

- [1] „WELMEC-Leitfaden 7.2: Softwareleitfaden“, *WELMEC*, <https://www.welmec.org/guides-and-publications/guides>.
- [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, S. 149 - 250, 29. März 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, 30.04.2004.
- [4] „WELMEC Guide 7.3 Reference Architectures Based on WELMEC Guide 7.2“, *WELMEC*, 2020.

6 Revisionshistorie

Nr.	Datum	Wichtige Änderungen
0	August 2018	Erste Version
1	April 2019	Überarbeitete Fassung nach Treffen von WG 7. Alle Verweise auf Teile und Baueinheitenzertifikate wurden entfernt.
2	April 2020	Kapitel 4.1.1, 4.1.2, 4.2.1 und 4.2.2 wurden bezüglich der zu erfüllenden Anforderungen angepasst. Die akzeptable Lösung in Kapitel 4.2.3 wurde an Messgeräte zum Messen von Flüssigkeiten außer Wasser angepasst. 4.3 Anhang D: Download von rechtlich relevanter Software wurde hinzugefügt.
3	März 2022	Um die Ergänzung von Anhang O im Leitfaden 7.2 zu vervollständigen, wurden die Kapitel 4.4 „Anhang O: Komponente der Kategorie 1“ und 4.5 Anhang O: „Komponente der Kategorie 2“ hinzugefügt.

Tabelle 10-1: Revisionshistorie