Arbeitsgruppe 8.51 „Metrologische Software“ Stand: 23.05.2017

Merkblatt:
Anforderungen an die Dokumentation für Softwareprüfungen nach WELMEC Guide 7.2

Für jedes zur Konformitätsbewertung vorgelegte Messgerät, das Software enthält, muss eine Software-Dokumentation eingereicht werden, welche folgende allgemeine Merkmale aufweisen muss:

- Dokumententitel oder Bezeichner des Dokuments,
- Name der Bauart, auf die sich das jeweilige Dokument bezieht,
- Versionsnummer, Ausgabedatum oder Ähnliches,
- Seiten-, Abschnittsnummerierungen oder andere Referenzierungsmöglichkeiten.

Die Dokumente müssen gut lesbar und widerspruchsfrei sein. Sie sind in deutscher Sprache zu verfassen, sofern sie für Verwender, Benutzer, Marktaufsicht oder Eichbehörden vorgesehen sind. In allen anderen Fällen sind Deutsch oder Englisch zulässig.

Sofern Dokumente in elektronischer Form zur Verfügung gestellt werden, dürfen sich deren Inhalte nach Aufruf der Datei nicht automatisch aktualisieren (z.B. Abschaltung der automatischen Datumsaktualisierung). Daher ist die Bereitstellung der elektronischen Dokumente als ungeschützte pdf-Dateien zu empfehlen.

Die nachfolgend geforderten Inhalte müssen nicht in geschlossener Form vorliegen, sondern können auf mehrere Dokumente verteilt werden. Die Gebrauchsanweisung für das Messgerät ist separat zu liefern.

Allgemeines

- Überblick über die System-Hardware (z.B. Block-Schaltbild mit den verwendeten Hardwarekomponenten, Übertragungswege der Messwerte),
- Angaben über die Softwarestruktur (z.B. Angaben darüber, in welcher Hardwarekomponente welches Softwareprogramm enthalten ist),
- Beschreibung aller rechtlich relevanten Softwarefunktionen, Parameter und Messwerte,
- Bei Verwendung eines Betriebssystems: Bezeichnung, Version, weitere Charakterisierungen (z.B. installierte „Service-Packs“ bei Microsoft Windows, Nennung der Distribution bei Linux), Beschreibung der Konfiguration des Betriebssystems hinsichtlich rechtlich relevanter Schutzmaßnahmen.
- Für Risikoklassen E und F:
  - Erklärung zur Erstellung der rechtlich relevanten lauffähigen Programme (Herstellererklärung),
  - Technische Beschreibung zur Erstellung der rechtlich relevanten lauffähigen Programme,

- Beschreibung der Methode und Angabe der technischen Mittel, mit denen die Bit-zu-Bit-Identität zwischen dem Baumuster und einem beliebigen Seriengerät geprüft werden kann (Falls nötig: Technische Hilfsmittel zum Bit-zu-Bit-Identitätsvergleich).

Für jedes **rechtlich relevante lauffähige Programm** muss folgendes dokumentiert sein:

Softwareidentifikation

- Art der Identifikation, Beschreibung der Realisierung (Auflistung der erfassten Softwareprogramme oder -programmteile, Berechnungsmethoden)
- Werte der Softwareidentifikatoren, für die die Zulassung erfolgen soll
- Anleitung zur Anzeige der Identifikatoren

Einflussnahme über die Benutzerschnittstellen

- Liste aller Benutzerschnittstellen (z.B. grafische Benutzeroberfläche, Tasten, Schalter, Regler, Dongles, Jumper, Schlüssel)
- Liste aller Benutzeraktionen (z.B. Eingaben, Befehle, Menüpunkte, Schaltflächen) für alle vorhandenen Benutzerschnittstellen und ggf. deren Kombinationsmöglichkeiten sowie deren Wirkung
- Erläuterung, wie eine unzulässige Beeinflussung der Softwareprogramme und ggf. des Betriebssystems über die Benutzerschnittstellen verhindert wird

Einflussnahme über die Kommunikationsschnittstellen

- Liste aller Kommunikationsschnittstellen (z.B. Schnittstellen für Kabelverbindungen, optische/infrarote, akustische, Funkverbindungen, analoge Verbindungen)
- Liste aller empfangbaren Befehle aller Kommunikationsschnittstellen sowie deren Wirkung
- Erläuterung, wie eine unzulässige Beeinflussung der Softwareprogramme und ggf. des Betriebssystems über die Kommunikationsschnittstellen verhindert wird

Schutz vor zufälligen oder unabsichtlichen Änderungen

- Beschreibung, wie rechtlich relevante lauffähigen Programme und bauartspezifische Parameter vor zufälligen oder unabsichtlichen Änderungen geschützt sind:
  - Welche Schutzmaßnahmen werden verwendet?
  - Wann kommt das Verfahren zum Einsatz?
  - Wie ist die Reaktion des Systems im Fehlerfall?
  - Welche Softwareprogramme, -programmteile oder Parameter(-sätze) werden geschützt?
- Beschreibung, wie kritische Benutzeraktionen (z.B. Löschen oder Ändern von Daten) abgesichert werden (z.B. Deaktivierung, Nachfrage)
- Beschreibung von Plausibilitätskontrollen bei Benutzereingaben

Schutz vor absichtlichen Änderungen

- Beschreibung, wie rechtlich relevante lauffähige Programme, bauartspezifische Parameter und ggf. wichtige Teile des Betriebssystems vor Manipulationen geschützt sind:
  - Welche Schutzmaßnahmen werden verwendet? (Hier können auch Hardwarelösungen zum Einsatz kommen, z.B. Plomben, Siegel, Dongles.)
  - Wann kommt das Verfahren zum Einsatz?
  - Wie ist die Reaktion des Systems im Fehlerfall?
  - Welche Softwareprogramme, -programmteile, Parameter(-sätze) oder Betriebssystemteile werden geschützt?

- Beschreibung, wie Speicher mit Softwareprogrammen oder Parametern vor Austausch oder Beschreiben geschützt sind

Parameterschutz

- Liste aller gerätespezifischen Parameter mit Name, Kurzbeschreibung, Wertebereich, Normalwert, Speicherort und Anzeige- und Änderungsmöglichkeiten
- Beschreibung der Schutzmaßnahmen der gerätespezifischen Parameter:
  - Welche Schutzmaßnahmen werden für welche gerätespezifischen Parameter verwendet?
  - Wann kommt das Verfahren zum Einsatz?
  - Wie ist die Reaktion des Systems im Fehlerfall?

Softwareauthentizität und Darstellung der Messwerte (nur bei Vorliegen von rechtlich nicht relevanter Software)

- Nennung der anzeigbaren rechtlich relevanten Messwerte
- Beschreibung, wie sichergestellt wird, dass ausschließlich die rechtlich relevante Software die rechtlich relevanten Messwerte anzeigt bzw. ausgibt und dass die angezeigten rechtlich relevanten Messwerte vom rechtlich relevanten Messsensor oder von anderen rechtlich relevanten Hardwarekomponenten stammen
- Beschreibung, wie sichergestellt wird, dass die Anzeige der rechtlich relevanten Messwerte und sonstigen Informationen nicht mit denen, die von rechtlich nicht relevanten Anwendungen oder Programmteilen erzeugt werden, verwechselt werden können (bei Betriebssystemen z.B. wie wird verhindert, dass Fenster mit rechtlich relevanten Anzeigen überdeckt werden)

Für jede **Hardwarekomponente, die rechtlich relevante Messwerte dauerhaft speichert** und für jeden **Transport rechtlich relevanter Messwerte zwischen zwei rechtlich relevanten Hardwarekomponenten** muss folgendes dokumentiert sein:

Vollständigkeit der gespeicherten/transportierten Messwerte

- Liste aller Messwerte, mit Name, Kurzbeschreibung, Format, Einheit
- Angabe des Speicherorts bzw. des Übertragungsweges

Schutz der gespeicherten/transportierten Messwerte vor zufälliger oder unabsichtlichen Änderung

- Nennung des Verfahren zum Schutz gegen unabsichtliche Änderungen (z.B. Checksumme)
- Nennung der Software-Module, die die Messwerte speichern oder absenden und die Schutzmaßnahmen anbringen sowie der Software-Module, die die Messwerte lesen oder empfangen und die Maßnahmen kontrollieren
- Angabe, welche Messwerte geschützt werden
- Verhalten im Fehlerfall
- Absicherung kritischer Benutzeraktionen (z.B. Löschen/Ändern der Messwerte)

Schutz der gespeicherten/transportierten Messwerte vor absichtlichen Änderungen

- Nennung des Verfahrens zum Schutz der Messwerte vor absichtlichen Änderungen (bei gespeicherten Werten: z.B. Schutz vor Speicheraustausch, Verwendung von Checksummen oder Hashwerten mit geheimen Startwerten, bei transportierten Werten: Hashwerte mit geheimen Startwerten, Verschlüsselungen, auch Hardwaremaßnahmen, z.B. Siegel)
- Nennung der Software-Module, die die Messwerte speichern oder absenden und die Schutzmaßnahmen anbringen sowie der Software-Module, die die Messwerte lesen oder empfangen und die Maßnahmen kontrollieren

- Angabe, welche Messwerte geschützt werden
- Verhalten bei Verletzung der Datenintegrität
- Absicherung kritischer Benutzeraktionen (z.B. Löschen/Ändern der Messwerte)

Zuordnung der gespeicherten/transportierten Messwerte

- Beschreibung, wie eine Messung identifiziert wird
- Beschreibung, wie die gespeicherten/transportierten Messwerte einer Messung zugeordnet werden
- Beschreibung, wie die Zuordnung vor Veränderungen geschützt ist
- Bei gespeicherten Messwerten: Beschreibung, ob und wie die Zuordnung zur Messung auch bei rechtlich relevanten Ausgaben (z.B. Anzeigen, Ausdrucke, Belege) erkennbar ist
- Bei transportierten Messwerten: Beschreibung, wie die Empfängerkomponente oder –Software die Herkunft der empfangenen Werte ermitteln kann (z.B. Seriennummer des Absenders)

Geheimhaltung der Schlüssel

- Falls geheime Schlüssel, Startwerte, Polynome o.ä. verwendet werden: Beschreibung, wie diese vor Auslesen, Löschen und Veränderung geschützt sind

Automatisches Speichern

- Beschreibung, inwieweit die Speicherung der Messwerte automatisch erfolgt
- Falls der Benutzer Messungen verwerfen oder das Speichern verzögern kann: Beschreibung der dafür geltenden Bedingungen oder Regeln

Speicherkapazität und -dauer

- Umfang der gespeicherten Messwerte mit ihren genauen Längenangaben
- Kapazität des verwendeten Speichermediums und ggf. Beschreibung, wie es ausgetauscht werden kann
- Angabe der Anzahl speicherbarer Messungen (absolute Angabe oder Berechnungsformel)
- Maßnahmen bei Erreichen ober Überschreiten der Speicherkapazität oder bei Fehlen des Speichermediums
- Schutzmaßnahmen vor vorzeitigem Löschen von gespeicherten Messwerte

Übertragungsverzögerung und Verfügbarkeit der Übertragungsdienste

- Beschreibung, wie der Empfänger bei Verzögerungen des Transports von Messwerte reagiert
- Falls Messwerte während des Transports nicht verloren gehen dürfen, muss beschrieben werden
  - Wie wird der Benutzer von der Unterbrechung des Transports abgehalten?
  - Wie erfolgt eine Rückmeldung über den erfolgreichen/nicht erfolgreichen Transport?
  - Wie werden transportierte Messwerte zwischengespeichert für eine eventuelle Übertragungswiederholung?
  - Was passiert, wenn Zwischenspeicher keine Messwerte mehr aufnehmen kann?
  - Wie wird eine verlorene Verbindung entdeckt und ggf. wiederaufgenommen?

Ist **während des laufenden Betriebs** eines Seriengeräts **eine Aktualisierung seiner rechtlich relevanten Software** vorgesehen, die **ohne einen Siegelbruch** (und damit ohne eine anschließende Eichung) ablaufen soll, muss diesbezüglich folgendes dokumentiert sein:

Download-Mechanismus

- Beschreibung des Download-Mechanismus
  - Wie weit läuft der Mechanismus automatisch ab?

- Welcher Teil der Software wird ausgetauscht, welcher nicht?
- Wie wird die neue Software nach dem Download in Betrieb genommen?
- Welche vorhandenen Schutzmaßnahmen werden für den Download außer Betrieb genommen? Wann und in welcher Form werden sie wieder in Kraft gesetzt (nach erfolgreichem/nicht erfolgreichem Download)?
- Welche Kontrollen oder Überwachungen sind während des Download-Prozesses vorgesehen?
- Welche Folgen haben ein Fehler oder eine Unterbrechung des Downloads?
- Wie wird sichergestellt, dass während eines Download-Vorgangs rechtlich relevante Funktionen und Daten nicht beeinträchtigt oder verfälscht werden können?
- Gibt es länderspezifisch Sperrmöglichkeiten für den Download?
- Wie viele Downloads, Downloadversuche bzw. fehlgeschlagene Downloads sind erlaubt?

Authentifizierung und Integrität der heruntergeladenen Software

- Beschreibung der Überprüfung, dass die neu geladene Software die richtige/korrekte, zu dem betreffenden Messgerät passende Software ist
- Beschreibung der Integritätsprüfung der geladenen Software
- Beschreibung der Reaktion des Systems im Fehlerfall

Rückverfolgbarkeit des Downloads rechtlich relevanter Software

- Art der Protokollierung des Downloads
- Beschreibung des Protokollspeichers (Größe, sowie Schutz vor Änderung, Löschen oder Ausbau)

Für jede **Hardwarekomponente, die rechtlich relevante und rechtlich nicht relevante lauffähige Programme enthält**, wird folgende Zusatzdokumentation benötigt:

Umsetzung der Softwaretrennung

- Beschreibung der Programmstruktur, aus der hervorgeht, welche Programmteile den rechtlich relevanten und welche den rechtlich nicht relevanten Teil der Software bilden (z.B. Klassen/Objekte, Dateien, Bibliotheken).
- Beschreibung, wie die rechtlich relevante Software vor Änderung oder Austausch und unzulässiger Beeinflussung geschützt ist, falls die rechtlich nicht relevante Software im Betrieb geändert bzw. ausgetauscht werden kann.

Gemischte Anzeige

- Wenn rechtlich relevante und rechtlich nicht relevante Software das gleiche Ausgabemedium nutzen: Wie können die Ausgaben unterschieden werden?

Wechselwirkung zwischen rechtlich nicht relevanter und rechtlich relevanter Software

- Beschreibung aller Wechselwirkungen (z.B. Befehle, Datenflüsse) zwischen der rechtlich nicht relevanten Software und der rechtlich relevanten Software.

Für **Messgeräte nach MID Anhang III** müssen zusätzliche Dokumente geliefert werden, ggf. entsprechend Abschnitt 10 des WELMEC-Leitfadens 7.2.