DOCUMENT
INTERNATIONAL

OIML D 31

Edition 2008 (F)

Exigences générales pour les instruments de mesure contrôlés par logiciel

General requirements for software controlled measuring instruments

OIML D 31 Edition 2008 (F)

ORGANISATION INTERNATIONALE
DE MÉTROLOGIE LÉGALE

INTERNATIONAL ORGANIZATION
OF LEGAL METROLOGY

Sommaire

Avant-propos

L'Organisation Internationale de Métrologie Légale (OIML) est une organisation intergouvernementale mondiale dont l'objectif principal est d'harmoniser les réglementations et contrôles métrologiques mis en œuvre par les services nationaux de métrologie, ou organismes apparentés, de ses Etats Membres. Les principales catégories de publication de l'OIML sont :

- **Les Recommandations Internationales (OIML R)**, qui sont des modèles de réglementations fixant les caractéristiques métrologiques d'instruments de mesure et les méthodes et moyens de contrôle de leur conformité; les États Membres de l'OIML doivent, dans la mesure du possible, mettre en application ces Recommandations;

- **Les Documents Internationaux (OIML D)**, qui sont de nature informative et destinés à améliorer l'activité des services de métrologie;

- **Les Guides Internationaux (OIML G)**, qui sont de nature informative et qui sont destinés à donner des directives pour la mise en application à la métrologie légale de certaines exigences; et

- **Les Publications de Base Internationales (OIML B)**, qui définissent les règles de fonctionnement des différentes structures et systèmes OIML.

Les projets de Recommandations, Documents et Guides OIML sont élaborés par des Comités Techniques ou Sous-Comités Techniques composés de représentants d'États Membres. Certaines institutions internationales et régionales y participent également à titre consultatif. Des accords de coopération ont été conclus entre l'OIML et certaines institutions, telles que l'ISO et la CEI, pour éviter des prescriptions contradictoires; en conséquence les fabricants et utilisateurs d'instruments de mesure, les laboratoires d'essais, etc. peuvent appliquer simultanément les publications OIML et celles d'autres institutions.

Les Recommandations internationales, Documents et Guides sont publiés en français (F) et en anglais (E) et sont révisés périodiquement.

De plus l'OIML participe à la publication de **Vocabulaires (OIML V)** et mandate périodiquement des Experts en métrologie légale pour rédiger des **Rapports d'Expert (OIML E)**. Les Rapports d'Expert sont déstinés à fournir des informations et conseils aux autorités de métrologie, et reflètent uniquement le point de vue de leur auteur, en dehors de toute participation d'un Comité Technique ou d'un Sous-Comité Technique, ou encore de celle du CIML. Ainsi, ils ne reflètent pas nécessairement l'opinion de l'OIML.

Cette publication - référence OIML D 31, édition 2008 (F) – a été élaborée par le Sous-Comité Technique OIML TC 5/SC 2 *Logiciel*. Elle a été approuvée par le Comité International de Métrologie Légale en 2008 pour publication finale.

Les Publications de l'OIML peuvent être téléchargées depuis le site internet de l'OIML sous la forme de fichiers PDF. Des informations complémentaires sur les Publications OIML peuvent être obtenue au siège de l'Organisation :

Bureau International de Métrologie Légale
11, rue Turgot - 75009 Paris - France
Téléphone : 33 (0)1 48 78 12 82
Fax : 33 (0)1 42 82 17 27
E-mail : biml@oiml.org
Internet : http://www.oiml.org

Exigences générales pour les instruments de mesure contrôlés par logiciel

1 Introduction

L'objectif principal de ce Document International est de fournir aux Comités et Sous-Comités Techniques de l'OIML des conseils leur permettant d'établir les exigences portant sur les fonctionnalités logicielles des instruments de mesure couverts par les Recommandations de l'OIML.

De plus, ce Document International peut servir d'aide aux Etats Membres de l'OIML lors de la transcription des Recommandations OIML dans leur réglementation nationale.

2 Champ et domaine d'application

2.1 Ce Document International précise les exigences générales applicables aux fonctionnalités logicielles des instruments de mesure et donne des précisions sur les moyens de vérifier la conformité à ces exigences.

2.2 Ce Document doit être considéré par les Comités et Sous-Comités Techniques de l'OIML comme une base pour l'établissement d'exigences et de procédures spécifiques aux logiciels dans une Recommandation OIML relative à certaines catégories d'instruments de mesure (ci-après appelée Recommandation OIML appropriée).

2.3 Les instructions données dans ce Document s'appliquent uniquement aux instruments de mesure, ou dispositifs électroniques, contrôlés par logiciel.

Notes :

- Ce Document ne couvre pas toutes les exigences techniques applicables aux instruments de mesure contrôlés par logiciel. Ces exigences doivent être indiquées dans la Recommandation OIML appropriée, par exemple, celles pour les instruments de pesage, celles pour les compteurs d'eau, etc.
- Ce Document traite certains aspects relatifs à la sécurité des données. En plus de ce dernier, les réglementations nationales dans ce domaine doivent être prises en compte.
- Comme les dispositifs contrôlés par logiciel sont toujours électroniques, il est également nécessaire de tenir compte de l'OIML D 11 *Exigences générales pour les instruments de mesure électroniques*.

3 Terminologie

Certaines définitions utilisées dans ce Document sont conformes au *Vocabulaire International des Termes Fondamentaux et Généraux de Métrologie* (VIM:1993 [1]), au *Vocabulaire International des Termes de Métrologie Légale* (OIML V 1:2000 [8]), au Document International de l'OIML *Exigences générales pour les instruments de mesure électroniques* (OIML D 11:2004 [3]) et à certaines Normes Internationales de l'ISO/CEI. Dans le cadre de ce Document, les définitions et abréviations suivantes sont applicables.

3.1 Terminologie générale

3.1.1 Solution acceptable

Conception ou principe de module logiciel ou d'unité matériel, ou conception ou principe d'une caractéristique qui est considéré comme conforme à une exigence donnée. Une solution acceptable fournit un exemple illustrant comment une exigence donnée peut être respectée, sans préjudice pour les autres solutions respectant également l'exigence.

3.1.2 Expertise de l'historique

Fichier continu de données contenant un enregistrement horodaté des évènements, par exemple des changements de valeur des paramètres d'un dispositif, ou les mises à jour d'un logiciel, ou toutes autres activités réglementairement pertinentes qui pourraient influencer les caractéristiques métrologiques.

3.1.3 Authentification

Vérification de l'identité déclarée ou présumée d'un utilisateur, processus, ou dispositif (par exemple vérification que le logiciel téléchargé a bien pour origine le détenteur du certificat d'approbation de type).

3.1.4 Authenticité

Résultat du processus d'authentification (succès ou échec).

3.1.5 Système de contrôle [OIML D 11:2004, 3.18]

Système intégré à un instrument de mesure permettant de détecter et de mettre en évidence les défauts significatifs.

Note : "*Mettre en évidence*" fait référence à toute réponse appropriée de l'instrument de mesure (signal lumineux, signal sonore, protection du processus de mesurage, etc.).

3.1.6 Réseau fermé

Réseau composé d'un nombre fixe de participants ayant une identité, une fonctionnalité et un emplacement connus (voir également *Réseau ouvert*).

3.1.7 Commandes

Peuvent être une séquence de signaux électriques (optiques, électromagnétiques, etc.) sur les interfaces d'entrée ou des codes dans les protocoles de transmission de données. Elles peuvent être générées par le logiciel de l'instrument de mesure/dispositif électronique/sous-ensemble électronique (commandes logicielles) ou bien être générées par l'utilisateur par le biais de l'interface utilisateur de l'instrument de mesure (commandes utilisateurs).

3.1.8 Communication

Echange d'informations entre deux ou plusieurs unités (par exemple modules logiciels, dispositifs électroniques, sous-ensembles, etc.) suivant des règles spécifiques.

3.1.9 Interface de communication

Interface électronique, optique, radio ou autre interface technique permettant le transfert d'informations entre les composants d'un instrument de mesure (par exemple les dispositifs électroniques) ou ses sous-ensembles.

3.1.10 Certificat cryptographique

Jeu de données contenant la clef publique appartenant à un instrument de mesure ou personne complétée par un identificateur unique du sujet tel que le numéro de série de l'instrument de mesure ou le nom ou Numéro d'Identification Personnel (PIN) de la personne. Le jeu de données est signé par une institution irrécusable à l'aide d'une signature numérique. L'affectation de la clef publique à un sujet peut être vérifiée en utilisant la clef publique de l'institution irrécusable et en décryptant la signature du certificat.

3.1.11 Moyens cryptographiques

Cryptage des données par l'émetteur (le programme de stockage ou de transmission) et décryptage par le récepteur (programme de lecture) avec pour objectif la dissimulation des informations aux personnes non autorisées.

Signer électroniquement des données dans le but de permettre au récepteur ou utilisateur des données de vérifier l'origine de ces données, i.e. de prouver leur authenticité.

Note : Pour signer électroniquement, un système de clef publique est en général utilisé, i.e. l'algorithme nécessite une paire de clés dont une doit être maintenue secrète, l'autre pouvant être publique.

L'émetteur (le programme de stockage ou de transmission) génère un code de hachage des données (voir 3.1.25) et l'encrypte avec sa *clef privée*. Le résultat est la signature. Le récepteur (le programme de réception ou de lecture) décrypte la signature avec la *clef publique* de l'émetteur et compare le résultat avec le véritable code de hachage des données. En cas d'égalité, les données sont authentifiées.

Le récepteur peut exiger un certificat cryptographique de l'émetteur (voir 3.1.10) afin de s'assurer de l'authenticité de la clef publique.

3.1.12 Domaine de données

Emplacement en mémoire dont chaque programme a besoin pour traiter les données. En fonction du type de langage de programmation utilisé, cet emplacement est défini par une adresse matérielle ou par des noms symboliques (noms de variables). La taille du plus petit domaine adressable est typiquement un octet, mais la taille n'est pratiquement pas limitée : elle peut aller de 1 bit (par exemple un drapeau ou un registre) à des structures de données arbitraires qui peuvent être aussi grandes que les besoins du programmeur le sont.

Les domaines de données peuvent appartenir à un module logiciel unique ou à plusieurs. Pour les langages de haut niveaux (tels que le JAVA, le C/C++, etc.) il est simple de séparer le domaine de données d'un module logiciel, afin d'interdire son accès aux autres modules logiciels, grâce au langage de programmation lui-même.

3.1.13 Paramètre spécifique au dispositif

Paramètre réglementairement pertinent ayant une valeur dépendant de l'exemplaire de l'instrument. Les paramètres spécifiques aux dispositifs comprennent les paramètres d'ajustement (par exemple l'ajustement de la pente ou autres ajustements et corrections) ainsi que les paramètres de configuration (par exemple la valeur maximale, valeur minimale, unité de mesure, etc.).

3.1.14 Durabilité [OIML D 11:2004, 3.17]

Aptitude d'un instrument de mesure à maintenir ses caractéristiques de performance durant une période d'utilisation.

3.1.15 Instrument de mesure électronique [OIML D 11:2004, 3.1]

Instrument de mesure déstiné à mesurer une quantité électrique ou non-électrique en utilisant des moyens électriques et/ou équipés de dispositifs électroniques.

Note : Pour les besoins de ce Document, les équipements complémentaires, dans la mesure où ils sont soumis au contrôle de la métrologie légale, sont considérés comme faisant partie de l'instrument de mesure.

3.1.16 Dispositif électronique [OIML D 11:2004, 3.2]

Dispositif qui utilise des sous-ensembles électroniques et qui accomplit une fonction spécifique. Les dispositifs électroniques sont habituellement fabriqués en tant qu'unités séparées et sont susceptibles d'être testés séparément.

Notes : Un dispositif électronique peut être un instrument de mesure complet (par exemple une balance, un compteur électrique) ou une partie d'instrument de mesure (par exemple une imprimante, un indicateur).

Un dispositif électronique peut être un module au sens du terme utilisé dans l'OIML B 3 *Système de Certificats OIML pour les Instruments de Mesure* [2].

3.1.17 Erreur (d'indication) [VIM:1993, 5.20; OIML D 11:2004, 3.5]

Indication de l'instrument de mesure moins la valeur vraie de la grandeur d'entrée correspondante.

3.1.18 Registre des erreurs

Fichier continu de données contenant un enregistrement des défaillances/fautes qui ont une influence sur les caractéristiques métrologiques. Ceci s'applique particulièrement aux défaillances volatiles qui ne peuvent être identifiées ensuite lorsque les valeurs de mesure sont utilisées.

3.1.19 Evaluation (de type) [OIML V 1:2000, 2.5]

Examen et essai systématiques des performances d'un ou de plusieurs exemplaires d'un type (modèle) identifié d'instrument de mesure par rapport à des exigences documentées et dont le résultat est contenu dans un rapport d'évaluation afin de déterminer si le type peut être approuvé.

3.1.20 Evènement

Action par laquelle une modification d'un paramètre, d'un facteur d'ajustement de l'instrument de mesure ou la mise à jour d'un module logiciel est effectuée.

3.1.21 Compteur d'évènements

Compteur non réinitialisable qui s'incrémente chaque fois qu'un évènement a lieu.

3.1.22 Code exécutable

Fichier installé dans le système informatique de l'instrument de mesure, dispositif électronique, ou sous-ensemble (EPROM, disque dur, etc.). Ce code est interprété par le microprocesseur et transposé en opérations logiques, arithmétiques, de décodage ou de transport de données.

3.1.23 Faute [adapté de l'OIML D 11:2004, 3.9]

Défaut ayant un impact sur les propriétés ou fonctions de l'instrument de mesure ou causant une erreur d'indication supérieure à l'EMT.

3.1.24 Partie logicielle résidente réglementairement pertinente

Partie du logiciel réglementairement pertinent dans le code exécutable qui est et demeure identique à celle du type approuvé[1)].

3.1.25 Fonction de hachage [ISO/CEI 9594-8:2001][4]

Fonction (mathématique) qui lie les valeurs d'un grand domaine (potentiellement très grand) à une plus petite étendue. Une "bonne" fonction de hachage est telle que les résultats de l'application de la fonction à une (grande) série de valeurs dans le domaine seront uniquement distribués (et apparemment aléatoirement) sur l'étendue.

3.1.26 Intégrité des programmes, données et paramètres

Assurance que les programmes, données, ou paramètres n'ont pas fait l'objet de changements non autorisés ou non intentionnels en cours d'utilisation, de transfert, de stockage, de réparation ou de maintenance.

3.1.27 Interface [ISO 2382-9:1995][5]

Limite partagée entre deux unités fonctionnelles, définie par diverses caractéristiques se rapportant aux fonctions, aux interconnexions physiques, aux échanges de signaux, et autres caractéristiques des unités, si appropriés.

3.1.28 Erreur intrinsèque [VIM:1993, 5.24; OIML D 11:2004, 3.7]

Erreur d'un instrument de mesure, déterminée dans les conditions de référence.

3.1.29 Réglementairement pertinent

Logiciel/matériel/donnée ou partie du logiciel/matériel/donnée d'un instrument de mesure qui interfère avec les propriétés réglementées par la métrologie légale, par exemple l'exactitude de mesure ou le fonctionnement correct de l'instrument de mesure.

1) Cette partie est responsable de la surveillance de la mise à jour du logiciel (chargement du logiciel, authentification, vérification de l'intégrité, installation et activation).

3.1.30 Paramètre réglementairement pertinent

Paramètre d'un instrument de mesure, dispositif électronique, ou sous-ensemble sujet au contrôle légal. Les types de paramètre réglementairement pertinent suivants peuvent être distingués : les *paramètres spécifiques au type* et les *paramètres spécifiques au dispositif*.

3.1.31 Partie logicielle réglementairement pertinente

Partie de tous les modules logiciels d'un instrument de mesure, dispositif électronique, ou sous-ensemble qui est réglementairement pertinente.

3.1.32 Erreur maximale tolérée (d'un instrument de mesure) [VIM:1993, 5.21; OIML D 11:2004, 3.6]

Valeur extrême d'une erreur tolérée par les spécifications, règlements, etc., pour un instrument de mesure donné.

3.1.33 Instrument de mesure [VIM:1993, 4.1]

Dispositif destiné à être utilisé pour faire des mesurages, seul ou associé à un ou plusieurs dispositifs annexes.

3.1.34 Mesurage non-interruptible / interruptible

Un mesurage non-interruptible est un processus de mesure cumulatif continu sans fin définie. Le processus de mesure ne peut être stoppé et poursuivi ultérieurement par l'utilisateur ou opérateur sans perturber inacceptablement le mesurage ou l'approvisionnement en bien ou énergie.

Si le mesurage cumulatif de la quantité d'une substance peut être aisément et rapidement arrêté en opération normale – pas uniquement en cas d'urgence – sans falsifier les résultats de mesure, alors le mesurage est dénommé interruptible.

3.1.35 Réseau ouvert

Réseau à participants arbitraires (dispositifs électroniques ayant des fonctions arbitraires). Le nombre, l'identité et l'emplacement d'un participant peuvent être dynamiques et inconnus des autres participants (voir également *réseau fermé*).

3.1.36 Performance [OIML D 11:2004, 3.16]

Aptitude d'un instrument de mesure à accomplir les fonctions qui lui sont assignées.

3.1.37 Code programme

Code source ou *code exécutable*.

3.1.38 Scellement

Moyen destiné à protéger l'instrument de mesure contre toute modification non autorisée, réajustement, suppression de partie, logiciel, etc. Il peut être matériel, logiciel ou une combinaison des deux.

3.1.39 Sécuriser

Prévenir les accès non autorisés aux parties matérielles et logicielles du dispositif.

3.1.40 Logiciel

Terme générique comprenant le code programme, les données et les paramètres.

3.1.41 Examen logiciel

Opération technique consistant à déterminer une ou plusieurs caractéristiques du logiciel conformément à la procédure spécifique (par exemple l'analyse de la documentation technique ou l'exécution du programme dans des conditions contrôlées).

3.1.42 Identification du logiciel

Séquence de caractères lisibles (par exemple un numéro de version, une somme de contrôle) qui est inextricablement liée au logiciel ou au *module logiciel* à l'étude. Elle peut être vérifiée sur l'instrument en cours d'utilisation.

3.1.43 Interface logicielle

Code programme et domaine de données dédiés qui reçoivent, filtrent, ou transmettent les données entre les modules logiciels (sans qu'ils soient nécessairement réglementairement pertinents).

3.1.44 Module logiciel [similaire à CEI 61508-4:1998, 3.3.7][6]

Entité logique telle que programme, sous-programme, et objet incluant son domaine de données, qui peut être en relation avec d'autres entités. Le logiciel d'un instrument de mesure, dispositif électronique ou sous-ensemble est constitué d'un ou plusieurs modules logiciels.

3.1.45 Protection du logiciel

Sécurisation du logiciel de l'instrument de mesure ou du domaine de données par la mise en oeuvre de scellement mécanique ou logiciel. Le scellement doit être retiré, endommagé, ou brisé pour obtenir l'accès permettant de changer le logiciel.

3.1.46 Séparation logicielle

Le logiciel d'un instrument de mesure/dispositif électronique/sous-ensemble peut être divisé en une partie réglementairement pertinente et une partie non réglementairement pertinente. Ces parties communiquent via une interface logicielle.

3.1.47 Code source

Programme informatique écrit sous une forme lisible et éditable (langage de programmation). Le code source est compilé ou interprété en un *code exécutable*.

3.1.48 Dispositif de stockage

Stockage utilisé pour conserver les données de mesurage disponibles, après l'achèvement du mesurage, à des fins ultérieures réglementairement pertinentes (par exemple la conclusion d'une transaction commerciale).

3.1.49 Sous-ensemble [OIML D 11:2004, 3.3]

Partie de dispositif électronique, utilisant des composants électroniques et ayant par elle-même une fonction qui lui est reconnue.

Exemples : Amplificateurs, comparateurs, convertisseurs de puissance, etc.

3.1.50 Essai [OIML D 11:2004, 3.20]

Série d'opérations destinée à vérifier que l'équipement soumis à l'essai (EUT) est conforme aux exigences spécifiées.

3.1.51 Horodatage

Valeur de temps unique croissante monotone, par exemple en seconde ou une chaîne date et heure indiquant la date et/ou l'heure à laquelle un évènement particulier ou une faute s'est produit. Ces données sont présentées dans un format cohérent, facilitant la comparaison de deux enregistrements différents et le traçage dans le temps.

3.1.52 Transmission des données de mesure

Transmission des données de mesure via des réseaux de communication, ou d'autres moyens, à un dispositif électronique distant où elles sont ensuite traitées et/ou utilisées à des fins réglementairement pertinentes.

3.1.53 Paramètre spécifique au type

Paramètre réglementairement pertinent ayant une valeur qui dépend uniquement du type de l'instrument. Les paramètres spécifiques au type font partie du logiciel réglementairement pertinent.

Exemple : Considérant un ensemble de mesurage de liquides autres que l'eau, la plage de viscosité cinématique d'une turbine est un paramètre spécifique au type qui est fixé par l'approbation de type de la turbine. Toutes les turbines produites de ce même type, ont la même plage de viscosité.

3.1.54 Ordinateur universel

Ordinateur qui n'est pas construit pour une tâche spécifique mais qui peut être adapté aux fonctions métrologiques à l'aide d'un logiciel. En général, ce logiciel est basé sur un système d'exploitation qui permet le chargement et l'exécution de logiciels, à des fins spécifiques.

3.1.55 Interface utilisateur

Interface permettant l'échange d'information entre un humain et l'instrument de mesure ou ses composants matériels ou logiciels, par exemple, des interrupteurs, un clavier, une souris, un afficheur, un écran, une imprimante, un écran tactile, une fenêtre logicielle sur un écran incluant le logiciel l'ayant générée.

3.1.56 Validation [dérivé de ISO/CEI 14598 et CEI 61508-4:1998][7]

Confirmation par l'examen et fourniture de preuves objectives (i.e. informations qui peuvent être démontrées comme vraies, basées sur des faits obtenus lors d'observations, mesurages, essais, etc.) que les exigences particulières pour l'usage spécifique prévu sont respectées. Dans le cas présent, ces exigences sont celles de ce Document.

3.1.57 Vérification [V 1: 2000, 2.13]

Procédure (autre que l'approbation de type) qui inclut l'examen et le marquage et/ou la délivrance d'un certificat de vérification et qui constate et confirme que l'instrument de mesure satisfait aux exigences réglementaires[2)].

3.2 Abréviations

EUT	Equipement soumis à l'essai
CEI	Commission Electrotechnique Internationale
E/S	Entrée / Sortie (se réfère aux ports)
ISO	Organisation Internationale de Normalisation
TIC	Technologies de l'Information et de la Communication
EMT	Erreur Maximale Tolérée
OIML	Organisation Internationale de Métrologie Légale
PCB	Carte de Circuit Imprimé
PIN	Numéro d'Identification Personnel
TC	Comité Technique OIML
SC	Sous-Comité OIML

4 Instructions pour utiliser ce Document lors de la rédaction de Recommandations OIML

4.1 Les dispositions de ce Document s'appliquent uniquement aux nouveaux Documents et Recommandations OIML, ainsi qu'aux Documents et Recommandations en révision. Les TCs et SCs doivent utiliser ce Document afin d'établir les exigences relatives aux logiciels, en complément des exigences techniques et métrologiques de la Recommandation OIML appropriée.

4.2 Tous les documents normatifs sont soumis à révision. Les utilisateurs de ce Document sont donc encouragés à envisager la possibilité d'appliquer la plus récente édition de ces documents normatifs.

4.3 L'objectif de ce Document est de fournir aux TCs ou SCs responsables du développement de Recommandations OIML, des séries d'exigences – certaines avec différents niveaux – qui sont appropriées pour couvrir les besoins de tout type d'instrument de mesure et cela, dans tous les domaines d'application. Les TCs et SCs doivent déterminer quel niveau est approprié pour les besoins de protection, de conformité et d'intensité de validation, et déterminer comment incorporer les parties pertinentes de ce Document dans les Recommandations en cours de rédaction. Le chapitre 8 fournit quelques aides pour accomplir cette tâche.

2) Note : Définition différente des autres Normes, par exemple ISO/CEI 14598, clause 4.23 or CEI 61508-4, clause 3.8.1.

5 Exigences relatives aux logiciels des instruments de mesure

5.1 Exigences générales

Au moment de publier ce Document, ces exigences générales représentent l'état de l'art des technologies de l'information et de la communication (TIC). Elles sont en principe applicables à tous types d'instrument de mesure, dispositifs électroniques, et sous-ensembles contrôlés par logiciel et devraient être considérées dans toutes les Recommandations OIML. Contrairement aux exigences générales, les exigences spécifiques aux configurations (5.2) traitent des fonctionnalités qui ne sont pas courantes pour certains types d'instrument ou certains domaines d'application.

Dans les exemples, lorsque applicables, deux niveaux, normal et élevé, de sévérité sont présentés. Leur notation dans le Document est la suivante :

(I) Solution technique acceptable en cas de niveau normal de sévérité,

(II) Solution technique acceptable en cas de niveau élevé de sévérité (voir 8).

5.1.1 Identification du logiciel

Le logiciel réglementairement pertinent d'un instrument de mesure/dispositif électronique/sous-ensemble doit être clairement identifié avec son numéro de version logiciel ou un autre moyen. L'identification peut être constituée de plus d'une partie mais au moins une d'elles doit être dédiée à l'application légale.

L'identification doit être inextricablement liée au logiciel lui-même et doit être présentée ou imprimée à la demande ou être affichée durant le fonctionnement ou au démarrage des instruments pouvant être éteint et mis en route successivement. Si un sous-ensemble / un dispositif électronique n'a ni afficheur ni imprimante, alors l'identification doit être transmise par le biais d'une interface de communication afin d'être affichée/imprimée par un autre sous-ensemble/dispositif électronique.

A titre d'exception, la sérigraphie de l'identification du logiciel sur l'instrument/dispositif électronique doit être une solution acceptable si les conditions suivantes sont remplies :

(1) L'interface utilisateur ne doit avoir aucune capacité de contrôle pour activer l'indication de l'identification du logiciel sur l'afficheur, ou l'afficheur ne permet pas techniquement la présentation de l'identification du logiciel (dispositif indicateur analogique ou compteur électromécanique).

(2) L'instrument/dispositif électronique ne doit pas avoir d'interface pour communiquer l'identification du logiciel.

(3) Après la production de l'instrument/dispositif électronique, un changement du logiciel n'est pas possible, ou uniquement possible si le matériel ou un composant matériel est également changé.

Le fabricant du matériel, ou du composant matériel concerné, a la responsabilité de s'assurer que l'identification du logiciel est correctement sérigraphiée sur l'instrument/dispositif électronique concerné.

L'identification du logiciel et les moyens d'identification doivent être déclarés dans le certificat d'approbation de type.

Les Recommandations OIML appropriées doivent autoriser ou interdire cette exception.

Note : Chaque instrument de mesure en service doit être conforme au type approuvé. L'identification du logiciel permet aux personnels de surveillance ainsi qu'aux personnes intéressées par le mesurage de déterminer si l'instrument considéré est conforme.

Exemple :

(I) Le logiciel contient une chaîne de texte ou un nombre, identifiant de façon non ambiguë la version installée. Cette chaîne est transférée à l'afficheur de l'instrument quand un bouton est pressé, quand l'instrument est mis en route, ou encore cycliquement contrôlé par une minuterie.

Un numéro de version peut avoir la structure suivante A.Y.Z. Si on considère un dispositif calculateur, la lettre A représentera la version du logiciel coeur, qui compte les impulsions. La lettre Y représentera la version de la fonction de conversion (aucune, à 15 °C, à 20 °C) et la lettre Z représentera la langue de l'interface utilisateur.

(II) Le logiciel calcule une somme de contrôle du code exécutable et présente le résultat en temps qu'identification au lieu de (ou en plus de) la chaîne en (I). L'algorithme de la somme de contrôle doit être un algorithme normalisé. Par exemple un algorithme de type CRC 16 est une solution acceptable pour ce calcul.

La solution (II) est appropriée, si une conformité élevée est requise (voir 5.2.5 (d) et 8).

5.1.2 Adéquation des algorithmes et fonctions

Les algorithmes et fonctions de mesure d'un dispositif électronique doivent être appropriés et fonctionnellement corrects pour le type de dispositif et l'application considérés (exactitude de l'algorithme, calcul de prix conforme à certaines règles, algorithme d'arrondi, etc.).

Le résultat de mesure et les informations l'accompagnant, requises par une Recommandation OIML spécifique ou par la réglementation nationale, doivent être affichés ou imprimés correctement.

Il doit être possible d'examiner les algorithmes et fonctions grâce à des essais métrologiques, des essais logiciels ou un examen du logiciel (tel que décrit en 6.3).

5.1.3 Protection du logiciel

5.1.3.1 Prévention des mauvais usages

Un instrument de mesure doit être construit de telle sorte que les possibilités de mauvais usage non intentionnel, accidentel ou intentionnel soient minimales. Dans le cadre de ce Document OIML, ceci s'applique plus particulièrement au logiciel. La présentation des résultats de mesure doit être sans ambiguïté pour toutes les parties intéressées.

Note : Les instruments contrôlés par logiciel ont souvent des fonctionnalités complexes. L'utilisateur a besoin de bons conseils pour une utilisation correcte et pour obtenir des résultats de mesure corrects.

Exemple :

L'utilisateur est guidé par des menus. Les fonctions réglementairement pertinentes sont combinées dans une branche de ce menu. Si des valeurs de mesure peuvent être perdues lors d'une action, l'utilisateur doit être alerté et requis d'effectuer une autre action avant que la fonction ne soit exécutée. Voir également 5.2.2.

5.1.3.2 Protection contre la fraude

5.1.3.2.a Le logiciel réglementairement pertinent doit être sécurisé contre les modifications non autorisées, les chargements ou les changements par échange de mémoire. En plus des scellements mécaniques, des moyens techniques peuvent être nécessaires pour sécuriser les instruments de mesure ayant un système d'exploitation ou une option de chargement de logiciel.

Note : Lorsque le logiciel est stocké sur une mémoire inviolable (sur laquelle les données sont inaltérables, par exemple une ROM "mémoire en lecture seule" scellée), les besoins en moyens techniques sont réduits en conséquence.

Exemple :

(I)/(II) Le boîtier contenant la mémoire est scellé ou la mémoire est scellée au PCB.

(II) Si un dispositif réinscriptible est utilisé, l'entrée autorisant l'écriture est inhibée par un interrupteur qui peut être scellé. Le circuit est conçu de telle sorte que la protection en écriture ne peut être annulée par un court-circuit des contacts.

(I) Un instrument de mesure est constitué de deux sous-ensembles dont l'un d'eux contenant les principales fonctions métrologiques incorporées dans un boîtier pouvant être scellé. L'autre sous-ensemble est un ordinateur universel avec un système d'exploitation. Certaines fonctions, telle que l'indication, sont localisées dans le logiciel de cet ordinateur. Une manipulation relativement simple – d'autant plus si un protocole normalisé est utilisé pour la communication entre les deux parties du logiciel – pourrait être un échange du logiciel de l'ordinateur universel. Cette manipulation peut être inhibée par un simple moyen cryptographique, par exemple l'encryptage des données transférées entre le sous-ensemble et l'ordinateur universel. La clef de décryptage est cachée dans le programme réglementairement pertinent de l'ordinateur universel. Ce programme est le seul à connaître la clef et est capable de la lire, de décrypter et d'utiliser les valeurs de mesure. Les autres programmes ne peuvent être utilisés à ces fins car ils ne peuvent décrypter les valeurs de mesure (voir également l'exemple en 5.2.1.2.d).

5.1.3.2.b Seules les fonctions clairement documentées (voir 6.1) sont autorisées à être activées par le biais de l'interface utilisateur, qui doit être réalisée de telle manière qu'elle ne facilite pas un usage frauduleux. La présentation des informations doit être conforme avec 5.2.2.

Note : L'examinateur décide si toutes les commandes documentées sont acceptables.

Exemple :

(I)/(II) Toutes les entrées de l'interface utilisateur sont redirigées vers un programme qui filtre les commandes entrantes. Il autorise et ne laisse passer que celles qui sont documentées et rejette toutes les autres. Ce programme ou module logiciel fait partie du logiciel réglementairement pertinent.

5.1.3.2.c Les paramètres qui fixent les caractéristiques réglementairement pertinentes de l'instrument de mesure doivent être sécurisés contre les modifications non autorisées. Si nécessaire, et à des fins de vérification, le parmètrage courant doit pouvoir être affiché ou imprimé.

Note : Les paramètres spécifiques au dispositif peuvent être ajustables ou sélectionnables uniquement dans un mode opérationnel spécifique de l'instrument. Ils peuvent être

classifiés comme ceux devant être sécurisés (inaltérables) ou ceux auxquels une personne autorisée peut accéder (paramètres réglables), par exemple le détenteur ou le vendeur de l'instrument.

Les paramètres spécifiques au type ont une valeur identique pour tous les exemplaires d'un même type. Ils sont fixés lors de l'approbation de type de l'instrument.

Exemple :

(I)/(II) Les paramètres spécifiques au dispositif à sécuriser sont stockés dans une mémoire non volatile. L'entrée autorisant l'écriture de la mémoire est inhibée par un interrupteur qui peut être scellé.

Se référer aux exemples 5.1.3.2.d (1) à (3) de cette section.

5.1.3.2.d La protection du logiciel comprend le scellement par des moyens mécaniques, électroniques et/ou cryptographiques, rendant toute intervention non autorisée impossible ou évidente.

Exemple :

(1) (I) Le scellement électronique : Les paramètres métrologiques d'un instrument peuvent être entrés et ajustés grâce à un élément du menu. Le logiciel reconnaît chaque changement et incrémente un compteur d'évènements pour chaque évènement de ce type. La valeur du compteur d'évènements peut être indiquée. La valeur initiale du compteur d'évènements doit être enregistrée. Si la valeur indiquée diffère de la valeur enregistrée, l'instrument est dans un état non vérifié (équivalent à un scellement brisé).

(2) (I)/(II) Le logiciel de l'instrument de mesure est construit de telle sorte (voir l'exemple 5.1.3.2.a) qu'il n'y a pas de possibilité de modifier les paramètres et la configuration réglementairement pertinente sauf à utiliser un menu protégé par un interrupteur. Cet interrupteur est scellé mécaniquement en position inactive, rendant toute modification des paramètres et de la configuration réglementairement pertinente impossible.

(3) (II) Le logiciel de l'instrument de mesure est construit de telle sorte (voir l'exemple (a)) qu'il n'est pas possible de modifier les paramètres et la configuration réglementairement pertinente sauf pour les personnes autorisées. Si une personne veut entrer dans le menu des paramètres, elle doit insérer sa carte à puce contenant un PIN comme partie d'un certificat cryptographique. Le logiciel de l'instrument est capable de vérifier l'authenticité du PIN avec le certificat et autorise l'accès au menu des paramètres. L'accès est enregistré dans une expertise de l'historique incluant l'identité de la personne (ou au moins la carte à puce utilisée).

Le niveau (II) des exemples de solution technique acceptable est approprié si un niveau élevé de protection contre la fraude est nécessaire (voir 8).

5.1.4 Support des fonctionnalités matérielles

5.1.4.1 Support de la détection de faute

La Recommandation OIML appropriée peut exiger des fonctions de détection de faute pour certaines fautes de l'instrument (traité dans l'OIML D 11 (5.1.2 (b) et 5.3)). Dans ce cas, il doit être exigé que le fabricant de l'instrument conçoive les systèmes de contrôle dans la partie logicielle ou dans la partie

matérielle ou encore donne les moyens par lesquels la partie matérielle peut être assistée par la partie logicielle de l'instrument.

Si le logiciel est impliqué dans la détection de faute, une réaction appropriée est requise. La Recommandation OIML appropriée peut prescrire que l'instrument/dispositif électronique soit désactivé ou qu'une alarme/un enregistrement dans un registre des erreurs soit généré dans le cas où une condition de faute est détectée.

La documentation soumise pour l'approbation de type doit inclure une liste des fautes qui sont détectées par le logiciel ainsi que la réaction attendue et, si nécessaire pour la compréhension, une description de l'algorithme de détection.

Exemple :

(I)/(II) A chaque démarrage, le programme réglementairement pertinent calcule la somme de contrôle du code programme et des paramètres réglementairement pertinents. La valeur nominale de ces sommes de contrôle a été calculée en avance et stockée dans l'instrument. Si les valeurs calculées et stockées ne correspondent pas, l'exécution du programme est arrêtée.

Si le mesurage n'est pas interruptible, la somme de contrôle est calculée cycliquement et contrôlée par une minuterie logicielle. En cas de détection de défaillance, le logiciel affiche un message d'erreur ou allume un indicateur de défaillance et enregistre l'heure du défaut dans un registre des erreurs (s'il en existe un).

Le CRC 16 est un algorithme de somme de contrôle acceptable.

5.1.4.2 Support de la protection de la durabilité

Il appartient au fabricant de choisir de réaliser les systèmes de protection de la durabilité traités dans l'OIML D 11:2004 (5.1.3 (b) et 5.4) de manière logicielle ou matérielle, ou de permettre aux systèmes matériels d'être assistés par logiciel. La Recommandation OIML appropriée peut recommander une solution appropriée.

Si le logiciel est impliqué dans la protection de la durabilité, une réaction appropriée est requise. La Recommandation OIML appropriée peut prescrire que l'instrument/dispositif électronique soit désactivé ou qu'une alarme/enregistrement dans un registre des erreurs, soit généré dans le cas où la durabilité serait détectée comme compromise.

Exemple :

(I)/(II) Certaines sortes d'instrument de mesure requièrent un ajustement après un intervalle de temps prescrit afin de garantir la durabilité des mesures. Le logiciel donne un avertissement lorsque l'intervalle de maintenance s'est écoulé et arrête même de mesurer si celui-ci est dépassé de plus d'une certaine durée.

5.2 Exigences spécifiques aux configurations

Les exigences données dans cette section sont basées sur des solutions techniques typiques pour les TIC. Aussi, elles peuvent ne pas être communes à tous les domaines d'application légale. Outre ces exigences, des solutions techniques possibles, présentant le même degré de sécurité et de conformité au type que les instruments n'étant pas contrôlés par logiciel, sont données.

Les exigences spécifiques suivantes sont nécessaires lorsque certaines technologies sont utilisées dans les systèmes de mesure. Elles doivent être considérées en complément de celles décrites en 5.1

Dans les exemples, lorsque applicable, deux niveaux, normal et élevé, de sévérité sont présentés. Leur notation dans le Document est la suivante :

(I) Solution technique acceptable en cas de niveau normal de sévérité,

(II) Solution technique acceptable en cas de niveau élevé de sévérité (voir 8).

5.2.1 Spécification et séparation des parties pertinentes et spécification des interfaces des parties

Les parties métrologiquement critiques d'un système de mesure – qu'elles soient des parties logicielles ou matérielles – ne doivent pas être inacceptablement influencées par les autres parties du système de mesure.

Cette exigence s'applique si l'instrument de mesure (ou le dispositif électronique, ou le sous-ensemble) a des interfaces pour communiquer avec d'autres dispositifs électroniques, avec l'utilisateur, ou avec d'autres parties logicielles en dehors des parties métrologiquement critiques de l'instrument de mesure (ou du dispositif électronique, ou du sous-ensemble).

5.2.1.1 Séparation des dispositifs électroniques et des sous-ensembles

5.2.1.1.a Les sous-ensembles ou dispositifs électroniques d'un système de mesure qui réalisent des fonctions réglementairement pertinentes, doivent être identifiés, clairement définis et documentés. Ils forment la partie réglementairement pertinente du système de mesure.

Note : L'examinateur décide si cette partie est complète et si d'autres parties du système de mesure peuvent être exclues de toute évaluation supplémentaire.

Exemple :

(1) (I)/(II)Un compteur électrique est équipé d'une interface optique pour connecter un dispositif électronique de lecture des valeurs de mesure. Le compteur stocke toutes les quantités pertinentes et conserve les valeurs disponibles à la lecture pendant une durée suffisante. Dans ce système, seul le compteur électrique est un dispositif réglementairement pertinent. D'autres dispositifs réglementairement non pertinents peuvent exister et peuvent être connectés à l'interface de l'instrument sous réserve que l'exigence 5.2.1.1.b est respectée. La sécurisation de la transmission des données n'est pas exigée (voir 5.2.3).

(2) (I)/(II) Un instrument de mesure est composé des sous-ensembles suivants:

- un capteur numérique calculant le poids ou le volume,
- un ordinateur universel calculant le prix,
- une imprimante qui imprime les valeurs de mesure et le prix à payer.

Tous les sous-ensembles sont connectés à un réseau local. Dans ce cas, le capteur numérique, l'ordinateur universel et l'imprimante sont des sous-ensembles réglementairement pertinents et sont optionnellement connectés à un système de vente qui n'est pas nécessairement réglementairement pertinent. Les sous-ensembles réglementairement pertinents doivent respecter l'exigence 5.2.1.1.b et – à cause de la transmission par le réseau – les exigences de 5.2.3. Il n'y a pas d'exigence sur le système de vente.

5.2.1.1.b Il doit être démontré durant les essais d'approbation que les fonctions et données pertinentes des sous-ensembles et dispositifs électroniques ne peuvent pas être inacceptablement influencées par les commandes reçues via l'interface.

Cela implique qu'il existe une affectation non ambiguë de chaque commande à chaque fonction ou changement de donnée dans le sous-ensemble ou le dispositif électronique.

Note : Se référer à 5.2.3 si les sous-ensembles ou dispositifs réglementairement pertinents interagissent avec d'autres sous-ensembles ou dispositifs électroniques réglementairement pertinents.

Exemple :

(1) (I)/(II) Le logiciel du compteur électrique (voir exemple (1) de 5.2.1.1.a ci-dessus) est capable de recevoir des commandes pour sélectionner les quantités requises. Il combine la valeur de mesure avec des informations additionnelles – par exemple l'horodatage, l'unité – et émet ce jeu de données vers le dispositif requerrant. Le logiciel accepte uniquement les commandes de sélection de quantités valides et autorisées et rejette toute autre commande, renvoyant uniquement un message d'erreur. Le contenu du jeu de données peut être sécurisé mais ces moyens de sécurisation ne sont pas requis puisque le jeu de données transmis n'est pas soumis au contrôle légal.

(2) (I)/(II) A l'intérieur du boîtier, qui peut être scellé, se trouve un interrupteur qui définit le mode opératoire du compteur électrique : une position de l'interrupteur indique le mode vérifié, l'autre le mode non-vérifié (des moyens de sécurisation autres qu'un scellement mécanique sont possibles, voir les exemples en 5.1.3.2.a/d). Lors de l'interprétation des commandes reçues, le logiciel vérifie la position de l'interrupteur : dans la position mode non-vérifié, le jeu de commande que le logiciel accepte est étendu par rapport au mode décrit ci-dessus. Par exemple, il est possible d'ajuster le facteur d'étalonnage par une commande qui est rejetée dans le mode vérifié.

5.2.1.2 Séparation des parties logicielles

Les TCs et SCs OIML peuvent spécifier dans la Recommandation appropriée que le logiciel/le matériel/ les données ou qu'une partie du logiciel/du matériel/des données est réglementairement pertinent.

La réglementation nationale peut prescrire qu'un logiciel/un matériel/des données ou qu'une partie du logiciel/du matériel/des donnée spécifique est réglementairement pertinent.

5.2.1.2.a Tous les modules logiciels (programmes, sous-programmes, objets, etc.) qui réalisent des fonctions réglementairement pertinentes ou qui contiennent des domaines de données réglementairement pertinents forment la partie logicielle réglementairement pertinente d'un instrument de mesure (dispositif électronique ou sous-ensemble). L'exigence de conformité s'applique à cette partie (voir 5.2.5) qui doit être identifiable suivant les prescriptions de 5.1.1.

Si la séparation du logiciel n'est pas possible ou si elle n'est pas nécessaire, le logiciel tout entier est considéré comme réglementairement pertinent.

Exemple :

(I) un système de mesure est constitué de plusieurs capteurs numériques connectés à un ordinateur personnel qui affiche les valeurs de mesure. Le logiciel réglementairement pertinent de l'ordinateur personnel est séparé de la partie réglementairement non pertinente

en compilant toutes les procédures réalisant des fonctions réglementairement pertinentes dans une bibliothèque de liens dynamiques. Une ou plusieurs applications réglementairement non pertinentes peuvent appeler les procédures de cette bibliothèque. Ces procédures reçoivent les données de mesure des capteurs numériques, calculent les résultats de mesure, et les affichent dans une fenêtre logicielle. Lorsque les fonctions réglementairement pertinentes sont terminées, le contrôle est rendu à l'application réglementairement non pertinente.

5.2.1.2.b Si la partie logicielle réglementairement pertinente communique avec d'autres parties, une interface logicielle doit être définie. Toute communication doit être exclusivement réalisée via cette interface. La partie logicielle réglementairement pertinente ainsi que l'interface doivent être clairement documentées. Toute fonction et domaine réglementairement pertinent du logiciel doivent être décrits pour permettre à l'autorité d'approbation de type de décider si la séparation logicielle est correcte ou non.

L'interface est constituée de codes programmes et de domaines de données dédiés. Les commandes définies et codées, ainsi que les données, sont échangées entre les parties logicielles grâce au stockage dans le domaine de données dédié par une partie logicielle et à la lecture par une autre partie logicielle. Les codes programmes de lecture et d'écriture font partie de l'interface logicielle. Le domaine de données formant l'interface logicielle, y compris le code qui exporte depuis la partie réglementairement pertinente vers l'interface du domaine de données, ainsi que le code qui importe depuis l'interface vers la partie réglementairement pertinente, doit être clairement défini et documenté. L'interface logicielle déclarée ne doit pas être contournée.

Le fabricant est responsable du respect de ces contraintes. Il n'est pas possible d'empêcher un programme de contourner l'interface ou d'empêcher la programmation de commandes cachées avec des moyens techniques (tel que le scellement). Des instructions concernant ces exigences doivent être données, par le fabricant, au programmeur de la partie logicielle réglementairement pertinente aussi bien qu'au programmeur de la partie réglementairement non pertinente.

5.2.1.2.c L'affectation de chaque commande doit être sans ambiguïté pour toutes fonctions initiées ou tous changements de données dans la partie réglementairement pertinente du logiciel. Les commandes qui communiquent à travers l'interface logicielle doivent être déclarées et documentées. Seules les commandes documentées sont autorisées à être activées à travers l'interface logicielle. Le fabricant doit déclarer l'exhaustivité de la documentation relative aux commandes.

Exemple :

(I) Dans l'exemple décrit en 5.2.1.2.a, l'interface logicielle est réalisée par les paramètres et les valeurs retournées par la procédure de la bibliothèque. Aucun pointeur du domaine de données à l'intérieur de la bibliothèque n'est retourné. La définition de l'interface est fixée dans la bibliothèque réglementairement pertinente compilée et ne peut être changée par une quelconque application. Il n'est pas impossible de contourner directement l'interface logicielle ainsi que les adresses des domaines de données de la bibliothèque, mais ce n'est pas une bonne pratique de la programmation. C'est plutôt compliqué et peut être considéré comme du piratage.

5.2.1.2.d Lorsque le logiciel réglementairement pertinent est séparé du logiciel réglementairement non pertinent, le logiciel réglementairement pertinent doit avoir priorité dans l'utilisation des ressources sur le logiciel réglementairement non pertinent. Le travail de mesure (réalisé par la partie logicielle réglementairement pertinente) ne doit pas être retardé ou bloqué par une autre tâche.

Le fabricant est responsable du respect de ces contraintes. Des moyens techniques doivent être prévus afin d'empêcher la perturbation des fonctions réglementairement pertinentes par un programme réglementairement non pertinent. Des instructions concernant ces exigences devraient être données, par le fabricant, au programmeur de la partie logicielle réglementairement pertinente aussi bien qu'au programmeur de la partie réglementairement non pertinente.

Exemples :

(1) (I) Dans les exemples 5.2.1.2.a/c l'application réglementairement non pertinente contrôle le démarrage des procédures réglementairement pertinentes dans la bibliothèque. Omettre un appel à ces procédures résulterait évidement en une inhibition de la fonction réglementairement pertinente du système. Aussi les dispositions suivantes ont été prises dans le système en exemple afin de respecter les exigences de 5.2.1.2.d. Les capteurs numériques émettent les données de mesure sous une forme cryptée. La clef de décryptage est cachée dans la bibliothèque. Seules les procédures de la bibliothèque connaissent la clef et sont capables de lire, décrypter et afficher les valeurs de mesure. Si le programmeur de l'application veut lire et traiter les valeurs de mesure, il est forcé d'utiliser les procédures réglementairement pertinentes de la bibliothèque qui réalisent toutes les fonctions exigées légalement comme effet secondaire de leur appel. La bibliothèque contient les procédures qui exportent les valeurs de mesure décryptées permettant au programmeur de l'application de les utiliser pour ses propres besoins après que le traitement réglementairement pertinent ait été terminé.

(2) (I)/(II) Le logiciel d'un compteur électrique électronique lit les valeurs brutes de mesure depuis un convertisseur analogique/numérique (CAN). Pour un calcul correct des valeurs de mesure, le retard entre les événements "données disponibles" du CAN pour finir la mise en mémoire tampon des valeurs de mesure est crucial. Les valeurs brutes sont lues par une routine d'interruption initiée par le signal "données disponibles". L'instrument est capable de communiquer en parallèle, via une interface, avec d'autres dispositifs électroniques servis par une autre routine d'interruption (communication réglementairement non pertinente). Il résulte de l'interprétation des exigences de 5.2.1.2, pour une telle configuration, que la priorité de la routine d'interruption pour le traitement des valeurs de mesure doit être plus élevée que celle de la routine de communication.

Les exemples de 5.2.1.2.a à 5.2.1.2.c et 5.2.1.2.d (1) sont des solutions techniques acceptables uniquement pour un niveau de sévérité (I). Si un niveau élevé de protection contre la fraude ou de conformité est nécessaire (voir 8), la seule séparation logicielle n'est pas suffisante. Des moyens additionnels sont nécessaires ou le logiciel tout entier doit être considéré comme étant sous contrôle légal.

5.2.2 Indications partagées

Un afficheur ou une imprimante peuvent être utilisés pour présenter les informations de la partie logicielle réglementairement pertinente et d'autres informations. Le contenu et l'agencement sont spécifiques à la nature de l'instrument et au domaine d'application et doivent être définis dans la Recommandation appropriée. Cependant, si l'indication est réalisée en utilisant une interface utilisateur multi fenêtrée, l'exigence suivante s'applique :

Le logiciel qui réalise l'indication des valeurs de mesure et d'autres informations réglementairement pertinentes appartient à la partie réglementairement pertinente. La fenêtre contenant ces données doit avoir la plus haute priorité, i.e. elle ne doit pas pouvoir être effacée par un autre logiciel ou être chevauchée par des fenêtres générées par d'autres logiciels ou être réduite ou être rendue invisible tant

que la mesure est en cours et que les résultats présentés sont nécessaires aux besoins réglementairement pertinents.

Exemple :

(I) Dans un système tel que celui décrit aux exemples de 5.2.1.2.a à 5.2.1.2.d, les valeurs de mesure sont affichées dans une fenêtre logicielle séparée. Les moyens décrits en 5.2.1.2.d garantissent que seule la partie de programme réglementairement pertinente peut lire les valeurs de mesure. Pour un système d'exploitation avec une interface utilisateur multi fenêtrée, un moyen technique additionnel est utilisé pour respecter l'exigence 5.2.2 : la fenêtre affichant les données réglementairement pertinentes est générée et contrôlée par des procédures de la bibliothèque de liens dynamiques réglementairement pertinente (voir 5.2.1.2). Durant les mesures, ces procédures vérifient cycliquement que la fenêtre appropriée est toujours au dessus des autres fenêtres ouvertes ; si ce n'est pas le cas, elle la place au dessus.

Si un niveau élevé de protection contre la fraude est nécessaire (II), une simple impression comme indication n'est pas appropriée. Il doit exister un sous-ensemble ayant des moyens de sécurisation élevés qui soit capable d'afficher les valeurs de mesure.

L'utilisation d'un ordinateur universel en temps que partie d'un instrument de mesure n'est pas appropriée si un niveau élevé de protection est nécessaire (II). Des précautions additionnelles pour empêcher ou minimiser le risque de fraude, sous forme logicielle ou matérielle, doivent être envisagées lorsqu'une protection élevée est nécessaire, tout comme lors de l'utilisation d'un ordinateur universel (par exemple PC, PDA, etc.).

5.2.3 Stockage des données, transmission par systèmes de communication

Si les valeurs de mesure sont utilisées en un autre lieu que celui du mesurage ou en d'autres temps que ceux du mesurage, il se peut qu'elles aient à quitter l'instrument (dispositif électronique, sous-ensemble) et soient stockées ou transmises dans un environnement non sûr avant d'être utilisées pour des applications légales. Dans un tel cas, les exigences suivantes s'appliquent :

5.2.3.1 Les valeurs de mesure stockées ou transmises doivent être accompagnées de toutes les informations pertinentes nécessaires à l'usage réglementairement pertinent futur.

Exemple :

(I)/(II) Un jeu de données peut inclure les entrées suivantes:

- la valeur de mesure incluant son unité,
- l'horodatage du mesurage (voir 5.2.3.7),
- le lieu du mesurage ou l'identification de l'instrument de mesure utilisé pour le mesurage,
- l'identification sans ambiguïté du mesurage, par exemple une série de nombres permettant l'affectation des valeurs imprimées sur une facture.

5.2.3.2 Les données doivent être protégées par des moyens logiciels afin de garantir leur authenticité, leur intégrité et, si nécessaire, l'exactitude des informations relatives à l'heure du mesurage. Le logiciel qui affiche ou qui traite ultérieurement les valeurs de mesure et les données les accompagnant doit vérifier l'heure du mesurage, l'authenticité et l'intégrité des données après les

avoir lues depuis un stockage non sûr ou après les avoir reçues par un canal de transmission non sûr. Si une irrégularité est détectée, les données doivent être rejetées ou marquées inutilisables.

Les modules logiciels qui préparent les données pour l'émission ou le stockage, ou qui vérifient les données à leur lecture ou réception, appartiennent à la partie logicielle réglementairement pertinente.

Note : Il est approprié d'exiger un niveau plus élevé de sévérité lorsque l'on considère un réseau ouvert.

Exemple :

(I) Le programme du dispositif émetteur calcule une somme de contrôle du jeu de données (un algorithme tel que BCC, CRC 16, CRC 32, etc.) et le joint au jeu de données. Il utilise une valeur initiale secrète pour ce calcul au lieu d'utiliser la valeur donnée dans la norme. Cette valeur initiale est utilisée en tant que clef et est stockée comme constante dans le code programme. Le programme de réception, ou de lecture, calcule la somme de contrôle et la compare avec celle stockée dans le jeu de données. Si les deux valeurs correspondent, le jeu de données n'est pas falsifié. Sinon, le programme présume la falsification et rejette le jeu de données.

5.2.3.3 Pour un niveau élevé de protection, il est nécessaire d'utiliser des méthodes cryptographiques. Les clés confidentielles employées pour cela doivent être gardées secrètes et sécurisées dans les instruments de mesure, dispositifs électroniques, ou sous-ensembles impliqués. Des moyens doivent être fournis de sorte que ces clés ne puissent être introduites ou lues que si un scellement est brisé.

Exemple :

(II) Le programme de stockage ou d'émission génère une "signature numérique" en commençant par le calcul de la valeur de hachage[3)] puis encrypte celle-ci avec la clef secrète d'un système de clef publique[4)]. Le résultat est la signature. Elle est jointe au jeu de données transmis ou stocké. Le récepteur calcule également la valeur de hachage du jeu de données et décrypte avec la clef publique la signature jointe au jeu de données. La valeur calculée et la valeur décryptée de la valeur de hachage sont comparées. Si elles sont égales, le jeu de données n'est pas falsifié (l'intégrité est prouvée). Pour prouver l'origine du jeu de données, le récepteur doit connaître si la clef publique appartient à l'émetteur, i.e. le dispositif émetteur. Aussi, la clef publique est affichée sur l'afficheur de l'instrument de mesure et peut être enregistrée une fois, par exemple avec le numéro de série du dispositif quand il est légalement contrôlé en service. Si le récepteur est sûr qu'il a utilisé la bonne clef publique pour décrypter la signature, alors l'authenticité du jeu de données est également prouvée.

5.2.3.4 Stockage automatique

5.2.3.4.a Lorsque, étant donnée l'application, le stockage des données est requis, les données de mesure doivent être stockées automatiquement lorsque le mesurage est conclu, i.e. lorsque la valeur finale utilisée pour l'application légale a été générée.

3) Algorithmes acceptables: SHA-1, MD5, RipeMD160, ou équivalent.

4) Algorithmes acceptables: RSA (avec une clef de 1024 bit), Elliptic Curves (avec une clef de 160 bit), ou équivalent.

Le dispositif de stockage doit avoir une stabilité suffisante pour garantir que les données ne sont pas corrompues dans des conditions normales de stockage. La capacité de stockage doit être suffisante pour toute application particulière.

Lorsque la valeur finale utilisée pour l'application légale résulte d'un calcul, toutes les données nécessaires au calcul doivent être automatiquement stockées avec la valeur finale.

Note : Les valeurs de mesurages cumulatifs tels que, par exemple, l'énergie électrique ou un volume de gaz, doivent être actualisées constamment. Comme le même domaine de données (variable du programme) est toujours utilisé, les exigences concernant la capacité de stockage ne sont pas applicables aux mesurages cumulatifs.

5.2.3.4.b Les données stockées peuvent être effacées si :

- la transaction est conclue,
- ces données sont imprimées par une imprimante soumise au contrôle légal.

Note : D'autres réglementations nationales générales (par exemple relatives aux taxes) peuvent inclure des limites strictes pour l'effacement des données de mesure stockées.

5.2.3.4.c Lorsque les exigences de 5.2.3.4.b sont remplies et lorsque le stockage est plein, l'effacement de données mémorisées est autorisé lorsque les deux conditions suivantes sont remplies :

- les données sont effacées dans le même ordre que l'ordre d'enregistrement et les règles établies pour l'application particulière sont respectées,
- l'effacement est effectué automatiquement ou après une opération manuelle particulière.

Note : L'utilisation de droits d'accès additionnels devrait être considéré lors de la mise en œuvre de "l'opération manuelle particulière" prescrite au second alinéa ci-dessus.

5.2.3.5 Retard de transmission

Les mesures ne doivent pas être influencées inacceptablement par un retard de transmission.

5.2.3.6 Interruption de transmission

Si le service réseau devient indisponible, aucune donnée de mesure ne doit être perdue. Le processus de mesure doit être stoppé pour éviter la perte de ces données de mesure.

Note : La distinction entre les mesurages statiques et dynamiques doit être étudiée.

Exemple :

(I)/(II) Le dispositif émetteur attend que le récepteur envoie une confirmation de bonne réception du jeu de données. Le dispositif émetteur conserve le jeu de données dans une mémoire tampon tant que la confirmation n'a pas été reçue. La mémoire tampon peut avoir une capacité supérieure à un jeu de données, organisée comme une pile FIFO [5)].

[5)] FIFO : Premier entré – premier sorti

5.2.3.7 Horodatage

L'horodatage doit être lu depuis l'horloge du dispositif. Selon la nature de l'instrument, ou le domaine d'application, régler l'horloge peut être réglementairement pertinent et nécessiter que des moyens de protection appropriés soient pris en accord avec le niveau de sévérité devant être appliqué (voir 5.1.3.2.c).

L'horloge interne d'un instrument autonome tend à avoir une grande incertitude car il n'existe pas de possibilité de la synchroniser avec l'horloge mondiale. Cependant, si l'information en rapport avec l'heure de mesurage est nécessaire à un domaine d'application spécifique, la fiabilité de l'horloge interne de l'instrument doit être renforcée à l'aide de moyens spécifiques.

Exemple :

(II) La fiabilité du dispositif horloge interne de l'instrument de mesure, contrôlée par quartz, est renforcée par redondance : une minuterie est incrémentée par l'horloge du microcontrôleur qui découle d'un autre cristal de quartz. Lorsque que la valeur de la minuterie atteint une valeur prédéfinie, par exemple 1 seconde, un drapeau spécifique du microcontrôleur est dressé et une routine d'interruption du programme incrémente un second compteur. A la fin de, par exemple, une journée, le logiciel lit le dispositif horloge contrôlée par quartz et calcule la différence avec le second compteur logiciel. Si la différence est comprise dans les limites prédéfinies, le compteur logiciel est remis à zéro et la procédure est répétée. Mais si la différence excède les limites, le logiciel réagit de façon appropriée à l'erreur.

5.2.4 Compatibilité des systèmes d'exploitation et du matériel, portabilité

5.2.4.1 Le fabricant doit identifier l'environnement matériel et logiciel qui est approprié. Les ressources minimales ainsi que la configuration adaptée (par exemple le processeur, la mémoire vive, le disque dur, les communications spécifiques, la version du système d'exploitation, etc.) qui sont nécessaires au bon fonctionnement, doivent être déclarées par le fabricant et énoncées dans le certificat d'approbation de type.

5.2.4.2 Des moyens techniques doivent être inclus dans le logiciel réglementairement pertinent afin d'empêcher toute opération si les exigences de configuration minimale ne sont pas respectées. Le système doit uniquement opérer dans l'environnement spécifié par le fabricant pour son bon fonctionnement.

Par exemple, dans le cas où un environnement invariable est spécifié pour un fonctionnement correct du système, des dispositions doivent être prises afin de maintenir fixe l'environnement opérationnel. Ceci s'applique plus particulièrement aux ordinateurs universels réalisant des fonctions réglementairement pertinentes.

Figer le matériel, le système d'exploitation, ou la configuration du système d'un ordinateur universel ou même exclure l'utilisation d'ordinateur universel standard, doit être considéré dans les cas suivants :

- si une conformité élevée est exigée (voir 5.2.5.d),
- si un logiciel figé est exigé (par exemple 5.2.6.3.b pour la Mise à jour Tracée du logiciel),
- si des algorithmes ou clés cryptographiques sont mis en œuvre (voir 5.2.3).

5.2.5 Conformité du dispositif fabriqué au type approuvé

Le fabricant doit produire des dispositifs et des logiciels réglementairement pertinents conformes au type approuvé et à la documentation soumise. Il existe différents niveaux de conformité exigibles :

(a) identité des *fonctions réglementairement pertinentes* de chaque dispositif décrites dans la documentation (6.1), avec celles du type (le code exécutable pouvant être différent),

(b) identité des *parties du code source réglementairement pertinent*, alors que le reste du logiciel réglementairement pertinent est conforme à (a),

(c) identité de tout le *code source réglementairement pertinent*, et

(d) identité de tout le *code exécutable*.

La Recommandation appropriée doit spécifier quel degré de conformité est adapté. Cette Recommandation peut également définir des sous-niveaux de ces degrés de conformité.

A l'exception de (d), il peut exister une partie logicielle sans exigence de conformité, si elle est séparée de la partie réglementairement pertinente conformément à 5.2.1.2.

Les moyens décrits en 5.1.1 et 5.2.1 doivent être fournis afin de rendre la conformité évidente.

Note : (a) et (b) doivent être appliqués pour les niveaux normaux de sévérité et (c) et (d) doivent être appliqués aux niveaux élevés de sévérité.

5.2.6 Maintenance et re-configuration

Mettre à jour le logiciel réglementairement pertinent d'un instrument de mesure en service doit être considéré comme :

- une modification de l'instrument de mesure, lors de l'échange du logiciel par une autre version approuvée,
- une réparation de l'instrument de mesure, lors de la réinstallation de la même version.

Un instrument de mesure qui a été modifié ou réparé alors qu'il est en service, peut nécessiter une vérification primitive ou une vérification ultérieure, selon les réglementations nationales.

Le logiciel qui n'est pas nécessaire au bon fonctionnement de l'instrument de mesure, ne nécessite pas de vérification après avoir été mis à jour.

5.2.6.1 L'utilisation des seules versions du logiciel réglementairement pertinent qui sont conformes au type approuvé est autorisée (voir 5.2.5). L'applicabilité des exigences suivantes dépend de la nature de l'instrument et doit être définie dans la Recommandation OIML appropriée. Elle peut différer également selon la nature de l'instrument considéré. Les options suivantes, 5.2.6.2 et 5.2.6.3, sont des alternatives équivalentes. Cette question concerne le contrôle en service. Se référer au chapitre 7 pour des contraintes additionnelles.

5.2.6.2 Mise à jour Vérifiée

Le logiciel à mettre à jour peut être chargé localement, i.e. directement sur le dispositif mesureur ou à distance via un réseau. Le chargement et l'installation peuvent être deux étapes différentes (tel que décrit en fig. 1) ou combinées en une, selon les besoins de la solution technique. Une personne doit être sur le site d'installation de l'instrument de mesure afin de vérifier l'efficacité de la mise à jour. Après la mise à jour du logiciel réglementairement pertinent de l'instrument de mesure (échange avec

une autre version approuvée ou réinstallation), l'instrument n'est pas autorisé à être employé à des fins légales avant qu'une vérification de celui-ci, telle que décrite en chapitre 7, n'ait été réalisée et que les moyens de sécurisation aient été renouvelés (s'il n'est pas déclaré autrement dans la Recommandation OIML appropriée ou dans le certificat d'approbation).

5.2.6.3 Mise à jour Tracée

Le logiciel est implémenté dans l'instrument conformément aux exigences de la Mise à jour Tracée (5.2.6.3.a à 5.2.6.3.g), si cela est conforme à la Recommandation OIML appropriée. La Mise à jour Tracée est la procédure de changement de logiciel d'un instrument ou d'un dispositif vérifié, après laquelle une vérification sur site par une personne responsable n'est pas nécessaire. Le logiciel à mettre à jour peut être chargé localement, i.e. directement sur le dispositif mesureur ou à distance via un réseau. La mise à jour du logiciel est enregistrée dans une expertise de l'historique (voir 3.1.2). La procédure de Mise à jour Tracée comprend plusieurs étapes : le chargement, la vérification de l'intégrité, la vérification de l'origine (authentification), l'installation, l'enregistrement et l'activation.

5.2.6.3.a La Mise à jour Tracée de logiciel doit être automatique. A l'achèvement de la procédure de mise à jour, l'environnement de protection logicielle doit être du même niveau que celui requis par l'approbation de type.

5.2.6.3.b L'instrument de mesure cible (dispositif électronique, sous-ensemble) doit avoir un logiciel réglementairement pertinent figé qui ne peut pas être mis à jour et qui contient toutes les fonctions de vérification nécessaires au respect des exigences de la Mise à jour Tracée.

5.2.6.3.c Des moyens techniques doivent être utilisés afin de garantir l'authenticité du logiciel chargé, i.e. qu'il provient du détenteur du certificat d'approbation de type. Si le logiciel chargé échoue à la vérification d'authenticité, l'instrument doit le rejeter et utiliser la version précédente du logiciel ou basculer dans un mode inopérant.

Exemple :

> (II) La vérification de l'authenticité est accomplie par des moyens cryptographiques tel qu'un système à clef publique. Le détenteur du certificat d'approbation de type (en général, le fabricant de l'instrument de mesure) génère une signature électronique du logiciel de mise à jour en utilisant la clef secrète, en usine. La clef publique est stockée dans la partie logicielle figée de l'instrument de mesure. La signature est vérifiée en utilisant la clef publique lors du chargement du logiciel dans l'instrument de mesure. Si la signature du logiciel chargé est OK, alors il est installé et activé. Si la vérification échoue, le logiciel figé rejette alors le logiciel chargé et utilise la version précédente du logiciel ou bascule dans un mode inopérant.

5.2.6.3.d Des moyens techniques doivent être utilisés afin d'assurer l'intégrité du logiciel chargé, i.e. qu'il n'a pas été changé de façon inacceptable avant son chargement. Ceci peut être accompli en ajoutant une somme de contrôle ou un code de hachage au logiciel chargé qui seront vérifiés lors de la procédure de chargement. Si le logiciel chargé échoue à cet essai, l'instrument doit le rejeter et utiliser la version précédente du logiciel ou basculer dans un mode inopérant. Dans ce mode, les fonctions de mesure sont inhibées. Seule la reprise de la procédure de téléchargement doit être possible, sans oublier aucune étape du diagramme de Mise à jour Tracée.

5.2.6.3.e Des moyens techniques appropriés, par exemple une expertise de l'historique, doivent être employés afin d'assurer que les Mises à jour Tracées de logiciels réglementairement pertinents sont adéquatement traçables dans l'instrument en vue des vérifications ultérieures, des surveillances ou des inspections.

L'expertise de l'historique doit contenir au minimum les informations suivantes : succès/échec de la procédure de mise à jour, l'identification de la version du logiciel installé, l'identification de la version du logiciel précédemment installé, l'horodatage de l'évènement, et l'identification des parties ayant effectué le téléchargement. Une entrée est générée pour chaque tentative de mise à jour indépendamment de son succès.

Le dispositif de stockage utilisé pour la Mise à jour Tracée doit avoir une capacité suffisante pour assurer au minimum la traçabilité des Mises à jour Tracées du logiciel réglementairement pertinent entre deux vérifications en service ou inspections successives. Il doit être garanti par des moyens techniques que tout téléchargement est impossible sans briser de scellement, lorsque la limite de stockage de l'expertise de l'historique est atteinte.

Note : Cette exigence permet aux autorités d'inspection, qui sont responsables de la surveillance métrologique des instruments légalement contrôlés, de retracer les Mises à jour Tracées du logiciel réglementairement pertinent sur une durée appropriée (en fonction de la réglementation nationale).

5.2.6.3.f En fonction des besoins et de la réglementation nationale, il peut être nécessaire que l'utilisateur ou que le détenteur de l'instrument de mesure ait à donner son consentement au téléchargement. L'instrument de mesure doit avoir un dispositif/sous-ensemble électronique permettant à l'utilisateur ou au détenteur d'exprimer son consentement, par exemple, un bouton poussoir, avant que le téléchargement ne commence. Il doit être possible d'activer/de désactiver ce dispositif/sous-ensemble électronique, par exemple à l'aide d'un interrupteur qui peut être scellé, ou à l'aide d'un paramètre. Si le dispositif/sous-ensemble électronique est activé, chaque téléchargement doit être initié par l'utilisateur ou le détenteur. Si il est désactivé, aucune action de la part de l'utilisateur ou le détenteur n'est nécessaire pour réaliser le téléchargement.

5.2.6.3.g Si les exigences de 5.2.6.3.a à 5.2.6.3.f ne peuvent être remplies, il demeure cependant possible de mettre à jour la partie logicielle réglementairement non pertinente. Dans ce cas, les exigences suivantes doivent être respectées :

- il existe une claire séparation entre le logiciel réglementairement pertinent et le logiciel réglementairement non pertinent, conformément à 5.2.1,
- le logiciel réglementairement pertinent tout entier ne peut être mis à jour sans briser de scellement,
- il est déclaré dans le certificat d'approbation de type que la mise à jour du logiciel réglementairement non pertinent est acceptable.

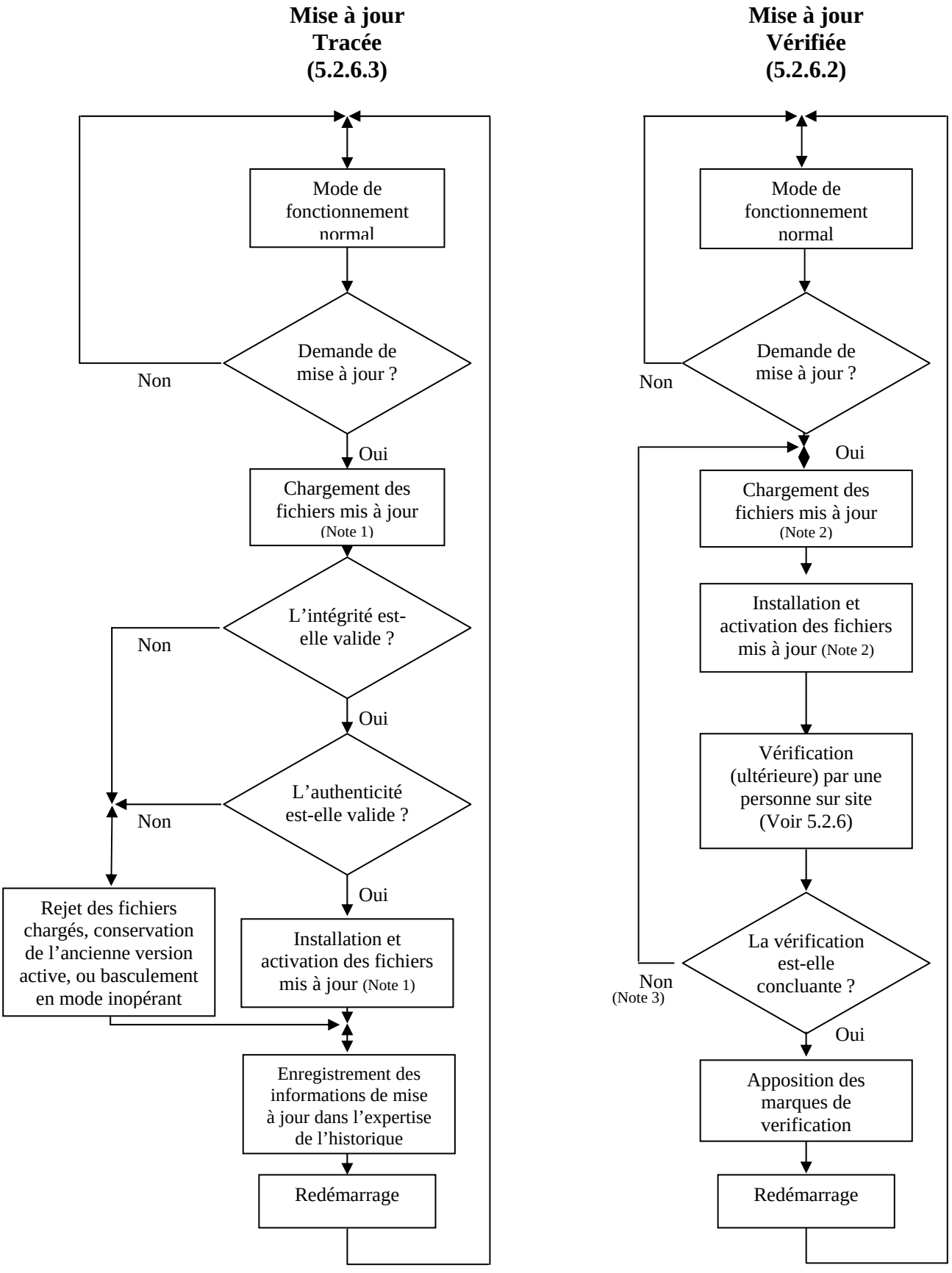

Figure 1 Procédure de mise à jour du logiciel

Notes : (1)Dans le cas de la Mise à jour Tracée, la mise à jour est divisée en deux étapes : le “chargement” et “l’installation/activation”. Cela implique que le logiciel est temporairement stocké après son chargement sans être activé car il doit être possible de rejeter le logiciel chargé et de revenir à la version antérieure, si les vérifications échouent.

(2)Dans le cas d’une Mise à jour Vérifiée, le logiciel peut également être chargé et temporairement stocké avant son installation, mais en fonction de la solution technique, le chargement et l’installation peuvent être accomplis en une étape.

(3) Ici, les échecs de vérification dus à la mise à jour du logiciel sont les seuls considérés. Les échecs dus à d’autres raisons ne nécessitent pas de re-chargement ni de réinstallation du logiciel, symbolisés ici par la branche "Non".

5.2.6.4 La Recommandation OIML appropriée peut exiger que le réglage de certains paramètres spécifiques au dispositif soit disponible pour l’utilisateur. Dans un tel cas, l’instrument de mesure doit être pourvu d’un système enregistrant automatiquement, et de manière non effaçable, tout ajustement de paramètre spécifique au dispositif, par exemple une expertise de l’historique. L’instrument doit être capable de présenter les données enregistrées.

Note : Un compteur d’évènements n’est pas une solution acceptable.

5.2.6.5 Les moyens de traçabilité et les enregistrements font partie du logiciel réglementairement pertinent et devraient être protégés en tant que tels. Le logiciel utilisé pour afficher l’expertise de l’historique (5.2.6.2 ; 5.2.6.3) fait partie du logiciel réglementairement pertinent figé.

6 Approbation de type

6.1 Documentation à soumettre pour l’approbation de type

Pour l’approbation de type, le fabricant de l’instrument de mesure doit déclarer et documenter toutes les fonctions du programme, les structures de données pertinentes ainsi que les interfaces logicielles de la partie réglementairement pertinente qui sont mises en œuvre dans l’instrument. Il ne doit pas exister de fonction cachée non documentée.

Les commandes et leurs effets doivent être complètement décrits dans la documentation du logiciel à soumettre à l’approbation de type. Le fabricant doit déclarer l’exhaustivité de la documentation des commandes. Si les commandes peuvent être entrées via l’interface utilisateur, elles doivent être décrites complètement dans la documentation du logiciel à soumettre à l’approbation de type.

De plus, la demande d’approbation de type doit être accompagnée par un document ou tout autre preuve supportant l’hypothèse que la conception et les caractéristiques du logiciel de l’instrument de mesure sont conformes avec les exigences de la Recommandation OIML appropriée dans laquelle les exigences générales de ce document auront été incorporées.

6.1.1 Une documentation typique (pour chaque instrument de mesure, dispositif électronique, ou sous-ensemble) inclut :

- une description du logiciel réglementairement pertinent et de la façon dont les exigences sont respectées :

  - une liste des modules logiciels qui appartiennent à la partie réglementairement pertinente (Annexe B), y compris une déclaration que toutes les fonctions réglementairement pertinentes sont incluses dans la description,
  - une description des interfaces logicielles de la partie réglementairement pertinente et des commandes et données qui transitent par ces interfaces ainsi qu'une déclaration de leur exhaustivité (Annexe B),
  - une description de la génération de l'identification du logiciel,
  - en fonction de la méthode de validation choisie dans la Recommandation OIML appropriée (voir 6.3 et 6.4), le code source doit être rendu disponible à l'autorité d'essai si une conformité élevée ou une forte protection est requise par la Recommandation OIML appropriée,
  - une liste des paramètres devant être protégés et une description des moyens de protection,

- une description de la configuration adéquate du système ainsi que des ressources minimales exigées (voir 5.2.4),
- une description des moyens de sécurité du système d'exploitation (mot de passe, etc., si applicable),
- une description des méthodes de scellement (logiciel),
- une description du système matériel, par exemple des diagrammes topologiques, le type d'ordinateur(s), le type de réseau, etc. Il doit également être identifié lorsque qu'un composant matériel est estimé réglementairement pertinent ou lorsqu'il réalise des fonctions réglementairement pertinentes,
- une description de l'exactitude des algorithmes (par exemple le filtrage du résultat d'une conversion A/N, le calcul de prix, les algorithme d'arrondi, etc.),
- une description de l'interface utilisateur, des menus et des boîtes de dialogue,
- l'identification du logiciel et les instructions pour l'obtenir d'un instrument en cours d'utilisation,
- la liste des commandes de chaque interface matériel de l'instrument de mesure, du dispositif électronique / sous-ensemble, y compris une déclaration de son exhaustivité,
- la liste des erreurs de durabilité qui sont détectées par le logiciel et si nécessaire pour leur compréhension, une description des algorithmes de détection,
- une description des jeux de donnés stockés ou transmis,
- si la détection de faute est réalisée par logiciel, une liste des fautes qui sont détectées et une description de l'algorithme de détection,
- le manuel d'utilisation.

6.2 Exigences pour la procédure d'approbation

Dans le cadre de l'approbation de type, les procédures d'essais, par exemple celles décrites dans l'OIML D 11:2004, sont basées sur des configurations et conditions d'essai bien définies et reposent sur des mesures comparatives déterminées. "Essayer" et "valider" un logiciel sont deux activités différentes. L'exactitude ou la justesse d'un logiciel en général, ne peut être mesuré au sens métrologique, bien qu'il existe des normes prescrivant comment "mesurer" la qualité d'un logiciel (par exemple l'ISO/CEI 14598 [9]). Les procédures décrites ici prennent en compte les besoins de la métrologie légale ainsi que les méthodes bien connues de validation et d'essais d'ingénierie logicielle,

bien que ces dernières n'aient pas les mêmes buts (par exemple les développeurs de logiciels cherchent les erreurs mais également à optimiser leurs performances). Telle que présentée en 6.4, chaque exigence logicielle a besoin d'une adaptation individuelle des procédures de validation appropriées. L'effort consacré à la procédure devrait refléter l'importance de l'exigence en terme d'exactitude, de fiabilité et de protection contre la corruption.

L'objectif est de valider le fait qu'un instrument devant être approuvé est conforme aux exigences de la Recommandation OIML appropriée. Pour les instruments contrôlés par logiciel, la procédure de validation comprend l'examen, l'analyse et les essais. La Recommandation OIML appropriée doit inclure une sélection appropriée des méthodes décrites ci-après.

Les méthodes décrites ci-après se concentrent sur l'examen de type. Les vérifications individuelles d'un instrument en service ne sont pas couvertes par ces méthodes de validation. Se référer au chapitre 7 *Vérification* pour plus d'informations.

Les méthodes spécifiées pour la validation du logiciel sont décrites en 6.3. Des combinaisons de ces méthodes, formant une procédure complète de validation adaptée à toutes les exigences définies au chapitre 5, sont spécifiées en 6.4.

6.3 Méthodes de validation (examen du logiciel)

6.3.1 Vue d'ensemble des méthodes et de leur application

La sélection et l'ordre des méthodes suivantes ne sont pas prescrits et peuvent varier au cas par cas dans une procédure de validation.

Abréviation	Description	Application	Conditions préalables, outils pour traiter la demande	Compétences spéciales pour la réalisation
AD	Analyse de la documentation et validation de la conception (6.3.2.1)	Toujours	Documentation	-
VFTM	Validation par essais fonctionnels des fonctions métrologiques (6.3.2.2)	Justesse des algorithmes, incertitude, algorithme de compensation et de correction, règle pour le calcul de prix	Documentation	-
VFTSw	Validation par essais fonctionnels des fonctions logicielles (6.3.2.3)	Fonctionnement correct des communications, indications, protections contre la fraude, protections contre les erreurs d'opération, protections des paramètres, et détection des fautes	Documentation, outils logiciels courants	-
DFA	Analyse du flux de données métrologiques (6.3.2.4)	Séparation logicielle, évaluation de l'impact des commandes sur les fonctions de l'instrument	Code source, outils logiciels courants (procédure simple), outils (procédure sophistiquée)	Connaissance des langages de programmation, méthode nécessitant des instructions
CIWT	Inspection et parcours du code (6.3.2.5)	Tout objet	Code source, outils logiciels courants	Connaissance des langages de programmation, protocoles, et autres sujets TIC
SMT	Essai de module logiciel (6.3.2.6)	Tout objet lorsque les entrées et sorties sont clairement définies	Code source, environnement d'essai, outils logiciels spécifiques	Connaissance des langages de programmation, protocoles, et autres sujets TIC. Utilisation de l'outil nécessitant des instructions

Tableau 1 : Vue d'ensemble des méthodes de validation sélectionnées

Note : Les éditeurs de texte, éditeurs hexadécimaux, etc. sont considérés comme des "outils logiciels courants".

6.3.2 Description des méthodes de validation sélectionnées

6.3.2.1 Analyse de la documentation et validation de la conception (AD)

Application :

Ceci est la procédure de base qui doit être appliquée dans tous les cas.

Conditions préalables :

La procédure est basée sur la documentation du fabricant portant sur l'instrument de mesure. En fonction des demandes, cette documentation doit avoir un contenu approprié :

(1) Sous une forme générale, les spécifications des fonctions de l'instrument accessibles depuis l'extérieur (convient aux instruments simples sans interface excepté l'afficheur, toutes les caractéristiques sont vérifiables par des essais fonctionnels, faible risque de fraude).

(2) Spécifications des fonctions logicielles et des interfaces (nécessaire pour les instruments avec interfaces et pour les instruments qui ne peuvent pas être testés fonctionnellement ainsi qu'en cas de risque accru de fraude). La description doit mettre en évidence et expliquer toutes les fonctions logicielles qui pourraient avoir un impact sur les caractéristiques métrologiques.

(3) Concernant les interfaces, la documentation doit inclure une liste complète des commandes ou signaux que le logiciel est capable d'interpréter. L'effet de chaque commande doit être documenté en détail. La façon dont l'instrument réagit aux commandes non documentées doit être décrite.

(4) Une documentation additionnelle sur les fonctions logicielles doit être fournie, si nécessaire, pour comprendre et évaluer les algorithmes complexes, les fonctions cryptographiques, ou les contraintes critiques de synchronisation.

(5) Quand la façon de valider une fonction d'un logiciel n'est pas évidente, l'obligation de développer une méthode d'essai devrait incomber au fabricant. De plus, les services du programmeur devraient être mis à disposition de l'examinateur dans le but de répondre aux différentes questions.

Une condition générale préalable à l'examen est l'exhaustivité de la documentation et la claire identification de l'EUT, i.e. du contenu logiciel qui contribue aux fonctions métrologiques (voir 6.1.1).

Description :

L'examinateur évalue les fonctions et les fonctionnalités de l'instrument de mesure en utilisant la description verbale ainsi que les représentations graphiques et décide si elles sont conformes aux exigences de la Recommandation OIML appropriée. Les exigences métrologiques, tout comme les exigences fonctionnelles - logicielles définies au chapitre 5 (par exemple, la protection contre la fraude, la protection des paramètres d'ajustement, les fonctions non autorisées, la communication avec d'autres dispositifs, la mise à jour du logiciel, la détection de faute, etc.) doivent être considérées et évaluées. Cette tâche peut être facilitée par le Format de Rapport d'Evaluation Logicielle (voir Annexe B).

Résultat :

La procédure donne un résultat pour toutes les caractéristiques de l'instrument de mesure, sous réserve que la documentation appropriée ait été soumise par le fabricant. Le résultat doit être documenté dans une section relative au logiciel dans un Rapport d'Evaluation

Logicielle (voir Annexe B) inclus dans le Format de Rapport d'Evaluation de la Recommandation OIML appropriée.

Procédures complémentaires :

Des procédures additionnelles doivent être appliquées si l'examen de la documentation ne fournit pas de résultat valable permettant la validation. Dans la plupart des cas, la "Validation par essais fonctionnels des fonctions métrologiques" (voir 6.3.2.2) est une procédure complémentaire.

Références :

Directive pour les examinateurs FDA et directive pour l'industrie sur le contenu relatif au logiciel des dispositifs médicaux des soumissions pour pré-commercialisation, 29 Mai 1998 [10]; CEI 61508-7, 2000 - 3 [9].

6.3.2.2 Validation par essais fonctionnels des fonctions métrologiques (VFTM)

Application :

Exactitude des algorithmes de calcul de la valeur de mesure à partir des données brutes, de linéarisation d'une pente, de compensation des influences environnementales, des arrondis du calcul de prix, etc.

Conditions préalables :

Manuel d'utilisation, schémas de fonctionnement, références métrologiques et moyen d'essai.

Description :

La plupart des méthodes d'approbation et d'essais décrites dans les Recommandations OIML sont basées sur des mesurages de référence dans des conditions diverses. Leur application n'est pas limitée à certaines technologies d'instrument de mesure. Bien qu'ils ne visent pas particulièrement à valider le logiciel, les résultats d'essais peuvent être interprétés comme une validation de certaines parties logicielles, en général la plus importante métrologiquement. Si les essais décrits dans la Recommandation OIML appropriée couvrent toutes les fonctionnalités métrologiques pertinentes de l'instrument, les parties logicielles correspondantes peuvent être considérées comme étant validées. En général, aucune analyse logicielle ni essai n'est nécessaire pour valider les fonctionnalités métrologiques de l'instrument de mesure.

Résultat :

L'exactitude des algorithmes est valide ou invalide. Les valeurs de mesure respectent les EMT, ou non, dans toutes les conditions.

Procédures complémentaires :

La méthode est normalement une amélioration de 6.3.2.1. Dans certains cas, il peut être plus simple ou plus efficace de combiner la méthode avec des examens basés sur le code source (6.3.2.5) ou en simulant les signaux d'entrées (6.3.2.6) par exemple pour les mesurages dynamiques.

Références :

Diverses Recommandations OIML spécifiques.

6.3.2.3 Validation par essais fonctionnels des fonctions logicielles (VFTSw)

Application :

Validation, par exemple, de la protection des paramètres, de l'indication de l'identification du logiciel, de la détection de faute assistée par logiciel, de la configuration du système (plus particulièrement de l'environnement logiciel), etc.

Conditions préalables :

Manuel d'utilisation, documentation du logiciel, schémas de fonctionnement, et moyen d'essai.

Description :

Les fonctionnalités requises décrites dans le manuel d'utilisation, la documentation de l'instrument ou la documentation du logiciel, sont vérifiées en pratique. Si elles sont contrôlées par logiciel, elles doivent être considérées comme validées si elles fonctionnent correctement, sans autre analyse du logiciel. Les fonctions traitées ici sont :

- le fonctionnement normal de l'instrument : si son fonctionnement est contrôlé par logiciel. Tous les interrupteurs ou toutes les touches ou combinaisons décrites doivent être utilisés et la réaction de l'instrument évaluée. Pour les interfaces utilisateurs graphiques, tous les menus et autres éléments graphiques doivent être activés et vérifiés,
- l'efficacité de la protection des paramètres peut être vérifiée en activant le moyen de protection et en essayant de changer un paramètre,
- l'efficacité de la protection des données stockées peut être vérifiée en changeant certaines données dans le fichier et en vérifiant si cela est détecté par le programme,
- la génération et l'indication de l'identification du logiciel peuvent être validées par une vérification pratique,
- si la détection de faute est assistée par logiciel, les parties logicielles pertinentes peuvent être validées en provoquant, exécutant ou simulant une faute et en vérifiant la réaction appropriée de l'instrument,
- si la configuration ou l'environnement du logiciel réglementairement pertinent sont amenés à être fixe, les moyens de protection peuvent être vérifiés en effectuant des modifications non autorisées. Le logiciel doit inhiber ces changements ou cesser de fonctionner.

Résultat :

Les fonctionnalités contrôlées par le logiciel à l'étude sont OK, ou non OK.

Procédures complémentaires :

Certaines fonctions ou fonctionnalités d'un instrument contrôlé par logiciel ne peuvent en pratique être validées tel que décrit. Si l'instrument comporte des interfaces, il n'est en général pas possible de détecter une commande non autorisée en essayant uniquement des commandes de façon aléatoire. En outre, un émetteur est nécessaire pour générer ces

commandes. Pour un niveau de validation normal, la méthode 6.3.2.1, comprenant une déclaration du fabricant, doit couvrir cette exigence. Pour un niveau d'examen étendu, une analyse du logiciel telle que décrite 6.3.2.4 ou 6.3.2.5 est nécessaire.

References :

Directive FDA pour l'industrie Partie 11, Août 2003 [11]; Guide WELMEC 2.3 [12]; Guide WELMEC 7.2 [13].

6.3.2.4 Analyse du flux de données métrologiques (DFA)

Application :

Construction du flux des valeurs de mesure à travers le domaine des données soumis au contrôle légal. Examen de la séparation logicielle.

Conditions préalables :

Documentation du logiciel, code source, éditeur, programme de recherche textuelle ou outils spéciaux. Connaissance des langages de programmation.

Description :

Le but de cette méthode est de trouver toutes les parties du logiciel impliquées dans le calcul de la valeur de mesure ou qui peuvent avoir un impact dessus. En partant du port matériel où les données de mesure brutes du capteur sont disponibles, on cherche le sous-programme qui les lit. Ce sous-programme les stockera dans une variable après avoir éventuellement effectué des calculs. De cette variable, est lue une valeur intermédiaire par un autre sous-programme et ainsi de suite jusqu'à ce que la valeur de mesure complète soit produite par l'afficheur. Toutes les variables qui sont utilisées comme stockage pour les valeurs de mesure intermédiaires et tous les sous-programmes transportant ces valeurs peuvent être trouvés dans le code source simplement en utilisant un éditeur de texte et un programme de recherche textuelle afin de trouver les noms de la variable ou du sous-programme dans d'autres fichiers du code source que celui actuellement ouvert dans l'éditeur de texte.

D'autres flux de données peuvent être trouvés grâce à cette méthode, par exemple depuis les interfaces vers l'interpréteur de commandes. De plus, tout contournement de l'interface logicielle (voir 5.2.1.2) peut être détecté.

Résultat :

La séparation du logiciel peut être validée comme conforme ou non à 5.2.1.2.

Procédures complémentaires :

Cette méthode est recommandée si la séparation logicielle est réalisée et si une conformité élevée ou une forte protection contre les manipulations sont requises. C'est une amélioration de 6.3.2.1 à 6.3.2.3 et de 6.3.2.5.

Référence :

CEI 61131-3.

6.3.2.5 Inspection et parcours du code (CIWT)

Application :

Toute fonctionnalité du logiciel peut être validée par cette méthode si une augmentation de l'intensité de l'examen est nécessaire.

Conditions préalables :

Code source, éditeur de texte, outils. Connaissance des langages de programmation.

Description :

L'examinateur parcourt le code source instruction par instruction, évaluant les parties respectives du code afin de déterminer si les exigences sont respectées et si les fonctions et fonctionnalités du programme sont en accord avec la documentation.

L'examinateur peut également se concentrer sur des algorithmes ou fonctions qu'il a identifiés comme complexes, comme des sources d'erreur, comme insuffisamment documentés, etc. et inspecte les parties respectives du code source en les analysant et les vérifiant.

Avant ces étapes d'examen, l'examinateur aura identifié la partie logicielle réglementairement pertinente, par exemple en appliquant la méthode d'analyse du flux de données métrologiques (voir 6.3.2.4). En général, l'inspection et le parcours du code sont limités à cette partie. En combinant ces deux méthodes, l'effort nécessaire à l'examen est minimal en comparaison à la mise en œuvre de ces méthodes dans une production normale de logiciel où l'objectif est la production de programme sans panne ou encore l'optimisation des performances.

Résultat :

Mise en oeuvre compatible avec la documentation du logiciel et en accord ou non avec les exigences.

Procédures complémentaires :

Ceci est une méthode renforcée, complémentaire à 6.3.2.1 et 6.3.2.4. Elle est normalement utilisée pour la vérification de point précis.

Référence :

CEI 61508-7:2000 - 3 [9].

6.3.2.6 Essai de module logiciel (SMT)

Application :

Uniquement si un niveau élevé de conformité et de protection contre la fraude est exigé. Cette méthode est appliquée lorsque les fonctions d'un programme ne peuvent être examinées exclusivement sur la base d'informations écrites. Elle est appropriée et économiquement avantageuse pour la validation d'algorithme de mesures dynamiques.

Conditions préalables :

Le code source, des outils de développement (au moins un compilateur), l'environnement de fonctionnement du module logiciel soumis à l'essai, un jeu de données d'entrée et le jeu correspondant de référence correcte de données de sortie, ou un outil d'automatisation. Des compétences en TIC, des connaissances en langages de programmation. La coopération avec le programmeur du module soumis à l'essai est souhaitable.

Description :

Le module logiciel soumis à l'essai est intégré dans un environnement d'essai, i.e. un programme spécifique d'essai de module qui appelle le module soumis à l'essai et lui fournit toutes les données d'entrée nécessaires. Le programme d'essai reçoit les données de sortie du module soumis à l'essai et les compare avec les valeurs de référence attendues.

Résultat :

Les algorithmes de mesure ou les fonctions testés sont corrects ou non.

Procédures complémentaires :

Ceci est une méthode renforcée, complémentaire à 6.3.2.2 ou 6.3.2.5. Elle est uniquement utile dans les cas exceptionnels.

Référence :

CEI 61508-7:2000 – 3 [9].

6.4 Procédure de validation

La procédure de validation consiste en une combinaison de méthodes d'analyse et d'essais. La Recommandation OIML appropriée peut spécifier les détails relatifs à la procédure de validation, incluant :

a) la méthode de validation décrite en 6.3 devant être appliquée pour l'exigence considérée,

b) comment l'évaluation des résultats doit être réalisée,

c) quel résultat doit être inclus dans le rapport d'essai et intégré dans le certificat d'essai (voir Annexe B).

En Tableau 2 sont définis deux niveaux alternatifs, pour les procédures de validation, notés A et B. Le niveau B implique un examen plus approfondi comparé au A. Une sélection entre les procédures de validation de types A et B peut être faite dans la Recommandation OIML appropriée – différentes ou identiques pour chaque exigence – en accord avec les attendus :

- risque de fraude,
- domaine d'application,
- conformité requise au type approuvé,
- risque de mauvais résultats de mesure dus aux erreurs d'opération.

Exigence		Procédure de validation A (niveau d'examen normal)	Procédure de validation B (niveau d'examen approfondi)	Commentaire
5.1.1	Identification du logiciel	AD + VFTSw	AD + VFTSw + CIWT	Sélectionner "B" si une conformité élevée est exigée
5.1.2	Adéquation des algorithmes et fonctions	AD + VFTM	AD + VFTM + CIWT/SMT	
Protection du logiciel				
5.1.3.1	Prévention des mauvais usages	AD + VFTSw	AD + VFTSw	
5.1.3.2	Protection contre la fraude	AD + VFTSw	AD + VFTSw + DFA/CIWT/SMT	Sélectionner "B" en cas de risque de fraude élevé
Support des fonctionnalités matérielles				
5.1.4.1	Support de la détection de faute	AD + VFTSw	AD + VFTSw + CIWT + SMT	Sélectionner "B" si une fiabilité élevée est requise
5.1.4.2	Support de la protection de la durabilité	AD + VFTSw	AD + VFTSw + CIWT + SMT	Sélectionner "B" si une fiabilité élevée est requise
Spécification et séparation des parties pertinentes et spécification des interface des parties				
5.2.1.1	Séparation des dispositifs électroniques et des sous-ensembles	AD	AD	
5.2.1.2	Séparation des parties logicielles	AD	AD + DFA/CIWT	
5.2.2	Indications partagées	AD + VFTM/ VFTSw	AD + VFTM/ VFTSw + DFA/CIWT	
5.2.3	Stockage des données, transmission par systèmes de communication	AD + VFTSw	AD + VFTSw + CIWT/SMT	Sélectionner "B" si la transmission de données de mesure à travers un réseau ouvert est prévue
5.2.3.1	Les valeurs de mesure stockées ou transmises doivent être accompagnées de toutes les informations pertinentes nécessaires à l'usage futur réglementairement pertinent	AD + VFTSw	AD + VFTSw + CIWT/SMT	Sélectionner "B" en cas de risque de fraude élevé
5.2.3.2	Les données doivent être protégées par des moyens logiciels afin de garantir leur authenticité, leur intégrité et si nécessaire l'exactitude des informations relatives à l'heure de mesurage	AD + VFTSw	/	
5.2.3.3	Pour un niveau élevé de protection, il est nécessaire d'utiliser des méthodes cryptographiques	/	AD + VFTSw + SMT	
5.2.3.4	Stockage automatique	AD + VFTSw	AD + VFTSw + SMT	
5.2.3.5	Retard de transmission	AD + VFTSw	AD + VFTSw + SMT	Sélectionner "B" en cas de risque élevé de fraude, par exemple transmission dans des systèmes ouverts
5.2.3.6	Interruption de transmission	AD + VFTSw	AD + VFTSw + SMT	Sélectionner "B" en cas de risque élevé de fraude, par exemple transmission dans des systèmes ouverts
5.2.3.7	Horodatage	AD + VFTSw	AD + VFTSw + SMT	
5.2.4	Compatibilité des systèmes d'exploitation et du matériel, portabilité	AD + VFTSw	AD + VFTSw + SMT	
Maintenance et re-configuration				
5.2.6.2	Mise à jour Vérifiée	AD	AD	
5.2.6.3	Mise à jour Tracée	AD + VFTSw	AD + VFTSw + CIWT/SMT	Sélectionner "B" en cas de risque élevé de fraude

Tableau 2 : Recommandations pour combiner les méthodes d'analyse et d'essai applicables aux diverses exigences logicielles (les acronymes sont définis au Tableau 1)

6.5 Equipement soumis à l'essai (EUT)

Normalement, les essais sont réalisés sur un instrument de mesure complet (essais fonctionnels). Si la taille ou la configuration de l'instrument de mesure ne permet pas un essai de l'instrument complet ou si seul un dispositif séparé (module) de l'instrument est concerné, la Recommandation OIML appropriée peut indiquer que les essais, ou certains essais, doivent être réalisés séparément sur les dispositifs électroniques ou modules logiciels, sous réserve que dans le cas d'essais avec les dispositifs en fonctionnement, ces dispositifs soient inclus dans une configuration de simulation suffisamment représentative du fonctionnement normal. Le demandeur de l'approbation est responsable de fournir tous les moyens et composants requis.

7 Vérification

Lorsque le contrôle métrologique des instruments de mesure est prescrit dans un pays, il doit exister des moyens pour vérifier l'identité du logiciel durant son fonctionnement, la validité de l'ajustement, et la conformité au type approuvé.

La Recommandation OIML appropriée peut exiger que la vérification du logiciel soit réalisée en une ou plusieurs phases, selon la nature de l'instrument de mesure considéré.

La vérification du logiciel doit inclure :

- un examen de la conformité du logiciel avec les versions approuvées (par exemple, la vérification du numéro de version et de la somme de contrôle),
- un examen de la compatibilité de la configuration minimale déclarée, si donnée dans le certificat d'approbation,
- un examen de la bonne configuration des entrées/sorties dans le logiciel de l'instrument de mesure lorsque leur affectation est un paramètre spécifique du dispositif,
- un examen de la conformité des paramètres spécifiques du dispositif (en particulier les paramètres d'ajustement).

Les procédures de mise à jour du logiciel sont décrites au 5.2.6.2 et 5.2.6.3

8 Evaluation des niveaux de sévérité (risque)

8.1 Cette section est destinée à donner des orientations dans la détermination du jeu de niveaux de sévérité à appliquer de manière générale pour les essais effectués sur les instruments de mesure électroniques. Elle n'est pas destinée à être une classification avec des limites strictes menant à des exigences spéciales comme dans le cas de classes d'exactitude.

Qui plus est, ce guide n'interdit pas aux Comités Techniques et Sous-Comités de produire des niveaux de sévérité qui diffèrent de ceux résultants des directives établies dans ce Document. Différents niveaux de sévérité peuvent être utilisés en accord avec les limites spécifiques prescrites dans les Recommandations OIML appropriées.

8.2 Le niveau de sévérité d'une exigence doit être sélectionné indépendamment d'une exigence à l'autre.

8.3 Lors de la sélection des niveaux de sévérité pour une catégorie particulière d'instrument de mesure et du champ d'application (commerce, vente directe au public, santé, application de la loi, etc.), les aspects suivants peuvent être pris en compte :

(a) le risque de fraude :

- les conséquences, l'impact social et sociétal d'un dysfonctionnement,
- la valeur des biens à mesurer,
- la plateforme utilisée (spécifique à l'application ou ordinateur universel),
- l'exposition aux sources potentielles de fraude (dispositif de libre service en mode non surveillé).

(b) la conformité requise :

- les possibilités pratiques pour l'industrie d'être conforme au niveau prescrit.

(c) la fiabilité requise :

- les conditions environnementales;
- les conséquences, l'impact social et sociétal des erreurs.

(d) l'intérêt du fraudeur :

- être simplement capable de commettre la fraude peut être un facteur de motivation suffisant.

(e) la possibilité de répéter le mesurage ou de l'interrompre.

Dans toute la section portant sur les exigences (voir le chapitre 5), divers exemples de solutions techniques acceptables sont donnés, illustrant le niveau normal de protection contre la fraude, la conformité, la fiabilité, et le type de mesurage (identifié par (I)). Lorsque appropriés, des exemples de mesures renforcées sont également présentés dans le cas où un niveau élevé de sévérité des aspects décrits ci-dessus est envisagé (identifié par (II)).

La procédure de validation et le niveau de sévérité (risque) sont inextricablement liés. Une profonde analyse du logiciel doit être réalisée lorsqu'un niveau élevé de sévérité est exigé afin de pouvoir détecter les défaillances ou les faiblesses de sécurité du logiciel. D'autre part, le scellement mécanique (par exemple le scellement d'un port de communication ou du boîtier) doit être envisagé lors du choix de la procédure de validation.

Annexe A
Bibliographie

Au moment de la publication du D 31:2008 (E) , les éditions indiquées étaient valides. Tous les documents normatifs sont sujets à révision, et les utilisateurs de ce Document sont invités à étudier la possibilité d'appliquer les versions les plus récentes des documents normatifs indiqués ci-dessous. Les Membres de la CEI et de l'ISO tiennent des registres des Normes Internationales actuellement valides.

Le véritable statu des Normes auxquelles il est fait référence peut être également trouvé sur internet :

Publications de la CEI :	http://www.iec.ch/searchpub/cur_fut.htm
Publications de l'ISO :	http://www.iso.org/iso/iso_catalogue.htm
Publications de l'OIML :	http://www.oiml.org/publications/ (téléchargement gratuit des fichiers PDF).

Afin d'éviter tout malentendu, il est hautement recommandé que les références aux Normes, dans les Recommandations OIML et Documents Internationaux, soient suivies par la version à laquelle il est fait référence (généralement l'année ou la date).

Réf.	Normes et documents de référence	Description
[1]	Vocabulaire International des Termes Fondamentaux & Généraux de Métrologie (VIM) (1993) [6)]	Vocabulaire préparé dans le cadre d'un travail collaboratif d'experts désignés par le BIPM, la CEI, l'ISO, l'UICPA, l'UIPPA, et l'OIML.
[2]	OIML B 3:2003 Système de Certificats OIML pour les Instruments de Mesure	Le Système de Certificats OIML pour les Instruments de Mesure est un système pour l'émission, l'enregistrement, et l'utilisation des Certificats OIML de Conformité, basés sur les exigences des Recommandations OIML, pour des types d'instrument de mesure.
[3]	OIML D 11:2004 Exigences générales pour les instruments de mesure électroniques	Lignes directrices pour établir les exigences appropriées d'essais de performance métrologique relatifs aux grandeurs d'influence pouvant affecter les instruments de mesure couverts par une Recommandation Internationale.
[4]	ISO/CEI 9594-8:2001 Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - L'annuaire : cadres de clé publique et de certificat d'attribut	ISO/CEI 9594-8:2005 spécifie trois cadres et un nombre d'objets de données qui peuvent être utilisés pour authentifier et sécuriser la communication entre deux entités, par exemple entre deux entités de services d'annuaire ou entre un serveur internet et un navigateur internet. Les objets de données peuvent également être utilisés pour mettre à l'épreuve la source et l'intégrité des structures de données tels que des documents signés numériquement.
[5]	ISO 2382-9:1995 Technologies de l'information. Vocabulaire. Partie 9 : communication de données	A pour objet de faciliter les échanges internationaux dans le domaine de la communication de données. Elle présente un ensemble de termes et de définitions ayant trait à des notions choisies dans ce domaine, et définit

[6)] Le VIM fut révisé par le JCGM en 2007.

Réf.	Normes et documents de référence	Description
		les relations pouvant exister entre les différentes notions.
[6]	CEI 61508-4:1998-12 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques-programmables relatifs à la sécurité. Partie 4 : définitions et abréviations	Contient les définitions et explications des termes utilisés dans les parties 1 à 7 de cette Norme. Elle est destinée à être utilisée par tous les comités d'études pour la mise au point de leurs normes, conformément aux principes décrits dans le Guide 104 de la CEI et dans le Guide 51 ISO/CEI.
[7]	Série ISO/CEI 14598 Technologies de l'information - Évaluation de produits logiciels	La série de Norme ISO/CEI 14598 donne les méthodes de mesure, évaluation de la qualité des produits logiciels. Elle ne décrit ni les méthodes d'évaluation des processus de production de logiciels, ni les méthodes de prévision des coûts (la qualité des produits logiciels peut, évidemment, être utilisé dans ce but).
[8]	V 1:2000 Vocabulaire international des termes de métrologie légale (VIML)	Le VIML inclut seulement les concepts utilisés dans le domaine de la métrologie légale. Ces concepts comprennent les activités d'un service de métrologie légale, les documents qui en relèvent et autres problèmes liés à ces activités. Sont également inclus dans ce Vocabulaire certains concepts de caractère général qui ont été extraits du VIM.
[9]	CEI 61508-7:2000 - 3 Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques-programmables relatifs à la sécurité - Partie 7 : présentation des techniques et mesures	Contient des informations sur les concepts sous-jacents de risques et la relation entre risque et intégrité de sécurité (voir Annexe A); des méthodes rendant possibles les niveaux d'intégrité de sécurité des E/E/PE relatifs à la sécurité, et autres systèmes relatifs à la sécurité basés sur d'autres technologies, et dispositifs externes de réduction de risque à définir (Voir Annexes B, C, D et E). Elle est destinée à être utilisée par tous les comités d'études pour la mise au point de leurs normes, conformément aux principes décrits dans le Guide 104 de la CEI et dans le Guide 51 ISO/CEI.
[10]	Directive pour les examinateurs FDA et directive pour l'industrie sur le contenu relatif au logiciel des dispositifs médicaux des soumissions pour pré-commercialisation, 29 Mai 1998	Ce guide est destiné à fournir des informations à l'industrie au regard de la documentation que la FDA recommande d'inclure dans les soumissions pour pré-commercialisation de dispositifs logiciels, incluant les logiciels autonomes et les dispositifs matériels comprenant un logiciel.
[11]	Directive FDA pour l'industrie Partie 11, Août 2003	Ce guide est destiné à fournir des informations aux personnes qui ont choisi de maintenir des enregistrements ou de soumettre des informations électroniquement et, en conséquence, la partie 11 s'applique aux documents sous forme électronique qui sont créés, modifiés, maintenus, archivés, récupérés, ou transmis en vertu des exigences d'enregistrement énoncées dans les règlements de l'Agence américaine.

Réf.	Normes et documents de référence	Description
[12]	Guide WELMEC 2.3, Mai 2005 Edition 3 Guide pour l'examen des logiciels (Instruments de pesage)	
[13]	Guide WELMEC 7.2, Mai 2008 Edition 3 Guide sur les logiciels (Directive Instrument de Mesure 2004/22/CE)	Ce document fournit des guides aux personnes concernées par l'application de la Directive Instruments de Mesure (Directive Européenne 2004/22/CE ; MID), plus particulièrement pour les instruments de mesure équipés de logiciels. Il s'adresse aux fabricants d'instruments de mesure et aux Organismes Notifiés qui sont responsables de l'évaluation de la conformité des instruments MID. Suivre ce Guide permet de présumer du respect aux exigences de la MID relatives aux logiciels.

Annexe B
Exemple de Rapport d'Evaluation Logicielle
(Informatif)

Note : Les Comités et Sous-Comités Techniques développant des Recommandations OIML doivent décider quelles informations doivent être incluses dans le Rapport d'Essais et le Certificat OIML de Conformité. Par exemple, le nom, la version et la somme de contrôle du fichier exécutable de l'exemple suivant doivent être inclus dans le Certificat d'Essai.

Rapport d'essai n° XYZ122344
Validation du logiciel du compteur Tournesol Metering **modèle** TT100

Le logiciel de l'instrument de mesure a été validé afin de démontrer la conformité aux exigences de la Recommandation OIML R-xyz.

La validation a été basée sur le rapport du Document International OIML D 31:2008, où les exigences essentielles applicables aux logiciels sont interprétées et expliquées. Ce rapport décrit l'examen du logiciel qui est nécessaire à la déclaration de conformité à la R-xyz.

Fabricant	Demandeur
Tournesol Metering	New Company
Boîte Postale 1120333	Nova Street 123
100 Klow	1000 Las Dopicos
Syldavie	San Theodorod
Référence : M. Tryphon Tournesol	Référence : M. Archibald Haddock

Objet soumis à l'essai

Le compteur Tournesol Metering TT100 est un instrument de mesure destiné au mesurage de débit de liquides. Son étendue de mesure va de 1 L/s à 2000 L/s. Les fonctions de base de l'instrument sont :

- mesurer le débit de liquide,
- indiquer le volume mesuré,
- s'interfacer au transducteur.

L'instrument est décrit comme étant un instrument spécifique à l'application (un système embarqué) muni d'un dispositif de stockage contenant les données réglementairement pertinentes.

Le compteur TT100 est un instrument de mesure indépendant doté d'un transducteur qui lui est connecté. Le transducteur inclut une compensation en température. L'ajustement des débits est possible par mémorisation des paramètres d'étalonnage dans une mémoire non volatile du transducteur. Ce dernier est solidaire de l'instrument et ne peut en être déconnecté. Le volume mesuré est indiqué sur un afficheur. Aucune communication avec un autre dispositif n'est possible.

Le logiciel embarqué de l'instrument de mesure a été développé par

Tournesol Metering, Boîte Postale 1120333, 100 Klow, Syldavie.

Le nom du fichier exécutable est "**tt100_12.exe**".

La version du logiciel validé est la **V1.2c**. La version du logiciel est présentée sur l'afficheur lors de la mise en route de l'instrument et lors d'une pression de plus de 4 secondes sur le bouton "niveau".

Le code source comprend les fichiers réglementairement pertinents suivants :

- main.c 12301 octet 23 nov. 2003,
- int.c 6509 octet 23 nov. 2003,
- filter.c 10897 octet 20 oct. 2003,
- input.c 2004 octet 20 oct. 2003,
- display.c 32000 octet 23 nov. 2003,
- ethernet.c 23455 octet 15 juin 2002,
- driver.c 11670 octet 15 juin 2002,
- calculate.c 6788 octet 23 nov. 2003.

Le fichier exécutable "**tt100_12.exe**" est protégé contre les modifications par une somme de contrôle. La valeur de la somme de contrôle par l'algorithme **XYZ** est **1A2B3C**.

La validation a été appuyée par la documentation du fabricant suivante :

- manuel Utilisateur TT 100 Edition 1.6,
- manuel de Maintenance TT 100 Edition 1.1,
- description du logiciel TT 100 (document interne de conception, daté du 22 nov. 2003),
- diagramme des circuits électroniques TT 100 (schémas n° 222-31, date du 15 oct. 2003).

La version finale de l'objet soumis à l'essai a été fournie au Laboratoire National de Mesurage et d'Essai le 25 novembre 2003.

Réalisation de la validation

La validation a été réalisée conformément à l'OIML D 31:2008. Elle a été réalisée entre le 1er novembre et le 23 décembre 2003. Une revue de la conception a été effectuée le 3 décembre par le Dr. K. Fehler au siège de Tournesol Metering, Klow. Les autres travaux de validation ont été effectués au Laboratoire National de Mesurage et d'Essai et par le Dr. K. Fehler et M. S. Problème.

Les exigences suivantes ont été validées :

- identification du logiciel,
- adéquation des algorithmes et fonctions,
- protection du logiciel,
- prévention des mauvais usages,
- protection contre la fraude,
- support des fonctionnalités matérielles,
- stockage des données, transmission par systèmes de communication.

Les méthodes de validation suivantes ont été utilisées :

- analyse de la documentation et validation de la conception,
- validation par essais fonctionnels des fonctions métrologiques,
- inspection et parcours du code,
- essai de module logiciel sur le module calculate.c à l'aide de SDK XXX.

Résultat

Les exigences suivantes de l'OIML D 31:2008 ont été validées sans que la moindre faute ne soit détectée :

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.

Deux commandes qui n'étaient pas initialement décrites dans le manuel utilisateur ont été trouvées. Les deux commandes ont été incluses dans le manuel utilisateur daté du 10 décembre 2003.

Une faute logicielle limitant le mois de février à 28 jours les années bissextiles a été trouvée dans le paquet logiciel V1.2b. Ceci est corrigé en V1.2c.

Le résultat s'applique uniquement à l'élément testé portant le numéro de série 1188093-B-2004.

Conclusion

Le logiciel **Tournesol Metering TT100 V1.2c** respecte les exigences de l'OIML R-xyz.

Laboratoire National de Mesurage et d'Essai
Département logiciel

Dr. K.E.I.N. Fehler	M. S.A.N.S. Problème
Manager technique	Technicien

Liste de contrôle

Clause	Exigence	Succès	Echec	Remarque
5.1	**Exigences générales**			
5.1.1	**Identification du logiciel** Le logiciel réglementairement pertinent doit être clairement identifié.			
5.1.2	**Adéquation des algorithmes et fonctions** Les algorithmes et fonctions de mesure d'un dispositif doivent être corrects.			
5.1.3	**Protection du logiciel**			
5.1.3.1	**Prévention des mauvais usages** Un instrument de mesure – et plus particulièrement son logiciel – doit être construit de telle sorte que les possibilités de mauvais usage non intentionnel, accidentel ou intentionnel soient minimales.			
5.1.3.2	**Protection contre la fraude**			
a)	Le logiciel réglementairement pertinent doit être sécurisé contre les modifications non autorisées, le chargement ou les changements par échange de mémoire. En plus des scellements mécaniques, des moyens techniques peuvent être nécessaires pour sécuriser les instruments de mesure ayant un système d'exploitation ou une option de chargement de logiciel.			
b)	Seules les fonctions clairement documentées (voir 6.1) sont autorisées à être activées par le biais de l'interface utilisateur, qui doit être réalisée de telle manière qu'elle ne facilite pas un usage frauduleux. La présentation des informations doit être conforme avec 5.2.2.			
c)	Les paramètres qui fixent les caractéristiques réglementairement pertinentes de l'instrument de mesure doivent est sécurisés contre les modifications non autorisées. Si nécessaire, et à des fins de vérification, le parmètrage actuel doit pouvoir être affiché ou imprimé.			
d)	La protection du logiciel comprend le scellement par des moyens mécaniques, électroniques et/ou cryptographiques rendant toute intervention non autorisée impossible ou évidente.			
5.1.4	**Support des fonctionnalités matérielles**			
5.1.4.1	**Support de la détection de faute** Il doit être exigé que le fabricant de l'instrument conçoive les systèmes de contrôle dans la partie logicielle ou dans la partie matérielle ou encore donne les moyens par lesquels la partie matérielle peut être supportée par la partie logicielle de l'instrument.			
5.1.4.2	**Support de la protection de la durabilité** Il appartient au fabricant de choisir de réaliser les systèmes de protection de la durabilité de manière logicielle ou matérielle, ou de permettre aux systèmes matériels d'être supportés par du logiciel.			
5.2	**Exigences spécifiques**			
5.2.1	**Spécification et séparation des parties pertinentes et spécification des interfaces des parties** Les parties métrologiquement critiques d'un système de mesure ne doivent pas être inacceptablement influencées par les autres parties du système de mesure			
5.2.1.1	**Séparation des dispositifs électroniques et des sous-ensembles**			
a)	Les sous-ensembles ou dispositifs électroniques d'un système de mesure qui réalisent des fonctions réglementairement pertinentes doivent être identifiés, clairement définis et documentés.			
b)	Il doit être démontré durant les essais d'approbation de type que les fonctions et données pertinentes des sous-ensembles et dispositifs électroniques ne peuvent pas être inacceptablement influencées par les commandes reçues via l'interface.			
5.2.1.2	**Séparation des parties logicielles**			
a)	L'exigence de conformité s'applique à toute partie réglementairement pertinente (voir 5.2.5) qui doit être identifiable suivant les prescriptions de 5.1.1.			

Clause	Exigence	Succès	Echec	Remarque
b)	Si la partie logicielle réglementairement pertinente communique avec d'autres parties, une interface logicielle doit être définie. Toute communication doit être exclusivement réalisée via cette interface. La partie logicielle réglementairement pertinente ainsi que l'interface doivent être clairement documentées. Toute fonction et domaine réglementairement pertinent du logiciel doivent être décrits pour permettre à l'autorité d'approbation de type de décider si la séparation logicielle est correcte ou non.			
c) **d)**	L'affectation de chaque commande doit être sans ambiguïté pour toute fonctions initiées ou tous changements de données dans la partie réglementairement pertinente du logiciel. Les commandes qui communiquent à travers l'interface logicielle doivent être déclarées et documentées. Seules les commandes documentées sont autorisées à être activées à travers l'interface logicielle. Le fabricant doit déclarer l'exhaustivité de la documentation relative aux commandes. Lorsque le logiciel réglementairement pertinent est séparé du logiciel réglementairement non pertinent, le logiciel réglementairement pertinent doit avoir priorité dans l'utilisation des ressources sur le logiciel réglementairement non pertinent.			
5.2.2	**Indications partagées** Si l'indication est réalisée en utilisant une interface utilisateur multi fenêtrée, l'exigence suivante s'applique : Le logiciel qui réalise l'indication des valeurs de mesure et d'autres informations réglementairement pertinentes appartient à la partie réglementairement pertinente. La fenêtre contenant ces données doit avoir la plus haute priorité**.**			
5.2.3	**Stockage des données, transmission par systèmes de communication**			
5.2.3.1	Les valeurs de mesure stockées ou transmises doivent être accompagnées de toutes les informations pertinentes nécessaires à l'usage futur réglementairement pertinent.			
5.2.3.2	Les données doivent être protégées par des moyens logiciels afin de garantir leur authenticité, leur intégrité et si nécessaire l'exactitude des informations relative à l'heure de mesurage. Le logiciel qui affiche ou traite ultérieurement les valeurs de mesure et les données les accompagnant doit vérifier l'heure de mesurage, l'authenticité et l'intégrité des données après les avoir lues depuis un stockage non sûr ou après les avoir reçues par un canal de transmission non sûr. Si une irrégularité est détectée, les données doivent être rejetées ou marquées inutilisables.			
5.2.3.3	Pour un niveau élevé de protection, il est nécessaire d'utiliser des méthodes cryptographiques.			
5.2.3.4 **a)** **b)** **c)**	**Stockage automatique** Les données de mesure doivent être stockées automatiquement lorsque le mesurage est conclu. Le dispositif de stockage doit avoir une stabilité suffisante pour garantir que les données ne sont pas corrompues dans des conditions normales de stockage. La capacité de stockage doit être suffisante pour toute application particulière. Lorsque la valeur finale utilisée pour l'application légale résulte d'un calcul, toutes les données nécessaires au calcul doivent être automatiquement stockées avec la valeur finale. Les données stockées peuvent être effacées si : ▪ la transaction est conclue, ▪ ces données sont imprimées par une imprimante soumise au contrôle légal. Lorsque les exigences de 5.2.3.4.b sont remplies et quand le stockage est plein, l'effacement de données mémorisées est autorisé lorsque les deux conditions suivantes sont remplies : ▪ les données sont effacées dans le même ordre que l'ordre d'enregistrement et les règles établies pour l'application particulière sont respectées, ▪ l'effacement est effectué automatiquement ou après une opération manuelle particulière.			
5.2.3.5	**Retard de transmission** Les mesures ne doivent pas être influencées inacceptablement par un retard de transmission.			
5.2.3.6	**Interruption de transmission** Si le service réseau devient indisponible, aucune donnée de mesure ne doit être perdue. Le processus de mesure doit être stoppé pour éviter la perte de données de mesure.			

Clause	Exigence	Succès	Echec	Remarque
5.2.3.7	**Horodatage** L'horodatage doit être lu depuis l'horloge du dispositif. Des moyens de protection appropriés doivent être pris en accord avec le niveau de sévérité devant être appliqué (voir 5.1.3.2.c). Si l'information en rapport avec l'heure de mesurage est nécessaire, la fiabilité de l'horloge interne de l'instrument doit être renforcée à l'aide de moyens spécifiques.			
5.2.4	**Compatibilité des systèmes d'exploitation et du matériel, portabilité**			
5.2.4.1	Le fabricant doit identifier l'environnement matériel et logiciel qui est approprié. Les ressources minimales ainsi que la configuration adaptée qui sont nécessaires au bon fonctionnement, doivent être déclarées par le fabricant.			
5.2.4.2	Des moyens techniques doivent être inclus afin d'empêcher toute opération si les exigences de configuration minimale ne sont pas respectées.			
5.2.6	**Maintenance et re-configuration**			
5.2.6.1	L'utilisation des seules versions du logiciel réglementairement pertinent qui sont conformes au type approuvé est autorisée.			
5.2.6.2	**Mise à jour Vérifiée** Après la mise à jour du logiciel réglementairement pertinent de l'instrument de mesure (échange avec une autre version approuvée ou réinstallation), l'instrument n'est pas autorisé à être employé à des fins légales avant qu'une vérification de celui-ci n'ait été réalisée et que les moyens de sécurisation aient été renouvelés.			
5.2.6.3	**Mise à jour Tracée**			
a)	La Mise à jour Tracée de logiciel doit être automatique. A l'achèvement de la procédure de mise à jour, l'environnement de protection logicielle doit être du même niveau que celui requis par l'approbation de type.			
b)	L'instrument de mesure cible doit avoir un logiciel réglementairement pertinent figé.			
c)	Des moyens techniques doivent être utilisés afin de garantir l'authenticité du logiciel chargé. Si le logiciel chargé à la vérification d'authenticité, l'instrument doit le rejeter et utiliser la version précédente du logiciel ou basculer dans un mode inopérant.			
d)	Des moyens techniques doivent être utilisés afin d'assurer l'intégrité du logiciel chargé, i.e. qu'il n'a pas été changé de façon inacceptable avant son chargement.			
e)	Des moyens techniques appropriés doivent être employés afin d'assurer que les Mises à jour Tracées soient adéquatement traçables dans l'instrument.			
f)	L'instrument de mesure doit avoir un dispositif/sous-ensemble électronique permettant à l'utilisateur ou au détenteur d'exprimer son consentement, par exemple, un bouton poussoir, avant que le téléchargement ne commence. Il doit être possible d'activer/de désactiver ce dispositif/sous-ensemble électronique, par exemple à l'aide d'un interrupteur qui peut être scellé ou à l'aide d'un paramètre. Si le dispositif/sous-ensemble électronique est activé, chaque téléchargement doit être initié par l'utilisateur ou le détenteur. S'il est désactivé, aucune action de la part de l'utilisateur ou du détenteur n'est nécessaire pour réaliser le téléchargement.			
g)	Si les exigences de 5.2.6.3.a à 5.2.6.3.f ne peuvent être remplies, il demeure cependant toujours possible de mettre à jour la partie logicielle réglementairement non pertinente. Dans ce cas, les exigences suivantes doivent être respectées : ▪ il existe une séparation distincte entre le logiciel réglementairement pertinent et le logiciel réglementairement, non pertinent conformément à 5.2.1, ▪ le logiciel réglementairement pertinent tout entier ne peut être mis à jour sans briser de scellement, ▪ il est déclaré dans le certificat d'approbation de type que la mise à jour du logiciel réglementairement non pertinent est acceptable.			
5.2.6.4	L'instrument de mesure doit être pourvu d'un système enregistrant automatiquement, et de manière non effaçable, tout ajustement de paramètre spécifique au dispositif, par exemple une expertise de l'historique. L'instrument doit être capable de présenter les données enregistrées.			

Clause	Exigence	Succès	Echec	Remarque
5.2.6.5	Les moyens de traçabilité et les enregistrements font partie du logiciel réglementairement pertinent et doivent être protégés en en tant que tels.			

Annexe C
Index