第2次委員会草案（2CD）- マーク付き版

プロジェクト：	**OIML D31**：2008の改訂
表題：	ソフトウェア制御計器に対する 一般的要件
日付：	2018年11月6日
文書番号：	TC5_SC2_P3 N028
置き換わる文書：	TC5_SC2_P3 N019
プロジェクトグループ：	OIML TC 5/SC 2/p 3
コンビナーシップ：	ドイツ
コンビナー：	マルコ・エシェ　＋ フェデリコ・グラッソ・トレ

次の目的のためにPメンバー及びOメンバー並びにリエゾン国際機関及び外部機関に配布：

	討議（期日及び会議の場所）：
	コメント提出期限：
X	投票（Pメンバーだけ）及びコメント提出期限：2019年2月6日

文書全体にわたる変更点リスト：

ドルドレヒトの会合で話し合われたすべての変更は実施された。

サブグループ 1“検定方法及び手段”の成果は，第 7 節及びその各項の中に組み込まれた。

サブグループ 2“オペレーティングシステム要件”の成果は，5.2.5 及びその各項の中に組み込まれた。

審査／検定／妥当性確認を取り巻く用語は，現在の VI 及び V2 の定義に適合させるために更新された。

型式評価／型式審査，報告書／証明書に関連する用語の使用は，OIML 認証制度の現行の B18 の記述に適合させるために更新された。

すべての節は，有効な規準用語を用いるために必要な場合に，レビューを行い変更された。

重複語（ソフトウェアモジュール，ソフトウェア部分，プログラムなど）の使用は，できるだけ一貫して定義されている用語及び定義を用いるために最小限に抑えられた。もはや使用されていない用語は，3.1 及び附属書 C から削除された。

機能及びコマンドに関連する用語は，文書全体を通じて同じ意味をもつことを確実なものとするために修正された：インターフェースを通じて機能を起動させるコマンド

略語は，文書中で 1 回又は 2 回を超えて用いられている場合に限り，3.2 の中に列記されている。そうでない場合は，略さない語が用いられている。

用語“汎用コンピュータ”は，現在及び今後の展開のための余地を作るために，“汎用装置”に更新された。

目次

まえがき.....5

1 はじめに.....5

2 適用の範囲及び分野.....5

3 用語及び定義.....6

3.1 一般用語.....6

3.2 略語.....12

4 OIML 勧告の起草にこの文書を使用するための説明.....13

5 ソフトウェア適用に関する計量器への要件.....13

5.1 一般要件.....13

5.2 構成に固有の要件.....18

6 型式評価.....31

6.1 型式評価提出文書.....31

6.2 評価手続きへの要件.....32

6.3 検定及び評価方法.....33

6.4 ソフトウエア評価手順.....38

6.5 被試験計器（EUT）.....42

7 計量器の検定.....42

8 リスク評価.....43

附属書 A 参考文献.....45

附属書 B ソフトウェア試験報告書の事例.....47

附属書 C 索引.....54

まえがき

国際法定計量機関（OIML）は世界的な政府間組織で，加盟国の国内計量業務部門又は関連組織によって適用される規則及び計量管理を整合化することを主な目的としている。OIML 出版物の主なカテゴリーは，次の通りである。

- **国際勧告（OIML R）**。これは，一定の計量器に要求される計量特性を策定するモデル規則であり，それへの適合を検査する方法及び設備を規定している。OIML 加盟国は，これらの勧告をできる限りの範囲で実施しなければならない。
- **国際文書（OIML D）**。これは，本来参考的性格のもので，法定計量分野における作業の整合化及び向上を目的としている。
- **国際ガイド（OUML G）**。これは，本来参考的性格のもので，法定計量分野にある要求事項を適用するためのガイドラインを提供することを目的としている。
- **国際基本出版物（OIML B）**。これは，さまざまな OIML の構造及びシステムの

OIML 勧告案，OIML 文書及び OIML ガイドは，加盟国からの代表者で構成する技術委員会またはその小委員会にとながったプロジェクトグループによって作成される。特定の国際機関及び地域機関も諮問ベースで参加している。OIML と特定機関，例えば，ISO 及び IEC などとの間で，矛盾した要求事項を避けることを目的として，協力協定が締結されている。この結果，計量器の製造事業者，計量器の使用者及び試験所などが，OIML の出版物及び他の機関による出版物を同時に適用することができる。

国際勧告，国際文書，国際ガイド及び国際基本出版物は，英語（E）で出版され，フランス語（F）に翻訳され，定期的に改訂されている。

さらに，OIML は**用語集（OIML V）**を出版し，またその出版イ参加していて，定期的に法定計量専門家に**専門家報告書（OIML E）**の執筆を委託している。専門家報告書は，上方位と助言を与えることを目的としていて，その著者自身の観点からだけで執筆されている，技術委員会または分科会が関与することなく，OIML の関与もない。従って，これは OIML の見解を必ずしも代表するわけはない。

この出版物，OIML D 31，YYYY 版（E）は，OIML 技術小委員会 TC 5/SC 2 *ソフトウェア*によって作成された。これは，YYYY 年の国際法定計量委員会によって最終出版が承認された。

OIML による出版物は，OIML のウェブサイトから PDF ファイル形式でダウンロードできます。また，OIML 出版物についての追加情報は，下記 OIML 本部から入手できます：

Bureau International de Métrologie Légale
11， rue Turgot – 75009 Paris – France
電話：33 (0)1 48 78 12 82 及び 42 85 27 11
Fax： 33 (0)1 42 82 17 27
E-mail：biml@oiml.org
インターネット：http://www.oiml.org

ソフトウェア制御計量器に対する一般的要件

1 はじめに

この国際文書の主な目的は，OIML 勧告の対象となる計量器のソフトウェア関連機能に対して，適切な要件を決定するための指針を OIML 技術委員会及び分科会に提供することである。

さらに，この国際文書は OIML 加盟各国の国内法における OIML 勧告実施における指針を提供することができる。

2 適用の範囲及び分野

2.1 この国際文書は，法定関連計量器のソフトウェア関連機能及び厳しさに適用する一般要件を規定し，計量器のこれらの要件への適合性検証のための指針を与える。

2.2 この文書は，特定カテゴリの計量器に適用する OIML 勧告（以下「関連勧告」という）に，特定のソフトウェア要件及び手順を策定する際の基礎として，OIML 技術委員会及び小委員会が考慮しなければならないものである。

2.3 この文書に規定した指示内容は，ソフトウェア制御計量器又はその構成部品にのみ適用する。

備考：

- この文書は，ソフトウェア制御計量器に特有のすべての技術的要件をカバーしているわけではない。それら要件は，例えば，はかり，水道メーターなどに対しては，関連勧告で規定されるべきである。
- この文書は，データの安全保護に関してかなりの観点について取り扱っている。加えて，この分野に対しては国内規制を考慮する必要がある。

3 用語及び定義

この国際文書で用いる定義の中には，国際計量基本用語集 第 3 版（OIML V 2-200: 2012 [1]），国際法定計量用語集（OIML V 1:2013 [6]），OIML 国際文書 *計量器のための一般的要件－環境条件*（OIML D 11:2013 [2]）及び複数の ISO/IEC 国際規格に準拠している者がある。この文書の目的のためには，次の定義及び略語を適用する。

3.1 一般用語

3.1.1

監査証跡

事象の時刻印付き情報記録を含む連続データファイルで，例えば，計量器のパラメータ変更，ソフトウェア更新又は法定関連で，かつその計量特性影響を与える可能性のあるその他活動。

[OIML V 1:2013，6.05]

3.1.2
身元認証

利用者，プロセス又は計量器の宣言又は申し立てた身元の正当性を確認すること

備考： この用語は，ダウンロードされたソフトウェアが，証明書の所有者に由来するこ と を確認する際に必要となることがある。

3.1.3
信憑性

身元認証過程の結果（合格又は不合格）

3.1.4
専用目的の装置

計量作業の特定の目的のために組み立てた装置

備考： オペレーティングシステムに対する非宣言インターフェースは，アクセスできないか，又は存在しない。

3.1.5
点検機能

計量器に組み込まれていて，有意な誤りを検出し，それへの対処を可能にする機能。

備考：“対処する”とはその計量器による適切な反応（発光信号，音信号，計量プロセスの遮断 な ど）のことをいう。

[OIML V 1:2013，5.07 から引用]

3.1.6
通信インタフェース

計量器, 計量器の構成部品又はその他の外部システムの間で情報を渡すことを可能にする計器の一部

備考1： 通信インタフェースは，有線，光学，無線，その他の可能性があり，それらは，一般的に，特定のプロトコルを用いるように設計されている。

備考2： この定義には，ソフトウェア部品間の通信は含まれない。

3.1.7
暗号化証明書

計量器又は人物に属する公開鍵に加え主体を特定する識別，例えば，計量器のシリアル番号，人の名前又は個人識別番号（PIN）に加えて有効期限を含むデータセット。

3.1.8
暗号化手法

未認定の人物から，情報を隠蔽することを目的とした暗号化／復号化などの手段，例えば，暗号学的ハッシュ又は電子署名（3.1.13 を参照）。

3.1.9
データ領域

各プログラムがデータ処理のために必要とするメモリ領域。

備考： データ領域は，一つのソフトウェアモジュールにのみ又は複数のソフトウェアモジュールに付属することができる。

3.1.10
装置固有パラメータ

個々の計量器に依存する値を持つ法定関連パラメータ。

備考： 装置固有のパラメータは，補正パラメータ（例えば，スパン調整，その他調整値又は補正値）及び設定パラメータ（例えば，最大値，最小値，計量単位，など）からなる。

[OIML V 1:2013，4.12]

3.1.11
耐久性

使用期間にわたってその性能特性を維持する計量器の能力。

[OIML V 1:2013, 5.15]

3.1.12
電子計量器

電子的手段及び／又は電子部品を使って電気的又は非電気的量を計量することを目的とした計量器。

備考： 本文書の目的では，計器は，計量管理対象である場合，計量器の一部とみなされる。
[OIML D 11:2013, 3.1]

3.1.13
電子署名

ソフトウェア又はデータの発信元の検証，すなわち，その信憑性の証明又はそのソフトウェア若しくはデータが変更されていないことの確認，すなわち，その完全性の証明を目的として，ソフトウェア又はデータに付け加えられるソフトウェア手段。

*備考1：*電子署名については，一般的に公開鍵システム，すなわち，一方だけは秘密にする必要があり，もう一方は公開することができる一対の鍵が用いられる。

*備考2：*秘密鍵は，ソフトウェア又はデータのセキュリティを保護する際に用いられる。公開鍵は，使用前にソフトウェア又はデータを検証するときに用いられる。

*備考3：*検証するためのインスタンスは，保護するためのインスタンス（3.1.7 を参照）が公開鍵の信憑性を確実なものにしていることの暗号化証明書を必要とすることがある。

3.1.14
表示の誤差

計量器の表示値から基準量の値を引いたもの。

備考： この基準値は，場合によっては，（取決めによる）真の量の値と呼ばれることがある。ただし，OIML V2-200: 2012，2.12，備考 1 も参照のこと。
[OIML V 1:2013，0.04]

3.1.15
エラーログ

計量器の計量特性に影響を与える故障又は有意欠陥の情報記録を含む連続データファイル。

3.1.16

事象

計量器パラメータ，調整係数の修正又はソフトウェアモジュールの更新が行われる処置。
[OIML V 1:2013, 6.06]

3.1.17
事象計数器
事象が発生するたびに繰り上がるリセット不可能な計数器。

3.1.18
実行コード

計量器／構成部品（EPROM，ハードディスクなど）のコンピュータシステムに組み込まれたソフトウェア又はファームウェアの中で利用できるデジタル情報。

備考： このコードは，計量器の中央演算処理装置（CPU）によって解釈され，特定の論理，算術，

復号，又はデータ転送動作に変換される。

3.1.19
誤り

計量器の指示誤差と固有誤差との間の差異

備考 1： 主として，誤りは電子計量器に含まれる又は通過して流れるデータの不要な変化の結果である。

*備考*2： 定義から，“誤り”は，計量単位又は相対的数値，例えば，パーセンテージのいずれか で表される数値であることが分かる。

[OIML V 1:2013，5.12]

3.1.20
ハッシュ関数

大きな（非常に大きな場合もある）領域から，より小さな値域に値を位置付ける（数学的）関数。“良い”ハッシュ関数は，その領域の値の（大きな）セットに関数を適用した結果がその値域全体にわたって一様に（かつ，一見ランダムに）分散しているような関数である。

[ISO/IEC 9594-8:2014] [3]

3.1.21
（プログラム，データ又はパラメータの）完全性

プログラム，データ又はパラメータが，使用中，伝送中，保存中，修理中又は保守中に未認定又は意図しない変更に晒されていないことの保証。

3.1.22
インタフェース

二つの機能単位間の共有する境界で，必要に応じて，機能，物理的相互接続，信号交換及びその他の単位特性に関連するさまざまな特性によって適切に定義される。

[ISO 2382-9:1995] [4]

3.1.23
割り込み可能累積測定
通常の動作中に簡単かつ迅速に停止させることができる，ある物質の量の値の累積測定のプロセス

備考1： 例には次が含まれる：a) 不連続加算自動はかり，b) 燃料計量分配装置

備考2： 割り込み不能累積測定（3.1.29）も参照。

3.1.24
固有誤差
標準状態の下で決まる表示誤差
[OIML V 1:2013, 0.06]

3.1.25
法定関連

法規制の対象

[OIML V 1:2013, 4.08 の中で変更されることになっている]

3.1.26
法定関連パラメータ

法定管理対象の計量器／構成部品，（電子式）装置，ソフトウェア又はモジュールのパラメータ。

備考： 次のタイプの法定関連パラメータは，識別可能である：*型式特有のパラメータ及び装置特 有のパラメータ。*

[OIML V 1:2013, 4.10 の中で変更されることになっている]

3.1.27
法定関連ソフトウェア部分
法定管理の対象となっている計量器／構成部品の *ソフトウェアモジュール*のすべて。

3.1.28

（計量器の）最大許容誤差

仕様又は規制によって所定の測定，計量器又は計量システムに対して許容された既知標準量値に関した測定誤差の極値。

[O IML V 1:2013, 0.05]から引用

3.1.29
計量器

単独で又は 1 台以上の補助装置と共に測定を行うために使用する装置。
[OIML V 1:2013, 0.10]から引用

3.1.30
割り込み不能累積測定

明確な終わりの無い累積的で連続した測定プロセスで，その測定の結果を改ざんすることなく，使用者又は操作者が停止及び再継続することができないもの。

備考 1： 例には次が含まれる：a) 連続加算自動はかり，b) ヒートメータ

備考 2： 割り込み可能累積測定（3.1.23）も参照。

3.1.31
保護インターフェース

容認できない影響を防ぐために法定関連ソフトウェア部分へのすべてのデータフローを処理する法定関連ソフトウェアモジュール

3.1.32
封印

部品，ソフトウェア，などの未認定修正，再調整，削除に対して計量器を保護するための手段。

備考： ハードウェア，ソフトウェア又はその両者の組み合わせによって達成することができる。

[OIML V 1:2013, 2.20]

3.1.33
保全（機密保護）

ハードウェア又はソフトウェアへの不正なアクセスを防ぐ手段

[OIML V 1: 2013, 2.21]

3.1.34
有意欠陥

計量器の適合性に対する望ましくない影響をもつ事象又は誤り

備考： 有意欠陥の例には次が含まれる：a) 監査証跡の削除，b) 不正なパラメータの変更，c) 不正な更新

3.1.35
ソフトウェア審査

特定の手順に従って，ソフトウェアの一つ以上の特性を決定することからなる技術的作業（例えば，技術文書の解析又は管理条件下でのプログラムの作動）。

3.1.36
ソフトウェア識別

検討中のソフトウェア又はソフトウェアモジュールを表す判読可能な文字の列（例えば，バージョン番号，チェックサム）。
備考： これは，使用中の計量器で点検可能である。

3.1.37
ソフトウェアインタフェース
プログラムコード及び専用のデータ領域。*ソフトウェアモジュール*間でデータの受け取り，選別又はデータ伝送を行う。

備考1： ソフトウェアインタフェースは，必ずしも法定関連ではない。
備考2： ソフトウェアインタフェースは，データ交換及びコマンド伝送に使用する 2 個以上のソフトウェアモジュール間のインタフェースである。

[OIML V 1:2013, 6.03]

3.1.38
ソフトウェアモジュール

他の実体と関係のあるデータ領域を含むプログラム，サブルーチン，ライブラリ，パラメータ又はデータ・セット及びその他オブジェクトなどのソフトウェア実体。
備考： 計量器のソフトウェアモジュールは，一つ以上のソフトウェアモジュールから成っている。

3.1.39
ソフトウェア保護
ハードウェア又はソフトウェアで実現された封印によるソフトウェア又はデータ領域の保護。

備考： ソフトウェア変更のためのアクセスを得るためには，その封印を除去，損壊又は破壊しな　　ければならない。
[OIML V 1:2013, 6.04]

3.1.40
ソフトウェア分離
計量器のソフトウェアの分離で, これは*法定関連部分*及び非法定関連部分に分けることができる。

備考: これら部分は，ソフトウェアインタフェースを介して通信する。

[OIML V 1:2013, 6.02]

3.1.41
ソースコード
判読可能かつ編集可能な形式（プログラミング言語）で作成したコンピュータ・プログラム。

備考： ソースコードは，実行コードにコンパイルされるか又は解釈される。

3.1.42
データ保存装置
測定完了後にその測定データを保存し，後に法定関連目的（例えば，商取引の終結のため）で利用できるように保存しておくために使用する装置。
[OIML V 1:2013, 6.07]

3.1.43

時刻刻印

例えば，ある測定又は事象が発生した日付及び／又は時刻を指す秒数又は日付及び時刻の文字列で，独特の値。

3.1.44
測定データの伝送

通信ライン又はその他手段を介してさらに処理する受信器のもとへの測定データの電子的転送。

3.1.45
型式（type）（型式（pattern））評価

計量器の識別された型式（type）（型式（pattern））の一つ以上の供試器の適合性評価手順で，その結果，評価報告書 ／又は証明書が得られる。
[OIML V 1:2013, 2.04]

3.1.46
型式固有パラメータ

計器の型式のみに依存する値を持つ*法定計量関連パラメータ*。
備考： 型式固有パラメータは，法定計量関連ソフトウェアの一部である。
[OIML V 1:2013, 4.11]

例：
水以外の液体の計量器を考えると，タービンの型式評価時に確定したタービンの動粘性率範囲は型式固有のパラメータである。同じ型式の製造されたタービンは，すべて同じ動粘性率範囲をもつ。

3.1.47
汎用装置

特定目的のために作られたものではなく，ソフトウェアによって計量作業に適応可能な装置。

備考： この種の装置は，オペレーティングシステムに対する非宣言インターフェースをもつことがある。

3.1.48
ユーザインタフェース

人間と計量器又はそのハードウェア構成部品若しくはソフトウェアモジュールの間で情報交換を可能にするインタフェース

備考： その例は，スイッチ，キーボード，マウス，ディスプレイ，モニタ，印字装置，タッチスクリーン，スクリーン上のソフトウェアウィンドウを生成するソフトウェアである。
[OIML V 1:2013, 6.08 の中で変更されることになっている]

3.1.49
検定

所与の品目が規定要件を満たしていることの客観的証拠の提供。
[OIML V 2-200:2012, 2.44]から引用

3.1.50

計量器の検定

（型式評価以外の）適合性評価手順で, 検定証印の貼付及び／又は検定証明書の発行をもたらす。

備考： OIML V2-200:2012, 2.44 も参照。

[OIML V 1: 2013, 2.09]

3.2 略語

EUT 被試験機器
IEC 国際電気標準会議
ISO 国際標準化機構
IT 情報技術
MPE 最大許容誤差
OIML 国際法定計量機関
PG プロジェクトグループ

4 OIML 勧告の起草にこの文書を使用するための説明

4.1 この文書の規定は, 新規の OIML 勧告及び改訂中の OIML 文書に対してのみ適用する。OIML プロジェクトグループ（技術委員会，小委員会）は，ソフトウェア関連要件を策定するため適用可能な OIML 勧告の他の技術的及び計量的要件に加えて, このガイダンスを使用すべきである。

4.2 すべての参照文書は改訂対象であり，この文書の使用者は，その参照文書の最新版を適用できる可能性を探ることが勧められる。

4.3 この文書の目的は，OIML 勧告を起草する責任を負うプロジェクトグループにあらゆる種類の計量器及びすべての適用分野の要求を網羅するのに適したーある程度は, 異なる（リスク）レベルのー要件集を提供することである。そのプロジェクトグループは，どのリスクレベルが適しているか及びこの文書の関連部分を起草中の OIML 勧告にどのように取り入れるのかを決定しなければならない。第 8 節に，この課題を行うためのいくつかの助けとなるものが与えられている。

4.4 PG は，特定型式の計器に対して，どの影響が容認できないと見なされるかを定義す ることが望ましい。

5 ソフトウェア適用に関する計量器への要件

5.1 一般要件

この文書の出版時点では，その一般要件は情報技術（IT）の最先端状態を表している。それらは，原則として，計量器のソフトウェア制御計量器及び計量器の構成部品のすべての種類に適用される。それらは，すべての勧告において考慮されるべきである。これらの一般要件とは違って，構成に固有の要件（5.2）は，ある種の計量器に対して又はある適用分野において一般的でない技術的特徴を取り扱っている。

以下の例では，当てはまる場合，標準的及び一段高いリスクレベルの両方を示している。この文書における考え方は次の通りである：

(I) 標準リスクレベルの場合の容認可能な技術的解決策

(II) 一段高いリスクレベルの場合の容認可能な技術的解決策（8 を参照）

5.1.1 ソフトウェア識別

計量器／構成部品の法定関連ソフトウェアは，明確に識別できなければならない。その識別は，二つ以上の部分からなっていることがあるが，そのうち少なくとも一つの部分は，専ら法定目的に供するものでなくてはならない。

識別は，計量器によって表示又は印字されなければならない。

- コマンドで
- 動作中に
- 電源を入切できる計量器については起動時

計量器／ 構成部品がディスプレイも印字装置も備えていない場合は,別の構成部品上で表示／印字するため通信インタフェースを介して識別を送らなければならない。

例外として，次の条件のすべてが成立する場合，計量器／構成部品上へのソフトウェア識別の刻印が容認可能な解決策である：

(1) ユーザインタフェースがディスプレイ上にソフトウェア識別の表示を起動する制御能力を持っていない又はそのディスプレイがソフトウェア識別を技術的に表示できない（アナログ指示装置又は電子機械式計数器)。

(2) 計量器／構成部品が，そのソフトウェア識別を通信するためのインタフェースを持っていない。

(3) 計量器／構成部品の生産後，そのソフトウェアの変更ができないか，又はハードウェアも変更された場合のみ可能である。

ソフトウェア識別が当該計器上に正しくマークされていることを確実になものとしなければならない。

関連勧告は，この例外を可能又は不許可とすることが望ましい。

ソフトウェアが多少なりとも部分的に変更される場合，新たなソフトウェア識別が求められる。

ソフトウェア識別及びその識別手段（例えば，ソフトウェアのバージョン，ハッシュ値，チェックサム）は，その証明書の中に記載されていなければならない。ソフトウェア識別をどのように表示又は印字させるかの説明は，証明書の中になければならない。

備考: 稼働中の計量器はそれぞれ，承認済型式に適合していなければならない。ソフトウェア 識別によって市場監視者及びその測定で影響を受ける関係者が，当該計器が適合してい るかどうかを判定することができる。

例：

(I) ソフトウェアは，インストールされたバージョンを明白に識別文字列又は数字を含んでいる。ボタンを押したとき，計量器のスイッチを入れたとき又はタイマーによって周期的にスイッチが入ったとき，この文字列が計量器のディスプレイに伝送される。

バージョン番号は，次の構造 A.Y.Z を持っていることがある。流量（フロー）コンピュータを考えると，A はパルスを数える中核ソフトウェアのバージョンを表し，Y は変換関数のバージョン（温度について無条件，15 ℃，20 ℃）を表し，Z はユーザインタフェースの言語を表す。

(II) ソフトウェアは，実行コードのチェックサムを計算し，その結果を識別として， (I) の中の文字列の代わりに，又は文字列に加えて提示する。

5.1.2 アルゴリズム及び機能の正確さ

計量器の測定アルゴリズム及び機能は，その所定の用途及び機器型式にとって適切で，機能的に正しくなければならない（アルゴリズムの精度，特定の規則に従った価格計算，丸めアルゴリズム，など)。

特定の勧告又は国内法令によって要求される計量結果及び付随情報は，正確に表示又は印字されなければならない。

計量試験，ソフトウェア試験又は（項 6.3 に記述した）ソフトウェア審査のいずれかによってアルゴリズム及び機能を審査することが可能でなければならない。

隠された又は文書化されていない機能があってはならない。

5.1.3 ソフトウェア保護

5.1.3.1 誤用防止

計量器は，意図しない，偶発的又は故意の誤用の可能性が最小となるように構成されていなければならない。この文書の枠組では，このことは特にソフトウェアに当てはまる。測定結果の提示は，すべての関係者にとって曖昧さのないものであることが望ましい。

備考： ソフトウェア制御計器は，その機能性が複雑なことが多い。使用者には，正しい使用及び正確な測定結果を得るためのよい手引き書が必要である。

例：

使用者は，メニューで指導される。法定関連機能は，このメニューの中で 1 つの枝に組み合わされている。ある動作でどの測定値を消失しても，その使用者に警報が出て，その機能が実行される前に別の動作を実行するよう要求される。5.2.2 も参照。

5.1.3.2 介入の証拠

5.1.3.2.a ソフトウェアは，介入（例えば，ソフトウェアの更新，パラメータの変更）の証拠が利用できるような方法で保護しなければならない。ソフトウェアは，未認可の修正，ローディ

ング又はメモリ装置交換による変更に対して保全されていなければならない。ソフトウェアをローディングするオペレーティングシステム又はオプションを持っている計量器を保全するには，機械的封印又は他の技術的手段が必要である可能性がある。

例：

(I)/(II) メモリ装置を含む筐体は封印されているか又はそのメモリ装置がプリント基板上で封印されている。

(II) その装置の書き込み許可入力が封印可能なスイッチによって無効化されている。その回路は，接点の短絡で書込み防止機構を無効にできない方法で設計されている。

(I) 計量器が，二個の構成部品で構成されていて，そのうち一つは封印された筐体に組み込まれた主要計量機能を持っている。もう一つの構成部品は，オペレーティングシステムを搭載した汎用装置である。表示などの機能の中には，この汎用装置のソフトウェアに組み込まれているものがある。その汎用装置上のソフトウェアの入れ替えを防ぐために，構成部品と汎用装置間のデータ伝送は，暗号化される。復号化のための鍵は，汎用装置の法定計関連ソフトウェアの一部であるプログラムの中に隠蔽されている。このプログラムだけがその鍵を知っており，その測定値の読み出し，復号化及び使用をすることができる。他のプログラムは，その測定値を復号化できないので，このために使用することができない（5.2.1.2.d の例も参照）。

5.1.3.2.b 明確に文書化された機能（6.1 を参照）だけが，ユーザインタフェースによって起動させることができ，そのユーザインタフェースはその計器の計量特性に影響を与えない。

備考： 検査者は，これら文書化した機能すべてが容認可能かどうかを判定する。

例：

(I)/(II) ユーザインタフェースからのすべての入力は，入ってくるコマンドをフィルタ処理するソフトウェアモジュールに出力先変更される。それは，文書化した機能を起動させるコマンドだけを認めて，通過させ，それ以外はすべて廃棄する。このモジュールは，法定関連ソフトウェアの一部である。

5.1.3.2.c 計量器の法定関連特性を決定するパラメータは，未認定の改変に対して保全されなければならない。計量器の検定のために必要な場合，現行のパラメータ設定の表示又は印字が可能でなければならない。

備考： 装置固有パラメータは，型式評価後に調整又は選択可能なものがある。それらは，その計量器の特別動作モードにおいてのみ調整可能／選択可能であることが望ましい。

機器固有のパラメータは，保全されるもの（変更不能）及び権限保持者，例えば，計量器所有者又は製造事業者がアクセス可能なもの（調整可能／選択可能パラメータ）に分類することができる。

型式固有パラメータは，その型式のすべての供試器に対して同じ値である。それらは，その計量器の型式評価時に決定される。

例：

(I)/(II) 保全するべき装置固有パラメータは，不揮発性メモリに保存されている。そのメモリの書き換え許可信号は，封印可能なスイッチによって阻止されている。

この節の例 5.1.3.2.d (1) から(3) を参照。

5.1.3.2.d ソフトウェア保護は，機械的，電子的及び／又は暗号手段による適切な封印からなっていて，未認可介入を不可能又は明らかとなるようにする。

備考： 暗号化証明書を使用することができる。ソフトウェアは，信頼できる機関によって，電子署名を用いて，署名される。署名済みのソフトウェアの信憑性は，信頼できる機関の公開鍵を使い，証明書の署名を復号化することによって検証することができる。

例：

(1) 電子封印。計量器の法定関連パラメータは，メニュー項目で入力及び調整が可能である。ソフトウェアは，この種の事象毎にそれぞれの変更及び増分を認識する。この事象計数器値は，表示が可能である。この事象計数器の初期値は，計器上に耐久的にマークされる。その表示値が登録値と異なる場合，その計量器は未検定状態にある（破損封印に等しい）。

(2) (I)/(II) スイッチで保護されたメニューを介する場合を除いて，計量器のソフトウェアは，法定計量関連パラメータを変更する方法が無いように構成されている（例 5.1.3.2.a を参照）。このスイッチは，不活性位置で機械的に封印されていて，法定計量関連パラメータの変更を不可能にしている。

法定関連パラメータを変更するには，そのスイッチを作動させる必要があり，そうすることで必然的に封印を破らざるを得ないことになる。

(3) (II) 権限のある者による場合を除いて，法定計量関連パラメータにアクセスする方法が無いように，計量器のソフトウェアが作られている。パラメータメニュー項目にアクセスしたい者は，暗号化証明書の一部として，個人識別番号（PIN） を含む自分のスマートカードを挿入しなければならない。計器のソフトウェアはその証明書によって個人識別番号（PIN）の信憑性を検証することができ，そのパラメータメニュー項目に入ることを許可する。このアクセスは，この者の識別番号（又は少なくとも使用したスマートカードの識別番号）を含めて監査証跡に記録される。

5.1.4 ハードウェア機能の支援

5.1.4.1 有意欠陥の検出

関連勧告が，有意欠陥の検出機能を要求することがある。この場合，その計器の製造事業者に，そのチェック機能をソフトウェア又はハードウェア内に設計するか又はその計器のソフトウェア部分によってハードウェア部分が支援される手段を設けるよう要求しなければならない。

ソフトウェアが有意欠陥の検出に関わっていれば，適切な反応が要求される。例えば，関連勧告は，有意欠陥が検出された場合，その計器／構成部品を動作停止にするか，又はエラーログに警告／ 記録を生成することを規定することができる。

型式評価のため提出することになっている文書には，ソフトウェアが検出することになる有意欠陥及びその期待される反応のリストを含み，その動作を理解するのために必要な場合は，その検出アルゴリズムの説明を含まなければならない。

例：

(I) 起動する毎に，法定関連ソフトウェア部分が，プログラムコード及び法定関連パラメータのチェックサムを計算する。これらチェックサムの基準値は，予め計算されていて，その計器中に格納されている。その計算値と格納した基準値が一致しない場合は，法定関連ソフトウェア部分は実行を停止する。

割り込み不能累積測定の場合，，そのチェックサムは周期的に計算され，ソフトウェアタイマ

によって制御される。障害が検出された場合，そのソフトウェアはエラーメッセージを表示するか, 又は障害表示器のスイッチを入れて, エラーログにその有意欠陥の時刻を記録する。

(II) 起動する毎に，法定関連ソフトウェア部分は，プログラムコードの暗号化ハッシュ機能によって作成される値及び法定関連パラメータを計算する。ハッシュの基準値は，予め計算されていて，その計器中に格納されている。その計算値と格納した基準値が一致しない場合は，プログラムは実行を停止する。

割り込み不能累積測定の場合，ハッシュ値は，周期的に計算され，ソフトウェアタイマによって制御される。故障（障害）が検出された場合，ソフトウェアは，エラーメッセージを表示するか，又は故障（障害）表示器のスイッチを入れて，エラーログに有意な欠陥の時刻を記録する。

5.1.4.2 耐久性保護

OIML D 11:2013 [2] (5.1.3 (b) 及び 5.4) で扱っている耐久性保護機能をソフトウェア又はハードウェアで実現する又はハードウェア機能をソフトウェアで支援することを許容するかは，その製造事業者の選択である。その関連勧告で，適切な解決策を提案することができる。

ソフトウェアが耐久性保護に関与している場合, 適切な反応が求められる。例えば, 関連勧告で, その計器／構成部品が動作停止している又は耐久性が危険に晒されていることを検知した場合に警告／ 報告を生成することを規定することができる。

例：

(I)/(II) 計量器の中には，測定量の耐久性を保証する予め定めた時間間隔の後で調整を必要とするものがある。そのソフトウェアは，保守間隔が経過すると警告を発し，さらに一定の時間間隔を超えると測定を停止さえする。

5.1.5 時刻刻印

時刻刻印は，一貫性のある様式で示され，異なる 2 つの記録の簡単な比較及び経時的な進捗の追跡を可能にする。

時刻刻印は, 計器のクロックから読み出さなければならない。計器の種類又は適用地域に応じて, クロックの設定が法定関連となることがあり，適用されるリスクレベルに従って，適切な保護手段を講じなければならない（5.1.3.2.c を参照）。

独立型計量器の内部クロックは，このクロックを世界時標準に同期させるための手段がなにも組み込まれていない場合，かなり大きな不確かさをもつことがある。特定の適用分野により厳密な測定時刻に関する高精度の情報が求められる場合，特定の手段を用いて，内部クロックの信頼性を高める必要が生じることがある。

該当する場合，PG は，内部クロックの要件及び試験方法を定義することができる。

例：

（II） 計量器のクォーツ制御内部クロックの信頼性は，冗長性によって強化されている。タイマは，別の水晶に由来するマイクロコントローラのクロックによってインクリメン

ト　される。タイマの値が事前設定値，例えば 1 秒に達すると，マイクロコントローラの固
有　フラグが設定され，法定関連ソフトウェア部分の割り込みルーチンは，第 2 の計数器の
値　をインクリメントする。例えば 1 日の終わりに，ソフトウェアがクォーツ制御クロック
装　置を読み取り，その値とソフトウェアが計数した秒数の差を計算する。その差があらか
じ　め定義した限界値の範囲 内であれば，ソフトウェア計数器は，リセットされ，その手順
を　繰り返す。ただし，その差が限界値を超えている場合は，ソフトウェアは，適切な誤り
応　答を開始する。

5.2 構成に固有の要件

この節で規定した要件は，すべての法定応用分野では一般的でないことがあり得るが，情報技術における典型的な技術的解決策に基づいている。これらの要件に従うことで，ソフトウェア制御でない計器と同程度のセキュリティ及び型式への適合性を示す技術的解決策が可能である。

特定の技術が計量器に採用される場合には，次の固有の要件が必要になる。5.1 に記したものに加えて，それらを考慮しなければならない。

下記の例では，該当する場合，標準的なリスクレベル及び一段高いリスクレベルの両方が示されている。この文書での記法は次のとおりである：

(I) 標準的リスクレベルの場合に容認可能な技術的解決策

(II) 一段高いリスクレベルの場合に容認可能な技術的解決策（8 を参照）

5.2.1 法定関連部分の規定及び分離並びにインタフェースの規定

この要件は，計量器／構成部品が，他の計器／構成部品との，使用者との，又は計量器／構成部品内部の法定関連部分の他の他のソフトウェア部分との通信を行うためのインタフェースをもっている場合に適用される。

計量器の法定計量部分－ソフトウェア部分又はハードウェア部分に関わらずーは，その計量器の他の部分によって認められないほどの影響を受けてはならない。

勧告は，ソフトウェア ／ ハードウェア ／ データ又は法定関連であるソフトウェア／ハードウェア／データの一部を規定することができる。

5.2.1.1 構成部品の分離

5.2.1.1.a 法定関連機能を実行する計量器の構成部品は，識別，明確な定義及び文書化をされなければならない。これらはその計量器の法定関連部分を構成する。

備考： 審査官は，この部分が完全であり，その計量器の他の部分が以後の評価から除外できる かどうかを決定する。

例：

(1) (I)/(II) 電力量計には，測定値読み取り電子装置を接続するための光学インタフェースが備わっている。この計器は，関連するすべての量を保存し，十分な期間にわたって，読み取りができるように保持する。このシステムでは，電力量計だけが法定関連計器である。他に法定非関連装置があってもよく，5.2.1.1.b に適合するインタフェースに接続してもよい。データ伝送自体の保全（5.2.4 を参照）は要求されない。

(2) (I)/(II) 計量器は，次の構成部品からなっている：

- 重量又は体積を計算するデジタルセンサ
- 価格を計算する汎用装置
- 測定値及び支払い料金を印字する印字装置

すべての構成部品は，ローカルエリアネットワークで接続されている。この場合，デジタルセンサ，汎用装置及び印字装置は，法定計量関連構成部品であり，法定計量関連でない商用システムに随意的に接続されている。法定計量関連構成部品は，要件 5.2.1.1.b 及びー そのネットワークを介した伝送であるので－5.2.4 の要件も満たす。商用管理システムについての要件はない。

5.2.1.1.b 法定関連構成部品の機能及びデータが，他の法定非関連部分からのインタフェースを介して受け取ったコマンドによって許せない程の影響を受けないことを実証しなければならない。

このことは，各コマンドがすべての起動した機能又は構成部品内のデータ変化に明確な割り付けがなされていることを意味している。

備考： “法定関連”構成部品は，他の“法定関連”構成部品と相互に作用する場合，5.2.4 を参照すること。

例：

(1) (I)/(II) 電力量計（上記 5.2.1.1.a の例(1) を参照）のソフトウェアは，要求量を選択するコマンドを受け取ることができる。それは測定値と付加情報－例えば，時刻刻印，単位ーを組み合わせ，要求してきた装置にそのデータセットを送り返す。そのソフトウェアは，有効な定められた量を選択するコマンドを受理するだけで，エラーメッセージだけを返り返して，その他のコマンドはどれも捨て去る。データセットの内容に対する保全手段があり得るが，その伝送データセットは法規制対象でないので，それらは要求されることはない。

(2) (I)/(II) 封印された筐体内部に，電力量計の操作モードを決めるスイッチがある。一つのスイッチ設定が，保全モード及びその他の自由モードを示している（機械的封印以外の保全手段も可能である。例 5.1.3.2.a/.d を参照)。受信コマンドを解釈する際，ソフトウェアはこのスイッチの位置をチェックする。自由モードでは，ソフトウェアが受理するコマンド集合が保全モードに比べて拡張される（例えば，保全モードで捨てさるコマンドで校正因子を調整することが可能なことがある)。

5.2.1.2 ソフトウェア部分の指定及び分離

5.2.1.2.a 法定関連機能を実行する又は法定関連データを処理するすべてのソフトウェアモジュール（プログラム，サブルーチン，オブジェクト，など）は，計量器／構成部品の法定関連ソフトウェア部分を構成する。適合性要件をこの部分に適用して，5.1.1 に説明したように識別可能にしなければならない。

ソフトウェア分離が不可能であるか又は必要でない場合，そのソフトウェア全体として法定関連である。

例：

(I) 計量器は，測定値を表示するパーソナルコンピュータに接続した複数のデジタルセンサからなっている。パーソナルコンピュータ上の法定関連ソフトウェア部分は，法定関連機能（結果の提示を含む）を実現するすべての手順を一つの DLL（動的リンクライブラリ）にまとめることによって，法定非関連部分から分離されている。一つ又は複数の法定非関連アプリケーションが，このライブラリの中の機能を呼び出すことができる。これらの手順はデジタルセンサから測定データを受け取り，その測定結果を計算して，その結果をソフトウェアウィンドウに表示する。

5.2.1.2.b 法定計量関連ソフトウェア部分が他のソフトウェア部分と通信する場合，ソフトウェ

ア・インタフェースを定義しなければならない。すべての通信をこのインタフェースを介してのみ行わなければならない。その法定計量関連ソフトウェア部分及びそのインタフェースを明確に文書化しなければならない。そのソフトウェアの法定関連機能及びそのデータ領域すべては，型式評価当局が正しくソフトウェア分離を決定できるように記述されなければならない。

そのソフトウェアインタフェースは，プログラムコード及び専用データ領域からなる。確定したコード化コマンド又はデータの交換は，一ソフトウェア部分が専用データ領域に格納し，別のソフトウェアがそこから読み出すことによって行われる。書き込み及び読み出しプログラムコードは，そのソフトウェアインタフェースの一部である。

例：

(I) 5.2.1.2.a/.c の例では，法定関連ではないアプリケーションがライブラリの中の法定関連手順の開始を制御する。これらの手順の呼び出しを省けば，当然，システムの法定関連機能が禁止される。したがって，5.2.1.2.d の要件を満たすために例に挙げたシステム内では，次の設備が備えてある。デジタルセンサは，暗号化した形式で測定データを送信する。復号のための鍵は，ライブラリの中に隠されている。ライブラリの中の手順だけがその鍵を知っており，測定値の読み出し，復号及び表示を行うことができる。

5.2.1.2.c 法定関連ソフトウェア部分の中では，起動されたすべての機能又はデータの変更に対する各コマンドのあいまいでない割り当てがなければならない。ソフトウェアインターフェースを通じて起動させた機能は，宣言を行い文書化しなければならない。文書化された機能だけが，ソフトウェアインターフェースを通じて起動されなければならない。

例：

(I) 5.2.1.2.a に記載された例では，ソフトウェアインターフェースは，ライブラリの中手順及びそのパラメータで構成され，値を戻す。このインターフェースは，例えば，データに対するポインタによって回避することはできない。手順，パラメータ及び戻値の種類及び数は，コンパイル時に決定される。

(II) 法定関連ソフトウェア部分及び法定非関連ソフトウェア部分は，汎用装置上の別個仮想マシン内で動作する。いずれのマシンも，両方のソフトウェア部分間のあらゆる信は，定義済みのソフトウェアインターフェースを介してのみ行うことができるよう方法で構成されている。両方のソフトウェア間の通信方法を含め，仮想マシンの設定法定関連ソフトウェアの一部である。オペレーティングシステムは，その構成（コンギュレーション）が封印を破壊することなく部分的に変更できないことを確実なものする。

5.2.1.2.d 法定計量関連ソフトウェア部分が非関連ソフトウェア部分から分離されている場合，その法定計量関連ソフトウェア部分が，非関連ソフトウェアよりも計算資源利用に関して優先権を持つ。法定関連プロセスは，法定関連でないソフトウェアによって容認できないほどに中断されてはならない。（法定関連ソフトウェア部分により実現する）測定プロセスは，他のプロセスによって遅延又は阻害されたりしてはならない。.

例：

(1) 通常プロセスよりも高度で，計量器の使用者／オペレータが低下させることができない法定関連機能には優先レベルが割り当てられる。

(2) の生レる。っになの上フ法の

(I) 電子式電力量計のソフトウェアは，アナログ-デジタル変換器（ADC）からの測定値を読み出す。測定値の正しい計算のためには，ADC からの“データ・レディ”事象から測定値のバッファリング終了までの遅延は，きわめて重大である。生データは，“データ・レディ”信号によって開始される割り込みルーチンによって読み出される。計器は，インターフェースを介して，別の割り込みルーチンよって，平行して機能する他の電子装置と通信することができる（法定関連でない通信)。測定値を処理するための割り込みルーチンの優先度は，通信ルーチン優先度よりも高い。

(II) 法定関連ソフトウェア部分及び法定非関連ソフトウェア部分は，汎用装置の個別の仮想マシンの中で動作する。オペレーティングシステムの構成（コンィギュレーション）は，法定関連ソフトウェア部分が動作する仮想マシンが，定関連プロセスに利用できる十分なシステムリソースを備えることを確実なものとする。

5.2.1.2.a，5.2.1.2.b，5.2.1.c (I)及び 5.2.1.2.d (1) / (2) (I) の例は，標準リスクレベル(I) に対する技術的解決策としてのみ受諾容認可能である。不正に対するより強い保護又はより高い適合性が必要な場合（8 を参照)，ソフトウェア分離のみでは十分でなく，追加手段が求められるか又はソフトウェア全体が法定管理下にあると見なすべきである。

5.2.2 共有表示

法定関連ソフトウェア部分からの情報及びその他の情報の両方を提示するため，表示又は印字出力を使用することができる。その内容及びレイアウトは，計量器の種類及び適用分野に固有のものであり，その関連 OIML 勧告の中で定義されなければならない。法定関連出力及び法定非関連出力の両方に表示又は印字出力が用いられる場合，法定関連情報は，常に他の情報よりも，読みやすく，かつ明確に区別可能であることが望ましい。

例：

(I) 5.2.1.2.a から 5.2.1.2.d までの例で説明した計量器において，その測定値は個別のソフトウェアウィンドウに表示される。5.2.1.2.d で説明した手段は，法定関連ソフトウェア部分のみが測定値を読み取り，表示できることを保証している。計器は，複数のウィンドウユーザインタフェースをもつ。法定関連データを表示するウィンドウは，法定関連動的リンク・ライブラリ（5.2.1.2 を参照）の手順によって生成及び制御される。測定中，この関連ウィンドウが他の開いたウィンドウの上に表示されていることをこれらの手順が周期的にチェックし，そうでなければ，この手順でそのウィンドウを一番上になるようにする。

(II) 5.2.1.2.a から 5.2.1.2.d までの例の中に記載された計量器においては，測定アプリケーションは，キオスクモードで動作する。表示全体は，法定関連ソフトウェア部分によって制御される。法定非関連データは，法定非関連であるとマークされて特別な部分に提示される。

不正に対して増強した保護手段が必要である場合（II)，指示だけとしての印字出力は適切ではなく，。ハードウェア／ソフトウェアとしての追加的な予防措置を考慮しなければならない。測定値を表示できるより高い保全手段を備えた構成部品が存在すべきである。

5.2.3 データの保存

測定値を，法定目的で使用するために保存する場合，次の要件を適用する：

PG は，各種用途のための適切な保存条件を決定することができる。

5.2.3.1 保存された測定値には，将来の法的関連の使用に必要なあらゆる関連情報を添付しなければならない。

例：

(I)/(II) データセットは，次の入力を含む：

- 単位を含む測定値
- 測定の時刻刻印（5.2.3.4 を参照）
- 測定場所又はその測定に使用した計量器の識別
- 測定の曖昧さのない識別，例えば，請求書に印字した値に割り付けできる連続番号

5.2.3.2 保存したデータは，測定時刻に関する情報の信憑性，完全性及び，必要な場合，正確さを保証するため，ソフトウェア手段によって保護されなければならない。測定値及び付随データを表示又はさらに処理するソフトウェアは,保存装置から読み込んだ後,そのデータの測定時刻，信憑性及び完全性をチェックしなければならない。不正を検知した場合，そのデータを廃棄するか又は使用不能のマークを付けなければならない。

保存用にデータを準備するか又は読み込み後にデータをチェックするソフトウェアモジュールは，法定関連ソフトウェアの一部であると見なされる。

備考： 自由にアクセス可能な保存を考慮する場合，より高いリスクレベルを求めるのは妥当である。

より高いリスクレベルは，暗号化手法を適用する必要がある。適切な場合は，封印が破られた場合だけ，暗号鍵が入力又は読み取り可能となる手段を設けなければならない。例(I)は，局部記憶装置に適用され，また例(II)は，自由にアクセス可能な記憶装置に適用される。

例：

(I) 保存装置のプログラムは，そのデータセットの CRC32 チェックサムを計算し，それをそのデータセットに追加する。この計算には，規格の中で与えられた値の代わりに，秘密の初期値を使用する。この初期値を鍵として使用して，そのプログラムコードの中に 1 定数として保存する。読み込みプログラムも,そのプログラムコードの中にこの初期値を保存する。そのデータセットを使う前に，読み込みプログラムは，チェックサムを計算し，それをデータセットに保存したものと比較する。その両方の値が一致すれば，そのデータセットは改ざんされていないことになる。そうでなければ,そのプログラムは改ざんがあったと見なして，そのデータセットを廃棄する。

(II) 法定関連ソフトウェア部分である保存プログラムは，保存されたデータセットのための電子署名を生成する。それを保存済データセットに付加する。署名に用いられた公開鍵及び秘密鍵は，その秘密鍵を改ざん又は読み取りから保護し，かつ公開鍵をエクスポートするハードウェアセキュリティモジュールの中に生成される。読み取りプログラムは，そのデータセットの信憑性及び完全性をチェックするために，公開鍵をもつその署名を検証する。そのデータセットの源を立証するため，読み取りプログラムは，その公開鍵が本当にその保存プログラムにに属するものかどうかを知る必要がある。したがって，その公開鍵はその計量器のディスプレイ上に提示され，一度だけ，例えば，現場で検定された時，

その機器のシリアル番号と共に登録されることができる。

5.2.3.3 自動保存

5.2.3.3.a 用途考えると，データ保存が必要な場合，測定が終了したとき，即ち，法的目的に使用

する最終値が生成されたときに，測定データは自動的に保存されなければならない。

その保存装置は，データが通常の保存条件の下では破損しないことを確実にするため十分な恒久性を持っていなければならない。意図した用途に対して十分な記憶容量がなければならない。

法的目的に使用する最終値が計算結果によって得られる場合，その計算に必要なすべてのデータは最終値と共に自動的に保存されなければならない。

備考 1： 累積測定の場合，同じデータ領域（プログラム変数）が繰り返し使われることがある。その場合，記憶容量は，法定関連ではないことがある。

備考 2： すべての要件が満たされているかぎり，保存されたデータは，物理的に 1 つの記憶ユニットの中に置く必要はない。

5.2.3.3.b 保存データは，次のいずれかの場合に削除することができる：

- 取引が完了した場合，
- これらのデータが法的管理対象の印字器で印字されている場合

備考： 他の国内法（例えば，税法を目的とした）が保存測定データの削除に対して厳しい制限を設けることがある。PG は，データの削除の代替条件を定めることができる。

5.2.4 通信線を介した伝送

測定値を法的目的に使用する前に，転送する場合，次の要件が適用される。

5.2.4.1 伝送された測定値は，その後の法定関連利用のために必要なすべての関連情報を伴わなければならない。

例：

(1)/(II) データセットには，次のエントリが含まれる。

- 単位を含む測定値
- 測定の時刻刻印（5.1.5 を参照）
- 測定場所又は測定に用いられた計量器の識別
- 測定のあいまいさのない識別，例えば，請求書に印字された値への割当てを可能とする累積番号

5.2.4.2 伝送されたデータは，測定時刻に関する情報の信憑性，完全性及び，必要な場合は，正確さを保証するために，ソフトウェア手段によって保護されなければならない。測定値及び付随データを表示又はさらに処理するソフトウェアは，伝送チャンネルから受信したデータの測定時刻，信憑性，及び完全性をチェックしなければならない。不正を検知した場合，そのデータは，廃棄するか，又は使用不能とマークしなけれならない。

送信するためのデータを作成する，又は受信後にデータをチェックするソフトウェアモジュールは，法定関連ソフトウェアの一部であると見なされる。

備考： 開放型ネットワークを考慮する場合，より高いリスクレベルを求めるのは妥当である。

より高いリスクレベルには，暗号化手法の適用が必要である。封印が破壊された場合にだけ，これらの鍵が入力できる又は読み取りできるような手段を設けなければならない。

例：

(I) 送信装置の法定関連ソフトウェア部分は，データセットの CRC32 チェックサムを計算する。このチェックサムは，データセットの最後に追加される。このプログラムは，この計算に，規格で与えられた値の代わりに秘密の初期値を使用する。この初期値は，鍵として使用され，プログラムコードの中に 1 定数として保存される。受信装置の法定計量ソフトウエアの部分であるプログラムも，そのプログラムコードの中にこの初期値を既に保存している。データセットを使用する前にプログラムは，チェックサムを計算し，それをデータセットの中に保存されているものと比較する。両方の値が一致した場合，そのデータセットは改ざんされていない。そうでなければ，改ざんを想定して，そのデータセットを廃棄する。

(II) 送信装置の法手関連ソフトウェア部分は，伝送されたデータセットのための電子署名を生成する。その電子署名は，伝送されたデータセットの最後に追加される。署名に使用された秘密鍵及び公開鍵は，秘密鍵を改ざん又は読み取りから保護し，かつ公開鍵をエクスポートするハードウェアセキュリティモジュールの中で生成される。受信装置の法定関連ソフトウェアの部分であるプログラムは，そのデータセットの信憑性及び完全性をチェックするために，公開鍵をもつその署名を検証する。そのデータセットの源を立証するために，プログラムは，その公開鍵が本当に伝送プログラムに属するかどうかを知る必要がある。したがって，その公開鍵は，計量器の表示（計）器上に提示され，一度だけ，例えば，現場で検定されたときに，その計器のシリアル番号と共に登録することができる。

例：

(II) 伝送プログラムは，伝送されたデータセットの電子署名を生成する。この電子署名は，

伝送されたデータセットに追加される。署名に用いられる秘密及び公開鍵は，改ざん又は読み出しから秘密鍵を保護し，公開鍵をエクスポートするハードウェアセキュリティモジュールの中で生成される。受信プログラムは，公開鍵をもつ署名を検証する。データセットの源を立証するために，受信装置のプログラムは，その公開鍵が本当に伝送プログラムに属するかどうかを知る必要がある。したがって，その公開鍵は，計量器の表示（計）器上に提示され，一度だけ，例えば，現場で検証されたときに，その計器のシリアル番号と共に登録することができる。

5.2.4.3 伝送遅延

測定は，伝送遅延によって認められない程の影響を受けてはならない。

5.2.4.4 伝送中断

ネットワークサービスが利用できなくなった場合，測定値が喪失してはならない。測定データの喪失を避けるため，その測定プロセスを停止すべきである。

備考： 静的測定と動的測定の間を識別するよう考慮すべきである。

適用領域によって，また，測定が簡単に繰り返し可能な場合には，伝送データの喪失は許容可能である。

例：

(I)/(II) 送信器／構成部品は，受信器がデータセットの正しい受信確認を送信するまで待つ。 送信器／構成部品は，その確認を受信するまでそのデータセットをバッファに保存しておく。そのバッファは，FIFO（先入れ先出し）行列で整理した 2 つ以上のデータセットに対する容量を持つ。

5.2.5 オペレーティングシステム及びハードウェアの互換性

5.2.5.1 オペレーティングシステムが計量器の一部である場合，5.2.5.2 から 5.2.5.7 に従った要件を満たさなければならない。

次のオペレーティングシステム要件はそれぞれ，アプリケーションレベル，オペレーティングシステムレベル又はこの両レベルの組み合わせに対する措置によって満たさなければならない。例えば，保護インターフェースは，法定関連アプリケーション，オペレーティングシステム，物理層の範囲内で実装することができる。

5.2.5.2 保護ソフトウェアインターフェースを備えていないハードウェアインターフェースは，法定関連ソフトウェア部分に容認できないほどの影響を与えることができてはならない（例えば，物理的封印）。

例：

(I) 法定関連アプリケーションは，入力トラヒックに対するすべてのオープンな物理的インターフェースを定期的にチェックする。不正入力の場合は，このアプリケーションが測定を阻止する。

イ

(II) すべてのオープンインタフェースは，オペレーティングシステムによって，物理的に保護されるか，又は無効化される。

5.2.5.3 法定関連ソフトウェア部分の保護を確実なものとするためにセキュアブートプロセスが必要な場合，次の要件が適用される。

5.2.5.3.a 法定関連ソフトウェア部分の完全性及び信憑性を確実なものとするために，ブートプロセスの個々の構成要素全体にわたって信頼の連鎖を確立しなければならない。

5.2.5.3.b 信頼の連鎖の処理は，その完全性が保たれている限りは，中断することができる。

5.2.5.3.c ブートの構成（コンフィギュレーション）は，不正な部分的変更を防がなければならない。

5.2.5.3.d オープンインターフェースを介したブート処理は，保護しなければならない。

例：

(I) ブートローダは，安全保護手段，例えば，安全なパスワードによって守られる。

(II) TPM（高信頼プラットフォームモジュール）は，ブートローダの署名を検証し，その後，ブートローダは，オペレーティングシステムを検証する。これによって，順番に検証が行われ，法定関連アプリケーションが起動する。

の

5.2.5.4 法定関連ソフトウェア部分とオペレーティングシステムの組み合わせは，法定関連アプリケーションの動作のための十分なリソースがあることを確実なものとしなければならない。

例：

(I) 法定関連アプリケーションは，それが必要とするすべてのリソースを持つことを確実なものとしなければならない。

(II) 測定動作を確実なものとするために必要なオペレーティングシステム構成要素の最小数が選択される。

5.2.5.5 使用中の保護

5.2.5.5.a 法定関連ではないソフトウェアの動作は，容認できないほどに法定関連アプリケーションに影響を与えてはならない。

5.2.5.5.b 法定関連ソフトウェア部分とオペレーティングシステムの組み合わせは，法定関連表示が区別可能であることを確実なものとしなければならない。

5.2.5.5.c アクセス制御は，意図した使用が容認できないほどに影響を受けることがないような方法で構成しなければならない。

5.2.5.5.d 法定関連ソフトウェア部分の管理タスクは，保護しなければならない。

例：

(I) すべての法定関連ファイルは，書き込みが禁止され，かつ法定関連ソフトウェア部分によって，アクセス許可が定期的にチェックされる。

(II) 法定非関連ソフトウェアは，実質的に分離された環境の中で動作する。

5.2.5.6 法定関連ソフトウェア部分との通信は，保護インターフェースを介して行われなければならない。

例：

(I) 法定関連ソフトウェアモジュールは，法定関連ソフトウェア部分に到達するすべてのコマンドを解釈して，容認できないものを破棄する。

(II) オープンソフトウェアインターフェースを介した通信は，オペレーティングシステムの手段によって保護される。

5.2.5.7 可試験性及びトレーサビリティ

5.2.5.7.a オペレーティングシステムの構成は，識別可能でなければならない。

例：

(1) ユニックス（UNIX）タイプのオペレーティングシステムでは，その構成は，法定関連の次のもので構成される：

- カーネルモジュール
- インストールしたパッケージのリスト
- ライブラリ
- アカウント及び使用者特権
- パスワード
- 構成ファイル

- ファイル読み出し／書き込み／実行許可

上記すべては，チェックサムによって識別される。

2) WINDOWS オペレーティングシステム上では，構成は，法定関連の次のもので構成される：

- カーネルモジュール

- インストールしたパッケージのリスト
- ライブラリ
- アカウント及び使用者特権
- パスワード
- 構成ファイル
- ファイル読み出し／書き込み／実行許可
- レジストリキー

上記のそれぞれは，チェックサムによって識別される。

5.2.5.7.b　オペレーティングシステムの構成に対する変更が可能な場合，その変更はトレーサブルでなければならない。

5.2.5.8　製造事業者は，適切なハードウェア及びソフトウェア環境を識別しなければならない。正しく機能するために必要な最小限のリソース及び適切な構成（例えば，プロセッサ，記憶装置，特定通信，オペレーティングシステムのバージョンなど）は，製造事業者が宣言し，証明書に明記しなければならない。

5.2.5.9　法定関連ソフトウェアの中に，最小構成要件が満たされない場合には，動作を防止するための技術的手段を備えなければならない。システムは，それが正しく機能するために製造事業者が規定した環境の中だけで動作しなければならない。

次の場合には，汎用装置のハードウェア，オペレーティングシステム，又はシステム構成を固定すること，又は既製の汎用装置の使用を除外することさえも，考慮しなければならない：

- 高度な適合性が求められる場合
- 暗号化アルゴリズム又はキーを実装する必要がある場合（5.2.3 及び 5.2.4 を参照）

5.2.6　製造機器の承認済型式への適合性

製造事業者は，承認済型式及び提出文書に適合した装置及び法定関連ソフトウェアを製造しなければならない。

5.2.7 保守及び再構成

現場おける計量器の法定関連ソフトウェア部分の更新は，次の様に考えるべきである：

- ソフトウェアを別の承認済バージョンと交換する場合，その計量器の改造
- 同じバージョンを再インストールする場合，その計量器の修理

稼動中に改造又は修理された計量器には，国内法に基づいて，初期検定又は後続検定を要求することができる。

計量器の法定関連機能を実現しないソフトウェアは，更新後に検定を必要としない。

5.2.7.1 承認済型式に適合する法定関連ソフトウェア部分バージョンだけが，使用が許される（5.2.6 を参照）。それらのバージョンは，証明書の中に明記される。以下の要件の適用性は，機器の種類に依存し，その関連勧告の中でさらに検討される。以下のオプション 5.2.7.2 及び 5.2.7.3 は代替案である。装置固有パラメータ（特に校正パラメータ）に関係がある場合，検定済みの更新だけを行うことが望ましい。
この件は，現場における計量器の検定に関わっている。追加制約については，第 7 節を参照。

5.2.7.2 要検定更新

更新するソフトウェアは，局所的に，即ち，直接計量器上に又は遠く離れてネットワークを介してローディングすることができる。ローディング及びインストールは，二つの異なるステップ（図 1 に示したように）又は一つにまとめられるものである可能性があり，それは技術的解決策の必要性に依存する。封印は，更新が有効化するためには破壊する必要がある。更新の有効性をチェックする者は，その計量器の設置場所にいることが望ましい。計量器の法定関連ソフトウェア部分の更新（別の承認済バージョンとの交換又は再インストール）の後，第 7 節に記述した計量器の検定が行われ，かつその保全手段が更新される前に，その計量器を法定目的のために採用することは（関連勧告又は証明書の中で特に謳われていない限り）望ましくない。

5.2.7.3 追跡可能更新

ソフトウェアが関連勧告に従っている場合，追跡可能更新に対する要件（5.2.7.3.a から 5.2.7.3.h）に従ってそのソフトウェアは計量器に実装される。追跡可能更新は，検定済計量器又は構成部品のソフトウェアを更新する手順であり，後続検定を必要としない。このことは，追跡可能更新は，既存のパラメータに影響を与えてはならないことを意味する。更新されるソフトウェアは，局所的にローディング，即ち，直接計量器に又は遠く離れてネットワークを介してローディングすることができる。ソフトウェア更新は，監査証跡に記録される（3.1.1 を参照）。追跡可能更新の手順は，複数のステップで構成される：ローディング，完全性チェック，由来（信憑性）チェック，インストール，ロギング及び起動。

5.2.7.3.a ソフトウェアの追跡可能更新は，自動でなければならない。更新できるように，計器の保全手段にオフになっているものがある場合，更新後，更新プロセスの結果に関わらず，それらを再度直ちにオンとしなければならない。

備考： 追跡可能更新プロセスの起動は，その計量器の使用者による介入／手動操作を必要とする場合がある。

5.2.7.3.b ソフトウェアは，あらゆる介入の証拠を入手できるものとするような方法で保護しなけ

ればならない。更新中，あらゆる既存の監査証跡情報及び事象計数器の値は，保持しなければならない。

5.2.7.3.c ロードしたソフトウェアの信憑性，即ち，そのソフトウェアが証明書の所有者に由来することを保証するための技術的手段を採用しなければならない。

例：

(II) 信ぴょう性チェックは，公開鍵システムのような暗号的手段により行われる。証明書の所有者（一般的にはその計量器の製造事業者）は，更新済みソフトウェア又はソフトウェア部分の電子署名を，工場の*秘密鍵*を使って作成する。その*公開鍵*は，その署名付きの更新されたソフトウェアを受信する計量器の法定関連ソフトウェア部分に保存される。その署名は，更新済みソフトウェアを計量器にローディングする際，その*公開鍵*を使ってチェックされる。ローディングしたソフトウェアの署名が OK である場合，そのソフトウェアはインストールされて起動する。チェックに失敗すると，そのロードした更新済みソフトウェアは廃棄され，計器は，ソフトウェアの現行バージョンで動作するか，又は操作不能モードに切り替わる。

5.2.7.3.d ロードしたソフトウェアの完全性，即ち，ローディング前に許容できないほど変更されていないことを保証するため，技術手段を講じなければならない。これは，ロードしたソフトウェアのチェックサム又はハッシュコードを加えること及びローディング手順中に検証することによって遂行することができる。

5.2.7.3.e 法定関連ソフトウェア部分の追跡可能更新が，後続検定及び監査又は検査に対して計器内で十分追跡可能であることを保証するため，監査証跡を採用しなければならない。

監査証跡は，少なくとも，次のような情報を含んでいなければならない：

- 更新手順の成功／失敗
- インストールしたバージョンのソフトウェア識別
- 前にインストールしたバージョンのソフトウェア識別
- 事象の時刻刻印
- 可能な場合にはダウンロードした当事者の識別

成否に関わらず，各更新の試みに対して記録項目が生成される。

追跡可能更新を支援するデータ保存装置は，少なくとも，続けて 2 回の現地／検査における計量器の検定間の法定関連ソフトウェア部分の追跡可能更新のトレーサビリティを確実にするに十分な容量を持っていなければならない。監査証跡用のデータ保存容量が限界に達した後，封印を破壊しない限り，さらにダウンロードが不可能なことを技術的手段によって確実にしていなければならない。

監査証跡は，コマンドで表示又は印字されなければならない。証明書は，監査証跡をどのように表示又は印字することができるかを記述しなければならない。

備考： この要件によって，法定管理機器の計量監査に責任を負う検査当局は，十分な期間（国内 法による）にわたって，法定関連ソフトウェア部分の追跡可能更新を逆に辿ることが可能 となる。

5.2.7.3.f 必要性及び国内法規に基づいて，計量器の使用者又は所有者にとって，追跡可能更新に対するその承諾を与えることが必要であることがある。計量器には，ダウンロード開始前に，利用者又は所有者が承諾を表明するための機能，例えば，押しボタンを備えなければならない。

封印可能なスイッチ又はパラメータによって，この機能を有効又は無効にすることが可能ででなければならない。この機能が有効となっている場合，各追跡可能更新は，使用者又は所有者によって始動される必要がある。無効になっている場合，追跡可能更新を実行するのに使用者又は所有者による行動は必要でない。

5.2.7.3.g　ロードしたソフトウェアが完全性試験（5.2.7.3.d）又は信憑性試験（5.2.7.3.c）に不合格となった場合，その計器はそのソフトウェアの新バージョンを廃棄して，以前のバージョンを使用するか，不動作モードに切り替えなければならない。このモードでは，その測定機能は阻止されていなければならない。唯一可能なのは，ダウンロード手順を再び始めること又は誤りを示すことでなければならない。監査証跡に容量がないか（5.2.7.3.e），使用者又は所有者が承諾を拒んだ場合，その更新手順を全く開始すべきでない。

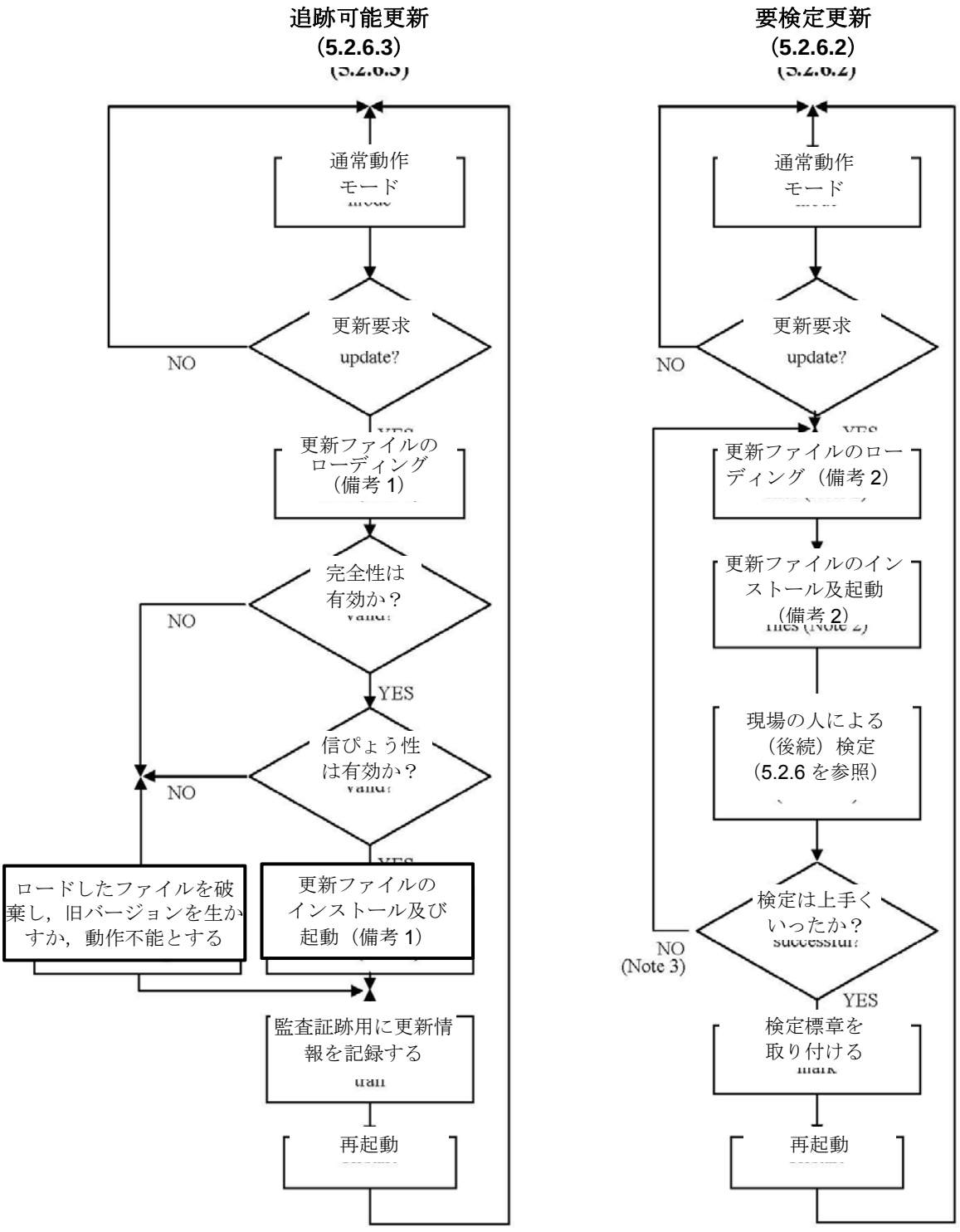

図 1　ソフトウェア更新手続き

備考： (1) 追跡可能更新の場合，更新は次の二つのステップ，“ローディング”及び“インストール／起動”，に分けられる。このことは，チェックで不合格となると，ローディングしたソフトウェアを破棄し，その古いバージョンに戻る可能性があるはずなので，そのソフトウェアはローディング後，作動することなく一時的に保存されることを意味する。

(2) 要検定更新の場合，ソフトウェアはロードされ，インストール前に一時的に保存されることがあるが，技術的解決策によってはローディングとインストールが一ステップで行われることもある。

(3) ここで，そのソフトウェア更新に起因する計量器の検定の不合格だけが考えられる。他の理由に起因する検定不合格では，NO 分岐で象徴されるソフトウェアの再ローディング及び再インストールを求めない。

5.2.7.4 関連勧告では，一定の機器固有のパラメータをユーザーが利用可能であるように設定することを要求することができる。そのような場合，その計量器は，その機器固有のパラメータのあらゆる調整を自動的及び消去不能に記録する機構，例えば，監査証跡を備えていなければならない。その計量器は，記録したデータを提示できなければならない。

5.2.7.5 監査証跡は，法定関連ソフトウェア部分の一部であり，そのようなものとして保護されなければならない。ソフトウェアが更新された場合，それを交換してはならない。

6 型式評価

6.1 型式評価ソフトウェア提出文書

型式評価のため，計量器の製造事業者は，計量器に実装している法定関連ソフトウェア部分のすべての機能，関連データ構造及びソフトウェア・インタフェースを宣言し，文書化しなければならない。

すべてのコマンドとその効果は，型式評価用に提出するソフトウェア文書に完全に記述しなければならない。

さらに，型式承認申請には，その計量器のソフトウェア設計及び特性がこの文書の要件を組み入れた関連勧告の要件に従っているとの前提を支持する文書又は他の証拠を添付しなければならない。

6.1.1（各計量器／構成部品に対する）典型的な書類は，基本的に次のものを含む：

- 法定関連ソフトウェア及び要件がどのように満たされているかの記述：
  - 法定関連部分に属するソフトウェアモジュールのリスト
  - 法定関連ソフトウェア部分のソフトウェアインタフェース及びコマンドの説明並びにこのインタフェースを介したデータフロー
  - 一段高いリスクレベルが関連勧告によって要求されるとき，その関連勧告で採用されている評価手法（6.3 と 6.4 を参照）に基づいて，そのソースコードを型式評価当局に提出しなければならない。
  - 保護されるパラメータのリスト及び保護手段の説明
- 適切なシステム構成及び最小要求リソースの説明（5.2.5 を参照）

- オペレーティングシステムの保全手段（該当する場合，パスワードなど）の説明

- （ソフトウェア）封印手法の説明
- システムハードウェア，例えば，トポロジーブロック図，コンピュータ型式，ネットワーク型式，などの概観。ハードウェア構成部品が法定関連であると見なされる又は法定関連機能を遂行する場合，これも特定するべきである。
- アルゴリズムの精度説明（例えば，A/D 変換結果のフィルタリング，料金計算，丸めアルゴリズム，など）
- ユーザインタフェース，メニュー及びダイアログの説明
- ソフトウェア識別及び稼動中の計量器からそれを取得する方法の説明
- 計量器／サブアセンブリの各ハードウェアインタフェースのコマンドリスト
- ソフトウェアによって検出される耐久性誤差のリスト及び理解に必要な場合，その検出アルゴリズムの説明
- 保存又はで伝送されるデータセットの説明
- 有意欠陥の検出がソフトウェア内で行われた場合，検出される有意欠陥のリスト及び検出アルゴリズムの説明
- 監査証跡がソフトウェアの中で実現されている場合，監査証跡にどのようにアクセスするか の説明
- 取扱説明書

6.2 評価手順への要件

型式評価の枠組における試験手順は，上手く明確に定義した試験設定及び試験条件に基づいていて，正確な比較測定に依存することができる。一般にソフトウェアの品質をどのように“測定する”かを説明した規格 [例えば，ISO/IEC 25040:2011 シリーズ [5]] があるけれど，ソフトウェアの精度又は正確さを計量の意味で測定することはできない。ここで説明する手順は，法定計量の必要性並びにソフトウェア工学においてよく知られた評価及び検証方法を考慮したものであるが，これら二つは同じ目的を持っているわけではない（例えば，誤差を探し求めるが，性能の最適化も行うソフトウェア開発者）。6.4 に示したように，ソフトウェアの各要件は，適当な評価手順を個別に適応させる必要がある。この手順のための努力は，そのリスクレベルを反映すべきである。

その目的は，承認すべき計器が関連 OIML 勧告の要件に準拠している事実を検証ことである。ソフトウェア制御計器に対して，その評価手順は，審査，解析及び試験から構成され，その関連勧告は以下に説明した手法から適切なものを選択することを含んでいなければならない。

以下に説明した手法は，型式評価に焦点を当てている。現場で使用中の個々の計量器の検証は，これら検証手法でカバーされていない。詳しくは第 7 節の*検定*を参照のこと。

ソフトウェア評価のため規定した方法が，6.3 に記述されている。第 5 節で定義したすべての要件に適応した完全なソフトウェア評価手順を構成するこれらの方法の組み合わせが，6.4 に規定されている。
製造事業者は，隠された又は文書化されていない特性（例えば，パラメータ，コマンド，関数，バックドア）が存在しないことを証明しなければならない。

この文書は，製造業者に対して，文書類が正しくかつ漏れがないことの追加的宣言を求めるものではない。しかし，どこの国も，規定のソフトウェア審査プロセスの一部として，この宣言を求めることができる。

6.2.1 証明書の中に含まれるべき情報

- すべての承認済みのバージョンのソフトウェア識別
- 使用中の承認済み計器に現在のソフトウェア識別を表示する方法

– 保全手段及びそれらをチェックする方法（例えば，ハードウェア封印，事象計数器，監査証跡）

6.3 検証及び評価手法

6.3.1 手法及びその適用の概観

以下の手法の選択及び順序は，規定されているわけではなく，場合によってソフトウェア評価手順で変更となることがある。

これは，大まかな総括である。より詳細は，6.3.2 を参照。

略語	説明	適用	前処理，適用のためのツール	実施に必要な特別技能
AD	文書解析と設計の評価 (6.3.2.1)	常に適用する	文書	-
VFTM	計量機能の機能試験による検証 (6.3.2.2)	アルゴリズムの正当性，不確かさ，補正及び校正アルゴリズム，料金計算規則	文書，供試器	-
VFTSw	ソフトウェア機能の機能試験による検証 (6.3.2.3)	通信，提示，介入の証拠の正しい機能，操作間違いからの保護，パラメータ保護，有意な欠陥の検出	文書，供試器	-
DFA	計量データフロー解析 (6.3.2.4)	ソフトウェア分離，計量器の機能へのコマンドのインパクト評価	ソースコード ソースコード解析用ツール ツール	プログラミング言語の知識
CIWT	コード精査及び渡り歩き (6.3.2.5)	あらゆる目的	ソースコード ソースコード解析用ツール ツール	プログラミング言語の知識
SMT	ソフトウェアモジュール試験 (6.3.2.6)	入力と出力の明確な定義が可能な場合，あらゆる目的	ソースコード，試験環境	プログラミング言語の知識

表 1：提案した検証及び評価手法の総括

6.3.2 選択した検証及び評価手法の説明

6.3.2.1 文書及び仕様の解析並びに設計の評価（AD）

適用：

ソフトウェアの評価のための基本的手順。

前提条件：

この手順は，計量器製造事業者の文書に基づいている。必要に応じて，この文書には適 切な適用範囲がなければならない：

(1) 一般的な形式の計量器の外部からアクセス可能な機能の仕様（ディスプレイ以外のインタフェースを持たない単純な計量器に適していて，機能試験によってすべての特性が検証可能で，低不正リスク)

(2) ソフトウェア機能及びインタフェース仕様（インタフェースを持つ計量器及び機能的に又高い不正リスクの場合に試験が不可能な機器機能に対して必要)。その記述は，計量特性に大きな影響を与える可能性のあるすべてのソフトウェア機能を明確にし，説明していなければならない。

(3) インタフェースに関して，その文書はそのソフトウェアが解釈可能なコマンド又は信号の完全なリストを含んでいなければならない。各コマンドの効果が，詳細に文書化されていなければならない。文書化されていないコマンドへの計量器の反応が，記述されなければならない。

(4) ソフトウェア機能の理解及び評価に必要な場合，複雑な測定アルゴリズム，暗号機能又は重要なタイミング制約についての追加文書を提供しなければならない。

審査に必要な前提は，文書の完全性及び EUT，即ち，計量機能に貢献するソフトウェア・パッケージの明確な識別である（6.1.1 を参照)。

説明：

審査官は，言葉による説明及びグラフ表示を使って計量器の機能及び機構を評価し，それらが関連勧告の要件に適合しているかどうかを決定する。第 5 節に定義されているソフトウェアー機能要件（例えば，介入の証拠，調整パラメータ保護，禁止機能，他機器との通信，ソフトウェア更新，有意 r 欠陥の検知など）だけでなく計量上の要件も考慮して評価しなければならない。この作業にはソフトウェア評価報告書式（附属書 B を参照）が助けとなる。

結果：

適切な文書が製造事業者によって提出されていると仮定すると，その手順はその計量器のすべての特性に対して結果を出す。その評価結果は，関連勧告の評価報告書式に含まれているソフトウェア評価報告書（附属書 B を参照）の中のソフトウェア関連の節に文書化するべきである。

補足手順：

文書審査で内容のある評価結果が得られない場合，追加手順を適用するべきである。ほとんどの場合，“機能試験による計量機能の検証”（6.3.2.2 を参照）が補足手順である。

参考文献：

IEC 61508-5, 2010 [7]

6.3.2.2 計量機能の機能試験による検証（VFTM）

適用：

生データから測定値の計算，特性の直線化，環境の影響の補正，料金計算における丸め，などを計算するアルゴリズムの正確さを検証するため

前提：

取扱説明書，機能している供試器，計量基準，試験装置，試験，試験台，試験装置説明書。

ソフトウェアの機能どのように検証するか明確でない場合，試験方法の開発責任をその製造事業者に負わせるべきである。さらに，そのプログラマーのサービスを，質問に応える目的で，審査官が利用できるようにするべきである。

説明：

勧告に記述されているほとんどの評価及び検証方法は，さまざまな条件下における標準計量に基づいている。その適用は，その計量器の特定技術に限定されていない。それらは，ソフトウェアの検証を主目的とするのではないが，その試験結果はあるソフトウェアの検証であると解釈することができ，一般的に，計量上最も重要であるとも解釈される。関連勧告に記述された試験が，計器の計量関連機能をすべて網羅していれば，その対応ソフトウェア部分が検証されたとみなされる。一般に，計量器の計量機能の検証に，追加のソフトウェア分析又は試験を適用する必要がない。

結果：

アルゴリズムは正しいか正しくないかのどちらかである。すべての条件下の測定値は，最大許容誤差（MPE）の範囲内にあるか，そうでないかである。

補足手順：

この方法は，通常は 6.3.2.1 を強化したものである。場合によっては，ソースコードに基づいた審査（6.3.2.5）又は入力信号をシミュレートすることによる審査（6.3.2.6）を伴う方法と併用することが，例えば，動的測定に対してより容易である又はより効果的であることがある。

参考文献：

様々な特定勧告。

6.3.2.3 ソフトウェア機能の機能試験による検証（VFTSw）

適用：

例えば，（特に，ソフトウェア環境の）パラメータ保護，ソフトウェア識別の表示，ソフトウェア支援の有意欠陥の検知，システム構成などの評価のため

前提：

操作説明書，ソフトウェア文書，機能している供試器，試験装置，試験台，試験装置の取扱

説明書

ソフトウェア部分の機能をどのように検証するかが明確でない場合，その試験方法を開発する責任はその製造事業者に課すのが望ましい。加えて，そのプログラマーのサービスを質問に回答する目的で，審査官が利用できるようにするのが望ましい。

説明：

操作説明書，計器の文書又はソフトウェア文書に記述された要求機能は，実質的にチェックされる。これらの機能がソフトウェア制御である場合，さらにソフトウェア分析を行うことなく正しく機能すれば，それらは検証されたと見なされるべきである。ここで扱う機能は，例えば，次の通りである：

- その動作がソフトウェア制御である場合，その計量器の正常動作。すべてのスイッチ又はキー及び説明書に記載されたスイッチ及びキーの組合せを採用し，その計量器の反応を評価すべきである。グラフィカルユーザインタフェースでは，すべてのメニュー及びその他のグラフィカルエレメントを作動させ，チェックすべきである。
- パラメータ保護の有効性は，その保護手段を起動させ，パラメータ変更を試みることによってチェックすることができる。
- 保存データ保護の有効性は，ファイルのいくつかのデータを変更して，その変更がソフトウェアで検出されるかどうかをチェックすることで確認できる
- ソフトウェア識別の表示は，現実的なチェックによって検証できる。
- 有意欠陥の検出がソフトウェア支援である場合，その関連ソフトウェア部分は，誤りを誘発，実施又はシミュレートすること又はその機器の正しい反応をチェックすることによって検証することができる。
- 保護機能は，無許可の変更を行うことによって，チェックすることができる。ソフトウェアが，これらの変更を禁止するか又は機能を停止するのが望ましい。

結果：

考慮中のソフトウェア制御機能は，許容できる又は許容できない。

補足手順：

ソフトウェア制御計量器の機能の中には，説明したように事実上検証できないものがある。計量器にインタフェースが備わっている場合，コマンドを無作為に試みるだけで未認可コマンドを検出することは一般的に不可能である。その上，コマンドの送り手がそれらのコマンドを生成する必要がある。通常の審査レベルに対しては，方法 6.3.2.1 がこの要件をカバーすることができる。拡大審査レベルに対しては，6.3.2.4 又は 6.3.2.5 などのソフトウェア分析が必要である。

参考文献：

WELMEC ガイド 2.3 [第 3 章[8]，WELMEC ガイド 7.2 4.2 及び 5.2 [9]

6.3.2.4 計量データフロー解析（DFA）

適用：

ソフトウェア分離の審査を含め，法規制対象のデータ領域内を通した測定値のデータフローの制御に関するソフトウェア設計の分析のため。

前提：

ソフトウェア文書，ソースコード，エディタ，テキスト検索プログラム又は特別ツール。プログラミング言語の知識.

説明：

測定値の計算に関与するか又はそれに影響を与えるソフトウェアのすべての部分を見付けるのが，この方法の目的である。センサーからの測定の生データ入手できるハードウェアポートから始め，データを読み出すサブルーチンを探す。このサブルーチンは，多分処理を少し行った後，それらを変数で保存する。この変数から，別のサブルーチンが中間値を読み取り，完全な測定値がディスプレイに出力されるまで繰り返す。中間測定値の保存として使用するすべての変数及びこれらの値を処理し，運ぶすべてのサブルーチンはテキストエディタ及び変数の他の発生又はサブルーチン名称を見付けるためのテキスト探索プログラムを使って簡単にそのソース・コードの中に見付けることができる。

他のデータフロー，例えば，ソフトウェアインタフェースから受け取ったコマンドの解釈プログラムへのフローは，この方法によって見つけることができる。さらに，ソフトウェアインタフェースの迂回（5.2.1.2 を参照）も検出できる。

結果：

5.2.1.2 に従ってソフトウェア分離が許容できるか又は許容できないかを検証することができる。
各インタフェース用コマンドの文書化リストが完全であるか，そうでないかを検証できる。

補足手順：

ソフトウェア分離が実現され，かつ高い適合性又は改ざんに対する強力な保護が要求されている場合，この方法が推奨される。これは，6.3.2.1 から 6.3.2.3 及び 6.3.2.5 への強化である。

参考文献：

IEC 61131-3.

6.3.2.5 コード検査及びわたり歩き（CIWT）

適用：

拡大した審査強度が必要な場合，ソフトウェアのどの機能でも，この方法によって検証できる。

前提：

ソースコード，テキストエディタ，ツール。プログラミング言語の知識。

説明：

審査官は，要件が実行されているかどうか並びに機能及び特性が文書に従っているかどうかを決定するため，それぞれのコード部分を評価しながら，ソースコードを見て回る。

審査官は，複雑である，間違いが発生しやすい，文書化が不十分である，などと見なしたアルゴリズム又は機能に集中して，分析及びチェックをすることによって，そのソース・コードのそれぞれの部分を点検することが可能である。

これらの点検段階に先立って，審査官は法定関連ソフトウェア部分を，例えば，計量データフロー解析（6.3.2.4 を参照）を適用して，識別してある。一般には，コード精査や渡り歩きは法定計量に関連する部分に限定される

これらの審査段階に先立って，審査官は法定計量に関連するソフトウェア部分を，例えば，計量データフロー解析（6.3.2.4 を参照） を適用することによって識別していることであ

ろう。一般的に，コード点検又は見回りは，法定この部分に限定される。

結果：

ソフトウェア文書に適合し，しかも要件に適合した履行であるか又は否か。

補足手順：

これは，6.3.2.1 及び 6.3.2.4 に追加した強化策である。通常，これは抜き打ち検査でのみ適用される。

参考文献：

IEC 61508-5:2010 [7]。

6.3.2.6 ソフトウェアモジュール試験（SMT）

適用：

この手法は，例外的な事例でのみ用いられる。これは，ソフトウェアモジュールの機能がもっぱら記述された情報に基づいてだけしか審査できない場合に適用する。動的測定アルゴリズムの検証において，この方法は適切であり，有利である。

前提：

ソースコード，開発ツール，試験対象のソフトウェアモジュールの機能環境，入力データセット及び対応基準出力データセット又は自動化ツール。情報技術のスキル，プログラミング言語の知識。試験対象のモジュールのプログラマーとの協力が推奨される。

説明：

試験対象ソフトウェアモジュールは，試験環境，即ち，試験対象ソフトウェアモジュールを呼び出して必要なすべての入力データを提供する特定試験プログラムに統合される。その試験プログラムは，試験対象モジュールから実出力データを受け取り，それを基準値と比較する

結果：

試験対処モジュールは，正しいか否か。

補足手順：

この方法は，6.3.2.2 又は 6.3.2.5 への追加で，強化策である。

参考文献：

IEC 61508-5:2010 [7]

6.4 ソフトウェア評価手順

ソフトウェア評価手順は，評価及び検証手法の組み合わせでできている。関連 OIML 勧告は，下記を含めて，ソフトウェア評価手順に関してその詳細を定めることができる：

(a) 考慮中の要件に対して，6.3 に記述した評価及び検証方法のどれかを実行しなければならない
(b) 試験結果の評価がどのように行うか;
(c) どの結果をソフトウェア試験報告に記載すべきか，また，どれを評価報告書に含めるべきか，及びどの結果を証明書に組み入れるべきか（付録 B を参照）

表 2 で，ソフトウェア評価に対してどちらかを選ぶべき二つの審査レベル，通常（A）及び拡大（B），が定義されている。DFA，CIWT 及び SMT 手法は，レベル B に対して提案されているだけである。レベル B は，A と比べ，拡大審査を示唆している。レベル B の選択は，PG によって，緩和リスクの証拠と共に正当であることを理由付けなければならない。A 及び B の審査レベルの選択は，次の予想に従って，各要件に対して異なる選択とするか又は同じ選択とするかを関連勧告の中で行うことができる。

- 不正のリスク
- 適用領域
- 求められている認証済み型式への適合性
- 操作エラーによる誤った測定結果のリスク

要件		審査レベル **A**（通常審査レベル）	審査レベル **B**（拡大審査レベル）	コメント
5.1.1	ソフトウェア識別	AD + VFTSw	AD + VFTSw + CIWT	高い適合性が求められる場合は“B”を選択する
5.1.2	アルゴリズム及び機能の正確性	AD + VFTM	AD + VFTM + CIWT/SMT	
ソフトウェア保護				
5.1.3.1	誤用の防止	AD + VFTSw	AD + VFTSw	
5.1.3.2	介入の証拠	AD + VFTSw	AD + VFTSw + DFA/CIWT/SMT	不正のリスクが高い場合は“B”を選択する
ハードウェア機構支援				
5.1.4.1	有意欠陥の検知支援	AD + VFTSw	AD + VFTSw + CIWT + SMT	高い信頼性が求められる場合は“B”を選択する
5.1.4.2	耐久性保護	AD + VFTSw	AD + VFTSw + CIWT + SMT	高い信頼性が求められる場合は“B”を選択する
5.1.5	時刻刻印	AD + VFTSw	AD + VFTSw + SMT	
法定関連部分の指定及び分離，並びにインターフェースの指定				
5.2.1.1	構成部品の分離	AD	AD + DFA/CIWT	
5.2.1.2	ソフトウェア部分の指定及び分離	AD	AD + DFA/CIWT	
5.2.2	共有表示	AD + VFTM/ VFTSw	AD + VFTM/ VFTSw + DFA/CIWT	
5.2.3	データ保存	AD + VFTSw	AD + VFTSw + CIWT/SMT	安全でない記憶装置への測定データの保存が予測される場合は“B”を選択する
5.2.3.1	保存する測定値に，将来の法定関連の使用に備えて，必要なすべての関連情報を添付	AD + VFTSw	AD + VFTSw + CIWT/SMT	不正のリスクが高い場合は“B”を選択する
5.2.3.2	保存したデータは，信ぴょう性，完全性，及び，必要な場合，測定時刻に関する情報の正確性を ソフトウェア手段で保護しなければならない	AD + VFTSw	AD + VFTSw + SMT	

5.2.3.3	自動保存	AD + VFTSw	AD + VFTSw + SMT	
5.2.4	通信線を介した伝送	AD + VFTSw	AD + VFTSw + CIWT/SMT	開放型ネットワークでの測定データの伝送が予測される場合は“B”を選択する
5.2.4.1	伝送された測定値は，その後の法定関連使用に必要なすべての関連情報を伴わなければならない	AD + VFTSw	AD + VFTSw + CIWT/SMT	不正のリスクが高い場合は“B”を選択する
5.2.4.2	伝送されたデータは，測定時刻に関する情報の信憑性，完全性，及び必要な場合は，正確さを保証するためにソフトウェア手段で保護しなければならない	AD + VFTSw	AD + VFTSw + SMT/	
5.2.4.3	伝送遅延	AD + VFTSw	AD + VFTSw + SMT	例えば開放型ネットワークでの伝送など不正のリスクが高い場合は“B”を選択する

5.2.4.4	伝送中断	AD + VFTSw	AD + VFTSw + SMT	例えば開放型ネットワークでの伝送など不正のリスクが高い場合は“B”を選択する
5.2.5	オペレーティングシステム及びハードウェアの互換性	AD + VFTSw	AD + VFTSw + SMT	
5.2.5.2	保護ソフトウェアインターフェースを備えていないハードウェアインターフェースは，法定関連ソフトウェア部分に容認できないほどに影響を与えてはならない。	AD + VFTSw	AD + VFTSw + SMT	
5.2.5.3	法定関連ソフトウェア部分の保護を確実なものとするためにセキュアブートプロセスが必要とされる場合，次の要件が適用される。	AD + VFTSw	AD + VFTSw + SMT	
5.2.5.4	法定関連ソフトウェア部分とオペレーティングシステムの組み合わせは，法定関連アプリケーションの動作のための十分なリソースがあることを確実なものとしなければならない。	AD + VFTSw	AD + VFTSw + SMT	
5.2.5.5	使用中の保護	AD + VFTSw	AD + VFTM/VFTSw + DFA	
5.2.5.6	法定関連ソフトウェア部分との通信は，保護インターフェースを介して行わなければならない。	AD + VFTSw	AD + VFTM/VFTSw + DFA	
5.2.5.7	可試験性及びトレーサビリティ	AD + VFTSw	AD + VFTSw + SMT	
5.2.5.8	製造事業者は，適切なハードウェア及びソフトウェアの環境を明らかにしなければならない。	AD + VFTSw	AD + VFTSw + SMT	
5.2.5.9	最小構成要件が満たされている場合，動作を阻止するために，法定関連ソフトウェアの中に技術的手段を備えなければならない。	AD + VFTSw	AD + VFTSw + SMT	

保守及び再構成				
5.2.7.2	要検定更新	AD	AD	
5.2.7.3	追跡可能更新	AD + VFTSw	AD + VFTSw + CIWT/SMT	不正のリスクが高い場合は“B”を選択する

表 2: さまざまなソフトウェア要件のための評価及び検証手法の組合せ推奨案
（表 1 で定義した頭字語）

6.5 被試験装置（EUT）

通常，試験は完全な計量器で実施される（機能試験）。計量器の大きさ又は構成が全体ユニットとして試験に対応できない場合，若しくは計量器の個別構成部品又はモジュールだけが関係する場合，動作中の構成部品又はソフトウェアモジュールを使った試験の場合に，それらはその正常動作を十分に表したシミュレートした設定に含まれていると仮定して，試験全体又は特定の試験を構成部品又はソフトウェアモジュールで個別に実施しなければならないと，その関連勧告は指示することができる。申請者は，必要な装置及び供試器すべてを提供する責任を負う。

7 計量器の検定

7.1 計量器の計量管理が規定されている国では，動作中にソフトウェア識別，調整の妥当性及び承認済型式への適合性を現場でチェックする手段がなければならない。

関連勧告は，対象計量器の性質に従って一局面以上の場面でソフトウェアの検証の実施を要求することができる。

ソフトウェアの検証には，以下を含まなければならない：

- ソフトウェアが承認済バージョンであることを検証するための，ソフトウェアの適合性の検査（例えば，ソフトウェア識別のチェック，保全手段のチェック）
- 証明書に記載されている場合，構成が宣言された最小構成と矛盾しないことを検証するための検査
- 計量器への入力／出力に不要な副次的悪影響のないことを検証するための同入力／出力の検査
- 装置固有パラメータ（特に校正パラメータ）が正しく設定されていることを検証するための同パラメータの検査

PG は，計器固有検証手順を書くときに，次の節を考慮しなければならない。7.2 の中で示されている手法は，標準手順として提案されている。

7.2 検定手法，試験項目

次の手法は，5.1 及び 5.2 の要件をチェックするために必要とされている検定手順で構成されている。次に列記する対応計器を用いて，次の側面を審査しなければならない。

7.2.1 文書

あらゆるソフトウェア検定の最初の手順は，EUT の証明書及びその附属書との適合性を求めるチェックで構成される。

- 証明書が有効であるかどうかをチェックする
- EUT が証明書及びその附属書の中に記載されている型式に適合するかどうか
- 操作説明書（オペレーティングマニュアル）が入手できるかどうか（求められている場合）

7.2.2 ソフトウェアの完全性

- 間接的： 証明書の中で求められているすべての封印が適切な位置に置かれ，無傷であるか どうかをチェックする。
- 直接的：ソフトウェア識別情報が証明書の中で求められているかどうかをチェックする。

例：

公称値と比較されるプログラムコードのチェックサムの計算。

7.2.3 パラメータ

7.2.3.1 正当性

- パラメータの間接的な計量的検証：測定を行い，結果を基準と比較する。
- すべての設定可能パラメータが許容範囲内であるかどうかをチェックする。

7.2.3.2 完全性

- パラメータを保護する封印が無傷であるかどうかをチェックする。
- パラメータに関する入力項目の監査証跡又はログをチェックする。

7.2.4 ソフトウェアの識別情報

- EUT によって提供されたソフトウェアの識別情報が証明書の中で使用に有効であると規定 されていることをチェックする。
- 監査証跡の入力項目をチェックする。

8 リスク評価

8.1 本節は，ソフトウェア制御の計量器に行われる試験に対して一般的に適用する一連のリスクレベルを決定するための指針となることを意図したものである。それは，精度等級付けの場合のような特定要件につながる厳格な限度値持つ等級付けを意図していない。

さらに，この指針は，プロジェクトグループがこの文書の定めるガイドラインから生じるものと異なるリスク評価を規定することを妨げるものではない。関連勧告の中で規定された特別限界値に従って異なるリスクレベルを使用することができる。

8.2 計器の特定カテゴリー及び適用領域（商取引，対面販売，健康，法の執行，など）に対するリスクレベルを選択する場合，次の側面を考慮することができる：

(a) 不正のリクス：
- 機能不良の結果並びに社会的及び社会への影響
- 測定する商品の価値
- 使用するプラットフォーム（専用目的装置又は汎用装置）
- 潜在的不正の源への暴露（無人セルフサービス機器）

(b) 必要な適合性：
- 産業が規定レベルに準拠するための現実的な可能性

(c) 必要な信頼性：
- 環境条件
- 誤動作の結果並びに社会的及び社会への影響

(d) 不正を働く側の動機づけ

(e) 測定を繰り返す又は中断する可能性

PG は，リスクレベルを決定するときに，リスク評価標準，例えば ISO27005 を考慮することが望ましい。

要件の節（5 を参照）を通して，容認可能な技術的解決策のさまざまな例が，不正に対する保護，

適合性，信頼性及び測定の種類の基本レベル（(I) とマーク）を図示して示されている。適切な場合，上記した側面の一段高めたリスクレベルを考慮した強化解決策を持つ例も提示される（(II) とマーク）。

審査レベル及びリスクレベルは，関連している。ソフトウェア誤り又はセキュリティの脆弱性を検出するため，一段高めたリスクレベルが要求されるときには，そのソフトウェアの深い分析を実施しなければならない。他方，審査レベルを選択するに当たって，機械的封印（例えば，通信ポート又は筐体の封印）を考慮すべきである。

附属書 A

参考文献

出版時に，下記の版は有効であった。すべての引用文書，は改定の対象であり，この文書の利用者は，下記引用文書の最新版を適用できることを調べるよう勧められる。IEC 及び ISO の加盟国は，現在有効な国際規格の登録簿を維持している。

参照された規格の現状は，インターネット上でも見ることができる：

IEC Publications: http://www.iec.ch/searchpub/cur_fut.htm

ISO Publications: http://www.iso.org

OIML Publications: https://www.oiml.org/en/publications/
（PDF ファイルの無料ダウンロードで）

誤解を避けるため，国際勧告及び国際文書の中の規格への参照にはすべて，バージョン（一般的に年又は日付）を付けることが強く推奨される。

Ref.	規格及び参考文書	説明
[1]	OIML V 2-200:2012 国際計量用語集（VIM)	計量関連ガイドに関する合同委員会（JCGM）によって作成された用語集
[2]	OIML D 11:2013 電子計量器の一般要求事項－環境条件	OIML 勧告に規定のある計量器への影響量に対する適正な計量性能試験要件確立のための手引き（EMC，気候，機械的影響）
[3]	ISO/IEC 9594-8:2014 情報技術－開放型システム間相互接続－：ディレクトリ：第 8 部：公開かぎ及び属性認証フレームワーク	ISO/IEC 9594-8:2014 は，二者間通信，たとえば，二つの住所録サービス間，又はウェブブラウザとウェブサーバーの間の通信，での身元認証及びセキュリティ確立に使える枠組及び多数のデータ・オブジェクトを指定する。このデータ・オブジェクトは，電子署名付き文書などデータ構造の身元及び完全性の証明にも使える。

[4]	ISO 2382-9:1995 情報技術－用語集－第 9 部：データ通信	データ通信における国際通信を容易にするためのもの。データ通信の領域に関する用語及びいくつかの選択した概念の定義を提示し，それらの関係を識別する。
[5]	ISO/IEC 25040:2011 シリーズ 情報技術－ソフトウェア製品の評価	ISO/IEC 25040:2011 シリーズの規格は，ソフトウェア製品品質の測定，評価及び評価の方法を規定している。それは，ソフトウェア生産工程評価もコスト予測方法も記述していない。ソフトウェア製品品質の測定は，もちろん，これらの目的両方に使うことができる）
[6]	OIML V 1:2013 国際法定計量用語集（VIML）	VIML は，法定計量分野で用いられる概念だけを含んでいる。これらの概念は，この活動に関連する他の問題だけでなく法定計量サービスの諸活動，関連文書に関係している。この用語集は，VIM から引用した一般的な性格の概念が含まれている。
[7]	IEC 61508-5:2010 電気／電子／プログラマブル電子安全関連系の機能安全－第 5 部：安全度水準の決定方法の例	リスク及びリスクと安全完全性の関係の基本的概念についての情報を提供する（附属書 A 参照よ）。E/E/PE 安全関連系，その他技術安全関連系及び外部リスク低減設備の安全完全性レベル決定を可能にする多数の方法（付録 C，C，D，E を参照）。IEC ガイド 104 及び ISO/IEC ガイド 51 に含まれた原則に従って規格作成で技術委員会が使用することを意図している。
[8]	WELMEC ガイド 2.3，2005 年 5 月第 3 版 ソフトウェア審査のための手引き（はかり）	
[9]	WELMEC ガイド 7.2，2015 年 ソフトウェア手引き（計量器指令 2014/32/EU)	この文書は，計量器指令（欧州指令 2014/32/E;MID），特に，ソフトウェア搭載計量器への適用に関わるすべての関係者に向けた手引きを提供する。それは計量器の製造事業者及び MID 計量器の適合性評価を司る認証機関を対象とする。この手引きに従えば，MID に含まれるソフトウェア関連要件へ準拠していることが見込まれる。

附属書 B

ソフトウェア試験報告書の事例

（参考）

備考: OIML 勧告を作成している技術委員会及び小委員会は，ソフトウェア試験報告書，評価報告書及び OIML 適合証明書がどの情報を含まなければならないかを決めなければならない。例えば，以下の例から，実行コードの名称，バージョン及びチェックサムが証明書に含まれるのが望ましい。

ソフトウェア試験報告 no XYZ122344
流用計 Tournesol Metering モデル TT100 のソフトウェア評価

計量器ソフトウェアが OIML 勧告 R-xyz の要件に適合していることを示すため，その検証を行った。

その妥評価は，報告書 OIML 文書 D-31 YYYY に基づくものであって，そこに，そのソフトウェアの重要要件が解釈，解説されている。この報告書は R-xyz への適合性を述べるために必要なソフトウェア評価を記述する。

製造事業者	申請者
Tournesol Metering	New Company
P.O. Box 1120333	Nova Street 123
100 Klow	1000 Las Dopicos
Syldavie	San Theodorod
照会先：Mr. Tryphon Tournesol	照会先：Archibald Haddock

試験対象

Tournesol Metering の計量器 TT100 は，液状の流量を測定するための計量器である。その意図する測定範囲は，1 L/s から 2000 L/s までである。この計量器の基本機能は，以下の通りである：

- 液状の流量を測定
- 測定体積の表示
- 変換器へのインタフェース

この流量計は，法定関連データを収納する記憶装置を備えた専用目的の装置（組込みシステム）である。

流量計 TT100 は，変換器を接続した独立計量器である。その接続した変換器は，温度補正機能を内蔵している。流速の調整は，その変換器の不揮発性メモリに保存された校正パラメータによって可能である。変換器は，流量計に固定されていて，取り外すことはできない。測定した体積は，ディスプレイ上に表示される。その他の装置との通信は，不可能である。

その計量器の組込みソフトウェアは，次の製造事業者によって開発された：

Tournesol Metering, P.O. Box 1120333, 100 Klow, Syldavie.

その実行コードのファイル名は，“**tt100_12.exe**”である。
このソフトウェアの検証済みバージョンは，**V1.2c** である。このバージョンは，装置の起動時及び“レベル”ボタンを **4** 秒間押した時に，ディスプレイ上に表示される。

ソースコードは，次の法定計量関連ファイルからなっている：

- main.c 12301 byte 23 Nov 2003;
- int.c 6509 byte 23 Nov 2003;
- filter.c 10897 byte 20 Oct 2003;
- input.c 2004 byte 20 Oct 2003;
- display.c 32000 byte 23 Nov 2003;
- ethernet.c 23455 byte 15 June 2002;
- driver.c 11670 byte 15 June 2002;
- calculate.c 6788 byte 23 Nov 2003.

実行可能コード“**tt100_12.exe**”は， チェックサムによって変更から保護されている。アルゴリズム **XYZ** によるチェックサムの値は，**1A2B3C** である。

その評価は，製造事業者からの次の文書によって裏付けられた：

- TT 100 利用者手引き 1.6 版
- TT 100 100 保守手引き 1.1 版;
- ソフトウェア記述書 TT100（内部設計文書，2003 年 11 月 22 日付）
- 電子回路図 TT100（図番 222-31，2003 年 10 月 15 日付）

試験対象の最終バージョンは，2003 年 11 月 25 日に国立計測研究所へ送付された。

評価の結果
評価は，OIML D31 YYYY に従って実施された。その評価は，2003 年 11 月 1 日から 2003 年 12 月 3 日の間に実施された。設計レビューは，12 月 3 日に Klow の Tournesol Metering 本社で, Dr. K. Fehler によって行われた。その他の評価作業は, 国立計測研究所において, Dr. K. Fehler 及び Mr. S.Probleme により行われた。

以下の要件に対する検証を行った：

- ソフトウェア識別
- アルゴリズム及び機能の正しさ
- ソフトウェア保護
- 偶発的誤使用防止
- 介入の証拠
- ハードウェア機能の支援
- データ保存，通信システムを介した伝送

次の評価及び検証手法が適用された：

- 文書解析と設計の評価
- 計量機能の機能試験による検証
- 渡り歩き，コード精査
- SDK XXX を持つモジュール calculate.c のフトェア・モジュール試験

結果
OIML D31 の次の要件：YYYY は，不適合が一切発見されず，検証された。

5.1.1，5.1.2，5.1.3.2，5.2.1，5.2.2.1，5.2.2.2，5.2.2.3

この結果は，シリーズ番号 1188093-B-2004 の試験サンプルにだけ適用される。

結論

Tournesol Metering TT100 V1.2c のソフトウェアは，OIML R-xyz の要件を満たしている。

国立計測研究所
ソフトウェア部門

Dr. K.E.I.N. Fehler	Mr. S.A.N.S. Problème
技術主任	技官

念

チェックリスト

条項	要件	合格	不合格	備考
5.1 **5.1.1**	**一般要件** **ソフトウェア識別** 計量器／構成部品のソフトウェアは，明確に識別されなければならない			
5.1.2	**アルゴリズムと機能の正しさ** 計量器の測定アルゴリズムと機能は，所与の用途及び装置型式に対し，適切かつ機能的に正しくなければならない。			
5.1.3 **5.1.3.1**	**ソフトウェア保護** **誤用防止** 計量器が，意図しない，偶発的な，又は意図的な誤用の可能性を最小にするように設計されていなければならない。			
5.1.3.2 **a)** **b)** **c)** **d)**	**不正防止** ソフトウェアは，あらゆる介入（例えば，ソフトウェアの更新，パラメータの変更）の証拠が入手できるような方法で保護しなければならない。ソフトウェアは，その記憶装置の未認定の修正，ローディング又はメモリ装置の取替による変更に対して保全されていなければならない。 明確に文書化された機能で，計器の計量特性に影響を与えないものだけが，ユーザインタフェースによって起動することができる。 計量器の法定計量関連特性を決定するパラメータが，不正な改変から保全されていなければならない。計量器の検定のために必要な場合，現在のパラメータ設定の表示又は印字が可能でなければならない。 ソフトウェア保護は，不正な介入を不可能又は明らかにする機械的，電子的及び／又は暗号的手段による適切な封印によってなっている。			
5.1.4 **5.1.4.1**	**ハードウェア機能の支援** **有意欠陥の検出の支援** 計量器製造事業者が，ソフトウェア又はハードウェア部分の中に検出機構を設計すること若しくはその計器のソフトウェア部分によってハードウェア部分が支援を受けられる手段を提供しなければならない。			
5.1.4.2	**耐久性保護の支援** ソフトウェア又ハードウェア内に耐久性保護機構を実現するか若しくはソフトウェアがハードウェア機構を支援できるようにするかの選択は製造事業者に委ねられる。			

5.1.5	**時刻刻印** 時刻刻印は，計器のクロックから読み出さなければならない。適用されるリスクレベルに応じて適切な保護手段を講じなければならない。			
5.2 **5.2.1**	**構成に固有の要件** **法定計量に関連する部分の特定と分離，及びインタフェースの特定** 計量器の法定関連部分は，不法に影響を受けてはならない。			
5.2.1.1 **a)** **b)**	**構成部品の分離** 法定計量関連機能を実行する計量器の構成部品が識別され，かつ明確に定義され，文書化されなければならない。 法定関連構成部品の機能及びデータが，他の法定非関連部分へのインタフェースを介して受け取るコマンドによって不法に影響されてはならない。			

5.2.1.2 **a)** **b)**	**ソフトウェア部分の指定及び分離** 計量器の法定関連ソフトウェア部分に適合性要件を適用し（5.2.6 を参照），5.1.1 に記述したように識別できなければならない。 法定計量関連ソフトウェア部分が他のソフトウェア部分と通信を行う場合，ソフトウェアインタフェースを定義しなければならない。すべての通信は，このインタフェースを介して独占的に行われなければならない。法定計量関連ソフトウェア部分及びそのインタフェースが明確に文書化されていなければならない。法定計量関連機能とソフトウェアのデータ領域がすべて記述され，型式評価当局が正しいソフトウェア分離について決定できるように記述されていなければならない。			

節	要件	合格	不合格	備考
c) **d)**	法定関連ソフトウェア部分では，すべての起動された機能又はデータ変更に対する各コマンドにあいまいでない割り当てが存在しなければならない。ソフトウェアインターフェースを介して起動される機能は，宣言され，文書化されていなければならない。文書化された機能だけが，そのソフトウェアインターフェースを介して起動することが可能である。 法定関連ソフトウェア部分が法定非関連ソフトウェア部分から分離されている場合，その法定関連ソフトウェア部分は，非関連ソフトウェアより多くのコンピュータ資源を利用する優先権を持っていなければならない。法定関連プロセスは，法定非関連ソフトウェアによる容認できないほどの割り込みがあってはならない。			
5.2.2	**共有表示** 表示又は印字出力が，法定関連出力及び法定非関連出力の両方に用いられる場合，法定関連情報は，常に判読可能で，かつ，その他の情報と明確言い区別できることが望ましい。			
5.2.3 **5.2.3.1**	**データの保存** 保存された測定値は，将来の法定関連利用に必要となるすべての関連情報を添付されていなければならない。			

2.3.2	保存されたデータは，信憑性，完全性及び，必要な場合，測定時刻に関する情報の正確性を保証するため，ソフトウェア手段によって保護されなければならない。測定値及び附属するデータを表示又はさらに処理するソフトウェアは，記憶装置からデータを読み出した後で，そのデータの測定時刻，信憑性及び完全性をチェックしなければならない。不備が検出された場合，そのデータは破棄し，使用不能とマークしなければならない。			

5.2.3.3 **a)** **b)**	**自動保存** データ保存が求められる場合，測定が終了した時，測定データは自動的に保存されなければならない。そのデータ記憶装置は，通常の保存条件下でデータが破損しないことを確実にするに十分な永続性を持っていなければならない。意図した用途に対して十分なメモリ容量がなければならない。 保存したデータは，次のいずれかの場合に削除することができる： – 伝送が完了した – データが法定管理対象の印字装置で印字された場合			
5.2.4	**通信線を介した伝送**			
5.2.4.1	伝送された測定値は，その後の法定利用のために必要なすべての関連情報を伴わなければならない。			
5.2.4.2	伝送されたデータは，測定時刻に関する情報の信憑性，完全性及び，必要な場合は，正確さを保証するために，ソフトウェア手段によって保護されなければならない。測定値及び附属するデータを表示又はさらに処理するソフトウェアは，記憶装置からデータを読み出した後で，そのデータの測定時刻，信憑性及び完全性をチェックしなければならない。不備が検出された場合，そのデータは破棄し，使用不能とマークしなければならない。			
5.2.4.3	データ伝送遅延によって測定は著しい影響を受けてはならない。			
5.2.4.4	ネットワークサービスが利用できなくなった場合，測定データを喪失してはならない。			

節	要件	合格	不合格	備考
5.2.5 **5.2.5.2**	**オペレーティングシステム及びハードウェアの互換性** オペレーティングシステムの要件それぞれは，アプリケーションレベル，オペレーティングシステムレベル，又はその両レベルの組み合わせに対する措置によって満たさなければならない。			

5.2.5.3 **a)**	保護ソフトウェアインターフェースを備えていないハードウェアインターフェースは，法定関連ソフトウェア部分に容認できないほど影響与えることが可能であってはならない。 法定関連ソフトウェア部分の完全性及び信憑性を確実なものとするために，ブートプロセスの個々の構成要素に全体に信頼の連鎖を確立しなければならない。			

b) **c)** **d)**	信頼の連鎖の処理は，その完全性が保たれている限りは，中断することができる。 ブート構成（コンフィギュレーション）は，不正な部分的変更を防がなければならない。 オープンインターフェースを介したブート処理は，保護しなければならない。			
5.2.5.4	法定関連ソフトウェア部分とオペレーティングシステムの組み合わせは，法定関連アプリケーションの動作のための十分なリソースがあることを確実なものとしなければならない。			
5.2.5.5 **a)** **b)** **c)** **d)**	**使用中の保護** 法定関連でないソフトウェアの動作は，法定関連アプリケーションに容認できないほどに影響を与えてはならない。 法定関連ソフトウェア部分とオペレーティングシステムの組み合わせは，法定関連表示が見分けられることを確実なものとしなければならない。 アクセス制御は，意図した使用が容認できないほどに影響を受けることがないような方法で構成しなければならない。 法定関連ソフトウェア部分の管理タスクは，保護しなければならない。			
5.2.5.6	法定関連ソフトウェア部分との通信は，保護インターフェースを介して行わなければならない。			
5.2.5.7 **a)** **b)**	**可試験性及びトレーサビリティ** オペレーティングシステムの構成は，識別可能でなければならない。 オペレーティングシステムの構成に対する変更が可能な場合，その変更はトレーサブルでなければならない。			
5.2.5.8	製造事業者は，適切なハードウェア及びソフトウェア環境を識別しなければならない。正しく機能するために必要な最小限のリソース及び適切な構成は，製造事業者が宣言しなければならない。			
5.2.5.9	最小構成要件が満たされない場合には，動作を防止するための技術的手段を備えなければならない。			
5.2.7 **5.2.7.1**	**保守及び再構成** 承認済型式に適合する法定関連ソフトウェアのバージョンだけが使用が許されている。			

5.2.7.2	**要検定更新** 計量器の法定関連ソフトウェアの更新（別の承認済バージョンとの交換又は再インストール）後，その計量器の検定が遂行され，その保全措置が更新されるまで，その計量器を法的目的のために用いること望ましくない。			

節	要件	合格	不合格	備考
5.2.7.3	**追跡可能更新**			
a)	ソフトウェアの追跡可能更新は，自動でなければならない。保全手段にオフとなっているものがある場合，更新後，更新プロセスの結果に関わらず，それらを再度直ちにオンとしなければならない。			
b)	ソフトウェアは，あらゆる介入の証拠を入手できるものとするような方法で保護しなければならない。更新中，あらゆる既存の監査証跡情報及び事象計数器の値は，保持しなければならない。			
c)	ロードしたソフトウェアの信憑性を保証するため，技術的手段を講じていなければならない。			
d)	ロードしたソフトウェアの完全性，即ち，ローディングの前に不法に変更されていないことを保証する技術手段が講じられていなければならない。			
e)	法定関連ソフトウェア部分の追跡可能更新が，その計量器内で十分追跡可能であることを保証するために，監査証跡を用いなければならない。			
f)	必要性及び国内法規に基づいて，計量器の使用者又は所有者が追跡可能更新に対する同者の承諾を与えることが必要であることがある。			
g)	ロードしたソフトウェアが完全性試験又は信憑性試験に不合格となった場合，その計器はそのソフトウェアの新バージョンを廃棄して，以前のバージョンを使用するか，不動作モードに切り替えなければならない。			
5.2.7.4	計量器には，その装置固有パラメータのあらゆる調整を自動的にしかも消去できないように記録する機構，例えば，監査証跡機構を備えなければならない。この計量器は記録したデータを提示できなければならない。			
5.2.7.5	監査証跡は，法定関連ソフトウェアの一部であり，そのように保護されなければならない。			

附属書 C

索引

容認可能位な事例: 5.1.1.

監査証跡: 3.1.1; 3.1.34; 5.1.3.2.d; 5.2.7.3; 5.2.7.3.b; 5.2.7.3.e; 5.2.7.3.g; 5.2.7.4; 5.2.7.5; 6.1.1; 6.2.1.

身元認証: 3.1.2; 3.1.3; 5.2.7.3.

信憑性: 3.1.3; 3.1.12; 5.1.3.2.d; 5.2.3.2; 5.2.4.2; 5.2.7.3.c; 5.2.7.3.g.

点検機能: 3.1.5; 5.1.4.1.

コマンド: 3.1.37; 5.1.3.2.b; 5.2.1.1.b; 5.2.1.2.b; 5.2.1.2.c; 6.1; 6.1.1; 6.2; 6.3.1; 6.3.2.1; 6.3.2.3; 6.3.2.4; Annex B（附属書 B）.

通信: 3.1.6; 3.1.44; 5.2.1.2.b; 5.2.1.2.c; 5.2.1.2.d; 5.2.4: 5.2.5.2; 6.3.1; 6.3.5.2.1; 6.4; 8.2; Annex B（附属書 B）.

通信インタフェース: 3.1.6; 5.1.1.

暗号化証明書: 3.1.7; 3.1.12; 5.1.3.2.d.

暗号化手法: 3.1.8; 5.1.3.2.d; 5.1.3.2.d; 5.2.7.3.c; 附属書 B.

データ領域： 3.1.9; 3,1,37; 3.1.38; 3.1.39; 5.2.1.2.b; 5.2.3.3.a; 6.3.2.4; 附属書 B.

装置固有パラメータ: 3.1.10; 3.1.26; 5.1.3.2.c; 5.2.7.1; 5.2.7.4.

耐久性: .3.1.11; 5.1.4.2; 6.1.1; 6.4; 附属書 B.

電子計量器: 3.1.12; 3.1.19; 8.1.

電子署名： 3.1.8; 3.1.13; 5.1.3.2.d; 5.2.3.2; 5.2.4.2; 5.2.7.3.c.

（指示の）誤差： 3.1.14; 3.1.19; 3.1.24; 8.2.

エラーログ： 3.1.15; 5.1.4.1.

評価: 3.1.45; 3.1.46; 3,1,350; 5.1.3.2.c; 5.1.4.1; 5.2.1.1.a; 5.2.1.2.b; 6.1; 6.1.1; 6.2; 6.3.1; 6.3.2.1; 6.3.2.2; 6.3.2.3; 6.4; 附属書 B

事象: 3.1.1; 3.1.16; 3.1.17; 3.1.34; 3.1.43; 5.1.3.2.d; 5. 2.7.3.e

事象計数計: 3.1.17; 5.1.3.2.d; 5.2.7.3.b; 6.2.1.

実行コード: 3.1.18; 3.1.41; 5.1.1; Annex B（附属書 B）.

誤り: 3.1.19; 3.1.19; 3.1.34; 3.1.43; Annex B（附属書 B）.

ハッシュ関数: 3.1.20; 5.1.4.1.

（プログラム，データ又はパラメータの）完全性: 3.1.13; 3.1.21; 5.2.3.2; 5.2.4.2; 5.2.5.3.a; 5.2.5.3.b; 5.2.7.3; 5.2.7.3.d; 5.2.7.3.g; 6.4; 附属書 B.

インタフェース: 3.1.4; 3.1.22; 5.1.1; 5.2.1; 5.2.1.1.a; 5.2.1.1.b; 5.2.1.2.d; 5.2.5.1; 5.2.5.2; 5.2.5.3.d; 6.1.1; 6.3.2.1; 6.3.2.3; 6.4; Annex B（附属書 B）.

固有誤差: 3.1.19; 3.1.24.

法定関連: 2.1; 3.1.1; 3.1.10; 3.1.25; 3.1.26; 3.1.27; 3.1.31; 3.1.37; 3.1.40; 3.1.42; 3.1.46; 5.1.3.1; 5.1.3.2.a; 5.1.3.2.b; 5.1.3.2.c; 5.1.3.2.d; 5.1.4.1; 5.1.5; 5.2.1; 5.2.1.1.a; 5.2.1.1.b; 5.2.1.2.a; 5.2.1.2.b; 5.2.1.2.c; 5.2.1.2.d; 5.2.2; 5.2.3.1; 5.2.3.2; 5.2.3.3.a; 5.2.4.1; 5.2.4.2; 5.2.5.1; 5.2.5.2; 5.2.5.3; 5.2.5.3.a; 5.2.5.3.d; 5.2.5.4; 5.2.5.5.a; 5.2.5.5.b; 5.2.5.5.d; 5.2.5.6; 5.2.5.7.a; 5.2.5.9; 5.2.6; 5.2.7; 5.2.7.1; 5.2.7.2; 5.2.7.3.c; 5.2.7.3.e; 5.2.7.5; 6.1; 6.1.1; 6.3.2.5; 6.4; Annex B（附属書 B）.

法定関連パラメータ: 3.1.10; 3.1.26; 3.1.46; 5.1.3.2.d; 5.1.4.1.

法定関連ソフトウェア部分: 3.1.27; 3.1.31; 3.1.40; 3.1.46; 5.1.3.2.a; 5.1.3.2.b; 5.1.4.1; 5.1.5; 5.2.1; 5.2.1.2.a; 5.2.1.2.b; 5.2.1.2.c; 5.2.1.2.d; 5.2.2; 5.2.3.2; 5.2.4.2; 5.2.5.2; 5.2.5.3; 5.2.5.3.a; 5.2.5.4; 5.2.5.5.b; 5.2.5.5.d; 5.2.5.6; 5.2.5.9; 5.2.6; 5.2.7; 5.2.7.1; 5.2.7.2; 5.2.7.3.e; 5.2.7.5; 6.1; 6.1.1; 6.3.2.5; 附属書 B.

最大許容誤差: 3.1.28; 3.2; 6.3.2.2.

計量器: 1; 2.1; 2.2; 2.3; 3; 3.1.1; 3.1.2; 3.1.5; 3.1.6; 3.1.7; 3.1.11; 3.1.12; 3.1.15; 3.16; 3.1.18; 3.1.19; 3.1.26; 3.1.27; 3.1.28; 3.1.29; 3.1.32; 3.1.34; 3.1.38; 3.1.39; 3.1.40; 3.1.45; 3.1.46; 3.1.48; 3.1.50; 4.3; 5.1; 5.1.1; 5.1.2; 5.1.3.1; 5.1.3.2.a; 5.1.3.2.c; 5.1.3.2.d; 5.1.4.2; 5.1.5; 5.2; 5.2.1; 5.2.1.1.a; 5.2.1.2.a; 5.2.1.2.d; 5.2.2; 5.2.3.1; 5.2.3.2; 5.2.4.1; 5.2.4.2; 5.2.5.1; 5.2.7; 5.2.7.1; 5.2.7.2; 5.2.7.3; 5.2.7.3.a; 5.2.7.3.c; 5.2.7.3.e; 5.2.7.3.f; 5.2.7.3.g; 5.2.7.4; 6.1; 6.1.1; 6.2; 6.3.2.1; 6.3.2.2; 6.5; 7.1; 8.1; Annex B（附属書 B）.

割り込み不能／割り込み可能測定: 3.1.23; 3.1.30; 5.1.4.1.

オペレーティングシステム：3.1.4; 3.1.47; 5.1.3.2.a; 5,2.1.2.c; 5.2.1.2.d; 5.2.2; 5.2.5.1; 5.2.5.2; 5.2.5.3.d; 5.2.5.5.b; 5.2.5.6; 5.2.5.7.a; 5.2.5.7.b; 5.2.5.8; 5.2.5.9; 6.1.1; 6.4; 附属書 B.

性能: 3.1.11; 6.2.

プログラムコード: 3.1.37; 5.1.4.1; 5.2.1.2.b; 5.2.3.2; 5,2,4,2; 7.2.2.

保護インターフェース：3.1.31; 5.2.5.1; 5.2.5.2; 5.2.5.6; 6.4; 附属書 B.

封印: 3.1.32; 5.1.3.2.a; 5.1.3.2.d; 6.1.1; 8.2; 附属書 B.

保全: 3.1.13; 3.1.33; 5.2.1.1.a; 5.2.1.1.b; 5.2.2; 5.2.7.2; 5.2.7.3.a; 6.2.1; 7.1; 附属書 B.

ソフトウェア審査: 3.1.35; 5.1.2; 6.2.

ソフトウェア識別: 3.1.36; 5.1.1; 5.2.7.3.e; 6.1.1; 6.2.1; 6.3.2.3; 6.4; 7.1; Annex B（附属書 B）.

ソフトウェアインタフェース: 3.1.37; 3.1.40; 5.2.1.2.b; 5.2.1.2.c; 5.2.5.2; 5.2.5.6; 6.1; 6.1.1; 6.3.2.4; 附属書 B.

ソフトウェアモジュール: 3.1.9; 3.1.16; 3.1.27; 3.1.31; 3.1.36; 3.1.37; 3.1.38; 5.1.3.2.b; 5.2.1.2.a; 5.2.3.2; 5.2.4.2; 5.2.5.6; 6.1.1; 6.3.1; 6.3.2.6; 6.5; Annex B（附属書 B）.

ソフトウェア保護: 3.1.39; 5.1.3; 5.1.3.2.d; 6.4; Annex B（附属書 B）.

ソフトウェア分離: 3.1.40; 5.2.1.2.b; 5.2.1.2.d; 6.3.1; 6.3.2.4; 附属書 B.

ソースコード: 3.1.41; 6.1.1; 6.3.1; 6.3.2.2; 6.3.2.4; 6.3.2.5; 6.3.2.6; Annex B（附属書 B）.

保存装置: 3.1.42; 5.2.3.a; 5.2.3.e; Annex B（附属書 B）.

試験 : 3.2; 5.1.2.; 5.1.5; 5.2.7.3.g; 6.2; 6.3.1; 6.3.2.1; 6.3.2.2; 6.3.2.3; 6.3.2.6; 6.4; 6.5; 7.2; 8.1; Annex B（附属書 B）.

時刻刻印: 3.1.1; 3.1.43; 5.1.5; 5.2.1.1.b; 5.2.3.1; 5.2.4.1; 5.2.7.3.e; 6.4; 附属書 B.

測定データの伝送: 3.1.44; 5.2.1.1.a; 5.2.4; 5.2.4.2; 5.2.4.3; 5.2.4.4; 6.4; Annex B（附属書 B）.

型式固有パラメータ: 3.1.26; 3.1.46; 5.1.3.2.c.

汎用装置: 3.1.47; 5.1.3.2.a; 5.2.1.1.a; 5.2.1.2.c; 5.2.1.2.d; 5.2.5.9; 8.2.

ユーザインタフェース: 3.1.48; 5.1.1; 5.1.3.2.b; 5.2.2; 6.1.1; 6.3.2.3; 附属書 B.

検定: 3.1.49; 3.1.50; 5.1.3.2.c; 5.2.7; 5.2.7.1; 5.2.7.2; 5.2.7.3; 5.2.7.3.e; 5.2.7.3.g; 6.2; 6.3; 6.3.2; 6.3.2.2; 6.3.2.3; 6.3.2.6; 6.4; 7.1; 7.2; 7.2.1; 附属書 B.