DOCUMENTO
INTERNACIONAL

OIML D 31

Edición 2008 (ES)

Requisitos generales para los instrumentos de medida controlados por software

OIML D 31 Edición 2008 (ES)

ORGANIZACIÓN INTERNACIONAL DE
METROLOGÍA LEGAL

ÍNDICE

Prólogo

La Organización Internacional de Metrología Legal (OIML) es una organización mundial e intergubernamental. Su principal objetivo consiste en armonizar las reglamentaciones y los controles metrológicos que aplican los servicios metrológicos nacionales u otras organizaciones análogas de sus Estados miembros. Las principales categorías de las publicaciones de la OIML son las siguientes:

- **Recomendaciones internacionales (OIML R).** Modelos de reglamentaciones que fijan las características metrológicas de los instrumentos de medida, y de los métodos y medios de control de su conformidad. Los Estados miembros de la OIML aplicarán estas Recomendaciones en la medida de lo posible,.

- **Documentos internacionales (OIML D).** Son de naturaleza informativa, están destinados a mejorar y armonizar la actividad de los servicios de metrología.

- **Guías internacionales (OIML G).** Son de naturaleza informativa, están destinados a proporcionar directrices para la aplicación de ciertos requisitos de la metrología legal.

- **Publicaciones internacionales básicas (OIML B).** Definen las reglas de funcionamiento de los diversos sistemas y estructuras de la OIML.

Los Comités o Subcomités técnicos, constituidos por representantes de los Estados miembros, elaboran proyectos de Recomendaciones, Guías y Documentos OIML. Algunas instituciones internacionales y regionales también participan a título consultivo. Entre la OIML y determinadas instituciones, como la ISO y la IEC, se han establecido acuerdos de cooperación con el objeto de evitar requisitos contradictorios. Como resultado, usuarios y fabricantes de instrumentos de medida, laboratorios de ensayos, etc. pueden aplicar de forma simultánea las publicaciones de la OIML y las de otras instituciones.

Las Recomendaciones internacionales, los Documentos, las Guías y las Publicaciones básicas se publican en lengua inglesa (E), se traducen al francés (F) y se revisan de forma periódica.

El presente documento ha sido traducido al español por el Centro Español de Metrología **(NIPO 706-10-013-3)**.

Además la OIML publica o participa en la publicación de **Vocabularios (OIML V)** y periódicamente encarga la redacción de **Informes de expertos (OIML E)** a expertos en metrología legal. La finalidad de los Informes de expertos consiste en proporcionar información y asesoramiento. Su contenido refleja exclusivamente el punto de vista del autor, ningún Comité o Subcomité técnico ni el CIML ha participado en su redacción, por lo que no representan necesariamente la opinión de la OIML.

El Subcomité técnico de la OIML TC 5/SC 2 *Software* elaboró la versión inglesa de esta publicación —referencia OIML D 31, edición 2008 (E) — que fue aprobada para su publicación final en 2008 por el Comité Internacional de Metrología Legal.

Las Publicaciones de la OIML pueden descargarse del sitio web de la OIML en formato de archivo PDF. Para obtener información adicional sobre las Publicaciones de la OIML puede ponerse en contacto con la Oficina central de la Organización:

Bureau International de Métrologie Légale

11, rue Turgot - 75009 París – Francia

Teléfono: 33 (0)1 48 78 12 82

Fax: 33 (0)1 42 82 17 27

E-mail: biml@oiml.org

Internet: www.oiml.org

Requisitos generales para los instrumentos de medida controlados por software

1. Introducción

El objetivo principal de este Documento internacional consiste en proporcionar a los Comités y Subcomités técnicos de la OIML una guía a la hora de establecer requisitos adecuados para aquellas funcionalidades relacionadas con el software de los instrumentos de medida incluidos en las Recomendaciones OIML.

Además, este Documento internacional puede orientar a los Estados miembros de la OIML en la implementación de las Recomendaciones OIML en su legislación nacional.

2. Ámbito y campo de aplicación

2.1 En este Documento internacional se describen los requisitos generales aplicables a las funcionalidades software de los instrumentos de medida, asimismo constituye una guía para verificar si un instrumento cumple con estos requisitos.

2.2 Los Comités y Subcomités técnicos de la OIML considerarán este Documento como una base para establecer los requisitos y los procedimientos específicos del software en las Recomendaciones de la OIML aplicables a categorías concretas de instrumentos de medida (en adelante denominadas «Recomendaciones OIML pertinentes»).

2.3 Las instrucciones que se incluyen en este Documento únicamente son aplicables a dispositivos electrónicos o instrumentos de medida controlados por software.

Notas:

- En este Documento no se incluyen todos los requisitos técnicos específicos para instrumentos de medida controlados por software; estos requisitos se incluirán en la Recomendación OIML pertinente, p. ej. para instrumentos de pesaje, contadores de agua, etc.

- En este Documento se tratan algunos aspectos relacionados con la protección de datos. Además, se debe tener en cuenta la reglamentación nacional en esta área.

- También es necesario considerar la OIML D 11 sobre *Requisitos generales para los instrumentos de medida electrónicos* (OIML D 11:2004 [3]), ya que los dispositivos controlados por software siempre son electrónicos.

3. Terminología

Algunas de las definiciones utilizadas en el presente Documento coinciden con las del *Vocabulario internacional de términos fundamentales y generales de metrología* (VIM:1993 [1] (Primera edición en español, 1994)), con el *Vocabulario internacional de términos de metrología legal* (OIML V 1:2000 [8]), con el Documento internacional OIML sobre *Requisitos generales para los instrumentos de medida electrónicos* (OIML D 11:2004 [3]) y con diversas Normas Internacionales ISO/IEC. Para este Documento se aplican las siguientes definiciones y siglas.

3.1 Terminología general

3.1.1 Solución aceptable

Diseño o principio de un módulo software o unidad hardware, o de una característica que se considera que cumple un requisito determinado. Una solución aceptable constituye un ejemplo de cómo puede cumplirse un requisito en concreto, sin perjuicio de otras soluciones que también satisfagan ese requisito.

3.1.2 Registro de actividades

Archivo de datos continuo que incluye un registro de información histórica de sucesos; p. ej. modificaciones en los valores de los parámetros de un dispositivo o actualizaciones del software, así como otras actividades legalmente relevantes que pueden influir en las características metrológicas.

3.1.3 Autenticación

Verificación de la identidad declarada o alegada de un usuario, proceso o dispositivo (p. ej. verificar que el software descargado procede del propietario del certificado de aprobación de modelo).

3.1.4 Autenticidad

Resultado del proceso de autenticación (aceptado o rechazado).

3.1.5 Dispositivo de control [OIML D 11:2004, 3.18]

Herramienta incorporada a un instrumento de medida que permite detectar fallos importantes y manifestarlos.

Nota: El término «manifestar» hace referencia a toda respuesta adecuada del instrumento de medida (señal luminosa, señal acústica, detener el proceso de medida, etc.).

3.1.6 Red cerrada

Red de un número fijo de participantes de quienes se conoce la identidad, la funcionalidad y la ubicación (véase también «Red abierta»).

3.1.7 Comandos

Secuencia de señales eléctricas (ópticas, electromagnéticas, etc.) en interfaces de entrada o códigos en protocolos de la transmisión de datos. Se pueden generar a partir del software del instrumento de medida / dispositivo electrónico / subconjunto (comandos de software), o bien por el usuario a través de la interfaz de usuario del instrumento de medida (comandos de usuario).

3.1.8 Comunicación

Intercambio de información entre dos o más unidades (p. ej. módulos de software, dispositivos electrónicos, subconjuntos, etc.) de acuerdo con reglas específicas.

3.1.9 Interfaz de comunicación

Interfaz electrónica, óptica, de radiofrecuencia o cualquier otra interfaz técnica que posibilita la transmisión de información entre los componentes de un instrumento de medida (p. ej. dispositivos electrónicos) o entre sus subconjuntos.

3.1.10 Certificado criptográfico

Conjunto de datos que contienen la clave pública de un instrumento de medida o de una persona más una identificación única del sujeto; p. ej. el número de serie del instrumento de medida, o el nombre o el número de identificación personal (PIN) de la persona. Una institución confiable con firma electrónica es la firmante del conjunto de datos. La asignación de una clave a un sujeto puede verificarse utilizando la clave pública de la institución confiable y descifrando la firma del certificado.

3.1.11 Métodos criptográficos

Procesos en los que el remitente cifra datos (programa de almacenamiento o de transmisión) y el receptor los descifra (programa lector) con el objetivo de ocultar información a personas no autorizadas.

Firma electrónica de los datos con el objeto de permitir al receptor o usuario de los mismos verificar su origen; es decir, comprobar su autenticidad.

Nota: Por lo general, se utiliza para firmar electrónicamente un sistema de clave pública. El algoritmo necesita un par de claves de las que sólo una debe mantenerse en secreto, el resto pueden ser públicas.

El remitente (el programa de envío o de almacenamiento) genera un código *hash* (véase el apartado 3.1.25) de los datos y lo cifra con su

«clave secreta», el resultado es la firma. El receptor (el programa receptor o lector) la descifra con la «clave pública» del remitente y compara el resultado con el código *hash* real de los datos. Si coinciden, los datos se autentican.

El receptor puede requerir un certificado criptográfico al remitente (véase el apartado 3.1.10) para confirmar la autenticidad de la clave pública.

3.1.12 Dominio de datos

Ubicación en la memoria que todo programa necesita para procesar datos. En función del tipo de lenguaje de programación utilizado, la ubicación se define mediante direcciones de hardware o nombres simbólicos (nombres de variables). El tamaño del domino direccional más pequeño suele ser un byte, pero prácticamente no está limitado: varía de 1 bit (p. ej. el *flag* de un registro) a estructuras de datos arbitrarias que pueden ser tan grandes como las necesidades del programador.

Los dominios de datos pueden pertenecer a un único «módulo software» o a varios. En el caso de lenguajes de alto nivel (como JAVA, C/C++, etc.) es fácil impedir el acceso al dominio de datos de un módulo de software desde otros módulos software a través del lenguaje.

3.1.13 Parámetro específico del dispositivo

Parámetro legalmente relevante cuyo valor depende de cada instrumento. Los parámetros específicos del dispositivo son los parámetros de ajuste (p. ej. ajuste de intervalo u otros ajustes o correcciones) y los parámetros de configuración (p. ej. valor máximo, valor mínimo, unidades de medida, etc.).

3.1.14 Durabilidad [OIML D 11:2004, 3.17]

Capacidad de un instrumento de medida para mantener sus características de funcionamiento durante el período de uso.

3.1.15 Instrumento de medida electrónico [OIML D 11:2004, 3.1]

Instrumento de medida diseñado para medir una magnitud ya sea eléctrica o no, utilizando métodos electrónicos y/o equipado con dispositivos electrónicos.

Nota: En este Documento el equipamiento auxiliar se considerará parte del instrumento de medida, siempre que esté sujeto al control metrológico legal.

3.1.16 Dispositivo electrónico [OIML D 11:2004, 3.2]

Dispositivo que utiliza subconjuntos y desempeña una función específica. Un dispositivo electrónico suele fabricarse como una unidad separada y se puede someter a ensayo de forma independiente.

Nota: Puede constituir un instrumento de medida completo (p. ej. una balanza o un contador de electricidad) o ser una parte del mismo (p. ej. una impresora o un puntero).

Puede constituir un módulo según el sentido con el que se utiliza en la OIML B 3 *Sistema de certificado OIML para instrumentos de medida* [2].

3.1.17 Error (de indicación) [VIM:1994, 5.20; OIML D 11:2004, 3.5]

Indicación de un instrumento de medida menos un valor verdadero de la magnitud de entrada correspondiente.

3.1.18 Registro de errores

Archivo continuo de datos con un registro de información de fallos o defectos que afectan a las características metrológicas. En concreto se aplica a fallos volátiles que no son reconocibles después de haber utilizado los valores de medida.

3.1.19 Evaluación (de modelo) [OIML V 1:2000, 2.5]

Examen y ensayo sistemáticos del funcionamiento de una o más muestras de un modelo identificado (patrón) de instrumento de medida frente a requisitos documentados. Los resultados se incluyen en el informe de evaluación con el objeto de determinar si el modelo se puede aprobar.

3.1.20 Suceso

Acción en la que se produce la modificación de un parámetro de un instrumento de medida, el ajuste de un factor o la actualización del módulo software.

3.1.21 Contador de sucesos

Contador no reiniciable que se incrementa con cada suceso nuevo.

3.1.22 Código ejecutable

Archivo instalado en el sistema informático del instrumento de medida, del dispositivo electrónico o del subconjunto (EPROM, disco duro, etc.). El microprocesador interpreta este código y lo traduce en determinadas operaciones lógicas, aritméticas, de decodificación o transporte de datos.

3.1.23 Fallo [definición adaptada de la OIML D 11:2004, 3.9]

Defecto que repercute en las propiedades o funciones del instrumento de medida o que provoca un error de indicación mayor que el EMP.

3.1.24 Parte fija del software legalmente relevante

Parte de un software legalmente relevante que es y permanece idéntica en el código ejecutable a la del modelo aprobado[1)].

3.1.25 Función *hash* [ISO/IEC 9594-8:2001][4]

Función (matemática) que proyecta los valores de un dominio amplio (probablemente muy amplio) en un rango menor. Una función hash correcta es aquella en la que los resultados de aplicar la función en un conjunto (amplio) de valores del dominio se distribuyen uniformemente (y aparentemente de forma aleatoria) sobre el rango.

3.1.26 Integridad de los programas, los datos o los parámetros

Garantía de que los programas, los datos o los parámetros no se han visto sujetos a ninguna modificación no autorizada o no intencionada durante su uso, transferencia, almacenamiento, reparación o mantenimiento.

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

Límite compartido entre dos unidades funcionales definidas por varias características pertenecientes a las funciones, las interconexiones físicas, los intercambios de señales, así como a otras características de las unidades según proceda.

3.1.28 Error intrínseco [VIM:1994, 5.24; OIML D 11:2004, 3.7]

Error de un instrumento de medida determinado en las condiciones de referencia.

3.1.29 Legalmente relevante

Software/hardware/datos, o parte de los mismos, de un instrumento de medida que interfiere en las propiedades reguladas por la metrología legal; p. ej. la adecuación de la medida o del correcto funcionamiento del instrumento de medida.

3.1.30 Parámetro legalmente relevante

Parámetro de un instrumento de medida, dispositivo electrónico o subconjunto sujetos al control legal. Se pueden distinguir los siguientes tipos de parámetros legalmente relevantes: «parámetros específicos del modelo» y «parámetros específicos del dispositivo».

---

1) Esta parte es la responsable de llevar un control de la actualización del software (carga del software, autenticación, comprobación de integridad, instalación y activación).

3.1.31 Parte legalmente relevante del software

Parte de todos los «módulos de software» de un instrumento de medida, dispositivo electrónico o subconjunto que es legalmente relevante.

3.1.32 Error máximo permitido (de un instrumento de medida) [VIM:1994 5.21; OIML D 11:2004, 3.6]

Valor extremo de un error permitido por especificaciones, normativas, etc., para un instrumento de medida dado.

3.1.33 Instrumento de medida [VIM:1994, 4.1]

Dispositivo destinado a utilizarse para hacer mediciones, solo o asociado a uno o varios dispositivos anexos.

3.1.34 Medición continua/ discontinua

Se denomina continua cuando consiste en un proceso de medición acumulativo sin interrupción cuyo final no está definido. Un usuario u operador no puede detener y reanudar de nuevo el proceso de medición sin que en consecuencia pueda perturbar inadmisiblemente la medida o el suministro de productos o energía.

Se denomina discontinua si la medición acumulativa de la magnitud de una sustancia puede detenerse fácil y rápidamente durante el funcionamiento normal —no sólo en caso de emergencia— sin falsificar el resultado de medición.

3.1.35 Red abierta

Red de participantes arbitrarios (dispositivos electrónicos con funciones arbitrarias). El número, la identidad y la ubicación de un participante pueden ser dinámicos y desconocidos para otros participantes (véase también «red cerrada»).

3.1.36 Funcionamiento [OIML D 11:2004, 3.16]

Capacidad de un instrumento de medida para llevar a cabo su función.

3.1.37 Código del programa

«Código fuente» o «código ejecutable».

3.1.38 Precintado

Método para proteger el instrumento de medida contra cualquier modificación no autorizada, reajuste, extracción de partes, software, etc. Puede realizarse mediante el hardware, el software o una combinación de ambos.

3.1.39 Protección

Acción de evitar el acceso no autorizado a la parte del software o del hardware de un dispositivo.

3.1.40 Software

Término genérico que comprende los parámetros, los datos y el código del programa.

3.1.41 Examen del software

Operación técnica basada en determinar una o más características del software en función de un procedimiento específico (p. ej. análisis de la documentación técnica o la puesta en marcha del programa en condiciones controladas).

3.1.42 Identificación del software

Secuencia de caracteres legibles (p. ej. número de versión, suma de comprobación) vinculada indefectiblemente al software o al «módulo de software» en cuestión. Se puede comprobar en un instrumento durante su uso.

3.1.43 Interfaz software

Código del programa y dominio de datos dedicado; recibe, filtra y transmite datos entre «módulos de software» (no necesariamente legalmente relevantes).

3.1.44 Módulo de software [definición similar a la IEC 61508-4:1998, 3.3.7][6]

Entidad lógica como un programa, una subrutina, una biblioteca o un objeto, incluyendo sus «dominios de datos», que puede estar relacionada con otras entidades. El software de los instrumentos de medida, los dispositivos electrónicos o los subconjuntos constan de uno o más módulos de software.

3.1.45 Protección del software

Acción de proteger el software o el dominio de datos de un instrumento de medida mediante un precinto instalado en el hardware o el software. Para modificar el software se debe eliminar, dañar o romper el precinto.

3.1.46 Separación del software

El software de dispositivos/subconjuntos instrumentos/electrónicos de medida puede dividirse en una «parte legalmente relevante» y una parte legalmente no relevante. Estas partes se comunican a través de una «interfaz software».

3.1.47 Código fuente

Programa informático escrito de tal forma (lenguaje de programación) que se puede leer y editar. El código fuente se compila o interpreta en un «código ejecutable».

3.1.48 Dispositivo de almacenamiento

Almacenamiento utilizado para conservar datos de medida disponibles después de completar la medición con fines legalmente relevantes (p. ej. el cierre de una transacción comercial).

3.1.49 Subconjunto [OIML D 11:2004, 3.3]

Parte de un dispositivo electrónico que utiliza componentes electrónicos y tiene una función reconocible por sí misma.

Ejemplos: amplificadores, comparadores, convertidores de energía, etc.

3.1.50 Ensayo [OIML D 11:2004, 3.20]

Serie de operaciones con el objeto de verificar si el equipo sometido a ensayo (EUT) cumple con los requisitos específicos.

3.1.51 Registro de fecha y hora

Valor de tiempo único que se incrementa de forma monótona; p. ej. en segundos, o una cadena de fecha y hora que indica cuándo se produjo un suceso o un fallo concreto. Estos datos se presentan en un formato coherente que permite comparar con facilidad dos registros distintos y su seguimiento a lo largo de tiempo.

3.1.52 Transmisión de datos de medida

Transmisión de datos de medida a través de redes de comunicación u otros medios a un dispositivo electrónico remoto, donde estos se siguen procesando y/o utilizando con fines regulados legalmente.

3.1.53 Parámetro específico del modelo

«Parámetro legalmente relevante» cuyo valor depende únicamente del modelo de instrumento. Los parámetros específicos del modelo forman parte del software legalmente relevante.

Ejemplo: En un sistema de medida de líquidos distintos del agua, el rango de viscosidad cinemática de una turbina es un parámetro específico de modelo fijado en la aprobación de modelo de la turbina. Todas las turbinas fabricadas del mismo modelo poseen el mismo rango de viscosidad.

3.1.54 Ordenador universal

Ordenador que no ha sido construido para un fin específico pero que puede adaptarse a la tarea metrológica mediante software. Por lo general este software se basa en un sistema operativo que permite cargar y ejecutar el software con fines específicos.

3.1.55 Interfaz de usuario

Interfaz que permite el intercambio de información entre una persona y el instrumento de medida, su hardware o los componentes software; como los interruptores, el teclado, el ratón, la pantalla, el monitor, la impresora, la pantalla táctil, la ventana software en una pantalla incluyendo el software que la había generado.

3.1.56 Validación [derivada de la ISO/IEC 14598 y la IEC 61508-4:1998][7]

Confirmación del cumplimiento de los requisitos particulares para el uso específico mediante el examen y la aportación de pruebas objetivas (es decir, información cuya certeza es demostrable y se basa en hechos a partir de observaciones, mediciones, ensayos, etc.). En este caso los requisitos son los establecidos en este Documento.

3.1.57 Verificación [V 1:2000, 2.13]

Procedimiento (distinto a la aprobación de modelo) que incluye el examen y el marcado y/o la emisión de un certificado de verificación y que establece y confirma que el instrumento de medida cumple con los requisitos reglamentarios [2)].

3.2 Listado de siglas

EUT Equipo sometido a ensayo

IEC Comisión Electrotécnica Internacional

E/S Entrada/Salida (puertos)

ISO Organización Internacional de Normalización

[2)] Nota: esta definición es distinta a la establecida en otras Normas, como por ejemplo la ISO/IEC 14598, apartado 4.23 o la IEC 61508-4, apartado 3.8.1.

TIC Tecnologías de la información y de las comunicaciones

EMP Error máximo permitido

OIML Organización Internacional de Metrología Legal

PCB Placa de circuito impreso

PIN Número de identificación personal

TC Comité técnico (OIML)

SC Subcomité (OIML)

4. Instrucciones para el uso de este Documento en la elaboración de Recomendaciones OIML

4.1 Los apartados de este Documento se aplican únicamente a las nuevas Recomendaciones OIML y a los Documentos OIML en proceso de revisión. Los TC y los SC deben utilizar este Documento orientativo para establecer los requisitos relacionados con el software, además de los requisitos técnicos y metrológicos de la Recomendación OIML correspondiente.

4.2 Todo documento normativo está sujeto a revisión y se invita a los usuarios de este Documento a investigar si existen ediciones más recientes de los documentos normativos y la posibilidad de aplicarlas.

4.3 La finalidad de este Documento consiste en proporcionar a los TC y SC responsables de elaborar las Recomendaciones OIML un conjunto de requisitos —con distintos niveles en algunos apartados— adecuados para todo tipo de instrumento de medida y en todas las áreas de aplicación. Cada TC y SC determinará el nivel adecuado de severidad en cuestiones de protección, conformidad o validación, así como el modo de incorporar las partes relevantes de este Documento a la Recomendación OIML que se está elaborando. En el apartado 8 se presentan unas pautas para llevar a cabo esta tarea.

5. Requisitos de las aplicaciones software de instrumentos de medida

5.1 Requisitos generales

En el momento de la publicación de este Documento los requisitos generales representan el estado actual de las tecnologías de la información (TIC). En principio son aplicables a todo tipo de instrumento de medida, dispositivo electrónico y subconjunto controlado por software, y deberían considerarse en todas las Recomendaciones OIML. En comparación con estos requisitos

generales, los específicos para la configuración (5.2) tratan características técnicas poco comunes en algunos tipos de instrumentos o en algunas áreas de aplicación.

En los ejemplos, cuando son aplicables, se ilustran los niveles de severidad normal y alto. En este Documento la notación se presenta del siguiente modo:

(I) Solución técnica aceptable con nivel de severidad normal.

(II) Solución técnica aceptable con nivel de severidad alto (véase el apartado 8).

5.1.1 Identificación del software

El software legalmente relevante de un instrumento de medida/ dispositivo electrónico/ subconjunto se debe identificar claramente con el número de versión del software u otro método. La identificación puede constar de más de una parte, pero al menos una debe estar orientada a fines legales.

La identificación debe estar vinculada de forma indefectible al propio software y se debe presentar o imprimir mediante un comando, o visualizarse durante su funcionamiento o en la puesta en marcha de un instrumento de medida que pueda encenderse y apagarse de nuevo. Si un subconjunto/ dispositivo electrónico no tiene pantalla ni impresora, la identificación debe transmitirse a través de una interfaz de comunicación para su visualización/impresión en otro dispositivo electrónico/subconjunto.

Como excepción, la identificación impresa del software en el instrumento/dispositivo electrónico debe considerarse una solución aceptable si se cumplen las siguientes condiciones:

(1) La interfaz de usuario no tiene capacidad de control para activar la indicación de la identificación del software en el dispositivo indicador, o éste no permite técnicamente mostrar la identificación del software (dispositivo indicador analógico o contador electromecánico).

(2) El instrumento/dispositivo electrónico no posee una interfaz para comunicar la identificación del software.

(3) Después de la fabricación del dispositivo electrónico/instrumento no es posible modificar el software, o únicamente lo es si se modifican también el hardware o un componente del mismo.

El fabricante del hardware o del componente del hardware en cuestión tiene la responsabilidad de garantizar que la identificación del software se haya marcado correctamente en el instrumento/dispositivo electrónico correspondiente.

La identificación del software y los métodos de identificación se deben establecer en el certificado de aprobación de modelo.

La correspondiente Recomendación OIML debe permitir o desestimar esta excepción.

Nota: Todo instrumento de medida en servicio debe ser conforme con el modelo aprobado. La identificación del software permite al personal inspector y a los usuarios del instrumento de medida verificar dicha conformidad.

Ejemplo:

(I) El software contiene una cadena de texto o un número que identifica de manera inequívoca la versión instalada. Esta cadena se transmite al dispositivo indicador al pulsar un botón cuando se enciende el instrumento o de manera cíclica, controlado por un temporizador.

Un número de versión puede seguir la estructura A.Y.Z. En el caso de un controlador de caudal, la letra A representará la versión del software central que cuenta impulsos, la letra Y representará la versión de la función de conversión (ninguna, a 15 ºC, a 20 ºC) y la letra Z representará el idioma de la interfaz de usuario.

(II) El software calcula una suma de comprobación del código ejecutable y presenta el resultado como la identificación en lugar o además de la cadena de (I). El algoritmo de la suma de comprobación será un algoritmo normalizado, p. ej. el algoritmo CRC16 es una solución aceptable para este cálculo.

La solución (II) es adecuada si se requiere un mayor nivel de conformidad (véanse los apartados 5.2.5 (d) y 8).

5.1.2 Adecuación de algoritmos y funciones

Los algoritmos de medida y las funciones de un dispositivo electrónico deben ser adecuados y funcionalmente correctos para la aplicación y el modelo de dispositivo dados (exactitud de los algoritmos, cálculo del precio según ciertas reglas, algoritmos de redondeo, etc.).

El resultado de medida y la información complementaria requerida por las Recomendaciones OIML o la legislación nacional se deben visualizar o imprimir correctamente.

Se deben poder examinar los algoritmos y las funciones, ya sea mediante ensayos metrológicos, ensayos de software o examen del software (como se describe en el apartado 6.3).

5.1.3 Protección del software

5.1.3.1 Prevención del uso incorrecto

Un instrumento de medida debe fabricarse de modo que las posibilidades de hacer un uso incorrecto intencionado, accidental o no intencionado sean mínimas. En el marco de este Documento OIML, lo anterior se aplica especialmente al software. La presentación de los resultados de medida debe ser inequívoca para todas las partes afectadas.

Nota: La funcionalidad de los instrumentos controlados por software suele ser compleja. El usuario necesita un buen asesoramiento para hacer un uso adecuado y obtener resultados de medida correctos.

Ejemplo:

El usuario se desplaza a través de menús. Las funciones legalmente relevantes se agrupan en una rama de dicho menú. Si algún valor de medida se perdiera por una acción, el usuario debería ser advertido e invitado a realizar otra acción antes de que se ejecute la función. Véase también el apartado 5.2.2.

5.1.3.2 Protección contra el fraude

5.1.3.2.a El software legalmente relevante se protegerá contra modificaciones no autorizadas, cargas o cambios derivados de la sustitución del dispositivo de memoria. Además del precintado mecánico, se pueden necesitar medios técnicos para proteger instrumentos de medida con sistema operativo o con una opción para la carga de software.

Nota: Cuando un software se almacena en un dispositivo de memoria inviolable (en el que los datos son inalterables; p. ej. un ROM precintado (siglas en inglés de «memoria de sólo lectura»)) se reduce la necesidad de medios técnicos.

Ejemplo:

(I)/(II) La carcasa de los dispositivos de memoria está precintada o el dispositivo de memoria está precintado en el PCB.

(II) Si se utiliza un dispositivo regrabable, un interruptor que se puede precintar inhibe la entrada que habilita la escritura. El circuito está diseñado de tal modo que la protección contra escritura no se puede cancelar mediante un cortocircuito de contactos.

(I) Un sistema de medida está formado por dos subconjuntos, uno contiene las principales funciones metrológicas en una carcasa que se puede precintar, y el otro es un ordenador universal con un sistema operativo. Algunas funciones, como la indicación, se encuentran en el

software de este ordenador. Una manipulación relativamente sencilla —especialmente si en la comunicación entre las dos partes del software se utiliza un protocolo estándar—, consistiría en sustituir el software del ordenador universal.

Esta manipulación puede evitarse mediante métodos criptográficos simples; p. ej. el cifrado de la transferencia de datos entre el subconjunto y el ordenador universal. La clave necesaria para descifrar está oculta en el programa legalmente relevante del ordenador universal. Únicamente este programa conoce la clave y puede leer, descifrar y utilizar los valores de medida. No pueden utilizarse otros programas con este objetivo, ya que no son capaces de descifrar los valores de medida (véase también el ejemplo del apartado 5.2.1.2.d).

5.1.3.2.b La interfaz de usuario únicamente puede activar aquellas funciones claramente documentadas (véase el apartado 6.1), dicha activación se realizará sin facilitar el uso fraudulento. La presentación de la información cumplirá con lo establecido el apartado 5.2.2.

Nota: El evaluador es quien decide si todos estos comandos documentados son aceptables.

Ejemplo:

(I)/(II) Todas las entradas de la interfaz de usuario se redirigen a un programa que filtra los comandos entrantes, que sólo permite y deja pasar aquellos documentados, descartando el resto. Este programa o módulo de software forma parte del software legalmente relevante.

5.1.3.2.c Los parámetros que fijan las características legalmente relevantes del instrumento de medida deben estar protegidos contra modificaciones no autorizadas. Si es necesario para llevar a cabo la verificación, los conjuntos de parámetros existentes se deben poder visualizar o imprimir.

Nota: Los parámetros específicos del dispositivo únicamente se pueden ajustar o elegir en un modo operativo concreto del instrumento. Se pueden clasificar como aquellos que deberían estar protegidos (inalterables) y aquellos accesibles para una persona autorizada (parámetros configurables), p. ej. el propietario del instrumento o el proveedor del producto.

Los parámetros específicos del modelo tienen valores idénticos para todos los ejemplares de un modelo. Se fijan en la aprobación de modelo del instrumento.

Ejemplo:

(I)/(II) Para proteger los parámetros específicos del dispositivo, estos se almacenan en una memoria permanente. Un interruptor que se puede precintar inhibe la entrada que habilita la escritura en la memoria.

Consúltense los ejemplos del apartado 5.1.3.2.d (1) al (3) en esta sección.

5.1.3.2.d La protección del software incluye un precintado adecuado a través de medios mecánicos, electrónicos y/o criptográficos, que imposibilita o hace evidente una intervención no autorizada.

Ejemplo:

(1) (I) Precintado electrónico. Los parámetros metrológicos de un instrumento se pueden introducir y ajustar a través de un elemento del menú. El software reconoce cada modificación e incrementa un contador de sucesos por cada suceso de este tipo. Se puede visualizar el valor de este contador. El valor inicial del contador se debe registrar. Si el valor visualizado difiere del registrado, el instrumento se encuentra en un estado sin verificar (equivalente a un precinto roto).

(2) (I)/(II) El software de un instrumento de medida está diseñado de tal modo (véase el ejemplo 5.1.3.2.a) que no existe la posibilidad de modificar los parámetros ni la configuración legalmente relevante si no es a través de un menú protegido por un interruptor. Este interruptor está precintado de forma mecánica en posición inactiva, imposibilitando la modificación de los parámetros y de la configuración legalmente relevante.

Para modificar los parámetros y la configuración debe activarse el interruptor, con lo que inevitablemente se rompe el precintado.

(3) (II) El software de un instrumento de medida se diseña de tal modo (véase el ejemplo (a)) que sólo el personal autorizado puede acceder a los parámetros y a la configuración legalmente relevante. Si un usuario quiere entrar en el elemento de menú de configuración de parámetros, debe insertar su tarjeta inteligente con un código PIN como parte de un certificado criptográfico. El software del instrumento puede verificar la autenticidad del PIN mediante el certificado, permitiendo la entrada al elemento de menú. El acceso queda grabado en un registro de actividades con la identidad del usuario (o al menos de la tarjeta inteligente utilizada).

El nivel (II) de los ejemplos de soluciones técnicas aceptables es el adecuado si se necesita un nivel de protección alto contra el fraude (véase el apartado 8).

5.1.4 Características de hardware

5.1.4.1 Detección de fallos

La Recomendación OIML pertinente puede requerir funciones de detección de ciertos fallos del instrumento (citadas en la OIML D 11:2004 (5.1.2 (b) y 5.3)). En este caso, se requerirá al fabricante del instrumento diseñar herramientas de comprobación en las partes del software o del hardware, o bien aportar medios a través de los cuales partes del software del instrumento puedan respaldar el funcionamiento de las partes del hardware.

Si el software actúa en una detección de fallos, debe reaccionar de forma adecuada. La Recomendación OIML pertinente puede determinar que en caso de detectar un fallo, se desactive el instrumento/dispositivo electrónico o se genere una alarma/registro en un registro de errores.

La documentación presentada para la aprobación de modelo incluirá una lista de fallos detectables mediante el software y su reacción esperada y además, si fuera necesario para facilitar la comprensión, una descripción del algoritmo detector.

Ejemplo:

(I)/(II) En cada puesta en marcha, el programa legalmente relevante calcula una suma de comprobación del código del programa y de los parámetros legalmente relevantes. El valor nominal de estas sumas de comprobación se ha calculado con anterioridad y se ha almacenado en el instrumento. Si los valores calculados y almacenados no coinciden, el programa detiene la ejecución.

Si la medición no puede interrumpirse, la suma de comprobación se calcula de forma cíclica y controlada mediante un temporizador software. En caso de detectar un fallo, el software visualiza un mensaje de error o enciende el indicador de fallos y registra la fecha del mismo en un registro de errores (si existe).

El CRC16 constituye un algoritmo de suma de comprobación aceptable.

5.1.4.2 Protección de durabilidad

El fabricante puede elegir implementar los sistemas de protección de la durabilidad, citados en la OIML D 11:2004 (5.1.3 (b) y 5.4), bien en el software o

en el hardware, los sistemas, o permitir que el software respalde el funcionamiento de los sistemas hardware. La Recomendación OIML pertinente puede proponer soluciones adecuadas.

Si el software participa en la protección de durabilidad, debe reaccionar de una forma adecuada. La Recomendación OIML pertinente puede determinar que se desactive el instrumento/dispositivo electrónico o que se genere una alarma/registro si se detecta que la durabilidad está en riesgo.

Ejemplo:

(I)/(II) Algunos tipos de instrumentos de medida necesitan un ajuste tras un intervalo de tiempo determinado, a fin de garantizar la durabilidad de la medición. El software advierte si el intervalo de mantenimiento ha transcurrido e incluso detiene la medición si se ha excedido durante cierto intervalo de tiempo.

5.2 Requisitos específicos para las configuraciones

Los requisitos descritos en esta sección se basan en soluciones técnicas habituales de las TIC, aunque puede que no sean comunes en todas las áreas de aplicación legal. Al cumplir estos requisitos se consiguen soluciones técnicas que presentan el mismo grado de seguridad y de conformidad con el modelo que los instrumentos que no están controlados por software.

Los siguientes requisitos específicos son necesarios cuando se utilizan ciertas tecnologías en sistemas de medida. Estos requisitos deber considerarse además de los descritos en el apartado 5.1.

En los ejemplos, cuando son aplicables, se muestran los niveles de severidad normal y alto. La notación en este documento es la siguiente:

(I) solución técnica aceptable en caso de nivel de severidad normal;

(II) solución técnica aceptable en caso de nivel de severidad alto (véase el apartado 8).

5.2.1 Especificación y separación de las partes relevantes y especificación de las interfaces de las mismas

Las partes de un sistema de medida críticas en cuanto a la metrología —ya sean partes de software o de hardware— no se deben ver influenciadas más allá de lo admisible por otras partes del sistema de medida.

Este requisito se aplica si el instrumento de medida (dispositivo electrónico o subconjunto) posee interfaces para establecer comunicación con otros dispositivos electrónicos, con el usuario, o con otras partes del software distintas de aquellas críticas en cuanto a metrología dentro de un instrumento de medida (dispositivo electrónico o subconjunto).

5.2.1.1 Separación de dispositivos electrónicos y subconjuntos

5.2.1.1.a Los subconjuntos o dispositivos electrónicos de un sistema de medida que llevan a cabo funciones legalmente relevantes se deben identificar, definir claramente y documentar. Éstos constituyen la parte legalmente relevante del sistema de medida.

Nota: El evaluador establece si esta parte está completa y si las demás partes del sistema de medida se pueden excluir en posteriores evaluaciones.

Ejemplo:

(1) (I)/(II) Un contador de energía eléctrica dispone de una interfaz óptica para conectar un dispositivo electrónico que lea valores de medida. El contador almacena todas las magnitudes relevantes y conserva los valores disponibles que se pueden leer durante una duración suficiente. En este sistema, el único dispositivo legalmente relevante es el contador de energía eléctrica. Pueden existir otros dispositivos legalmente no relevantes conectados a la interfaz del instrumento siempre que se cumpla el requisito 5.2.1.1.b. La protección en la transmisión de datos no es necesaria (véase el apartado 5.2.3).

(2) (I)/(II) Un sistema de medida está constituido por los siguientes subconjuntos:

- un sensor digital que calcula el peso o el volumen;
- un ordenador universal que calcula el precio;
- una impresora que imprime el valor de medida y el precio a pagar.

Todos los subconjuntos están conectados por una red de área local. En este caso el sensor digital, el ordenador universal y la impresora constituyen subconjuntos legalmente relevantes y se conectan de forma opcional a un sistema de ventas legalmente no relevante. Los subconjuntos legalmente relevantes deben cumplir con el requisito 5.2.1.1.b y —debido a la transmisión a través de la red— también con los requisitos incluidos en el apartado 5.2.3. No existen requisitos sobre el sistema de gestión de ventas.

5.2.1.1.b Durante el ensayo de modelo, se debe demostrar que los comandos recibidos a través de la interfaz no pueden influir de forma inadmisible en los datos y las funciones relevantes de los subconjuntos y dispositivos electrónicos.

Ello implica la existencia de una asignación inequívoca de cada comando para toda función iniciada, o modificación de datos, en el subconjunto o dispositivo electrónico.

Nota: Consúltese el apartado 5.2.3 si los subconjuntos o dispositivos electrónicos «legalmente relevantes» interactúan con otros subconjuntos o dispositivos electrónicos «legalmente relevantes».

Ejemplo:

(1) (I)/(II) El software del contador de energía eléctrica (véase el ejemplo (1) del apartado 5.2.1.1.a anterior) puede recibir comandos para seleccionar las magnitudes requeridas. Combina el valor de medida con información adicional —p. ej. registro de fecha y hora, unidad— y remite estos datos al dispositivo solicitante. El software únicamente acepta comandos para seleccionar magnitudes permitidas y válidas, descarta cualquier otro comando remitiendo únicamente un mensaje de error. Pueden existir métodos de protección para el contenido del conjunto de datos pero no es un requisito, pues el conjunto de datos transmitido no está sujeto al control legal.

(2) (I)/(II) En el interior de la carcasa que se puede precintar existe un interruptor que define el modo operativo del contador de energía eléctrica: una posición del interruptor indica el modo verificado y la otra el modo sin verificar (existen métodos de protección distintos al precinto mecánico; véanse los ejemplos de los apartados 5.1.3.2.a/.d). Al interpretar los comandos recibidos el software comprueba la posición del interruptor: en el modo sin verificar, el conjunto de comandos que el software acepta es más amplio en comparación con el modo descrito más arriba; p. ej. se puede ajustar el factor de calibración mediante un comando descartado en el modo verificado.

5.2.1.2. Separación de partes del software

Los TC y los SC de la OIML pueden especificar en la Recomendación pertinente el software/ el hardware/ los datos o la parte de los mismos legalmente relevantes.

Las regulaciones nacionales pueden prescribir que un software/ hardware/ unos datos específicos, o parte de los mismos, sea legalmente relevantes.

5.2.1.2.a Todos los módulos software (programas, subrutinas, objetos, etc.) que realizan funciones legalmente relevantes, o que contienen dominios de datos legalmente relevantes, constituyen la parte legalmente relevante del software de un instrumento de medida (dispositivo electrónico o subconjunto). El requisito de conformidad se aplica a esta parte (véase el apartado 5.2.5) y debe identificarse, como se describe en el apartado 5.1.1.

Si no es posible ni necesario separar el software, éste se considera legalmente relevante como un todo.

Ejemplo:

(l) Un sistema de medida contiene varios sensores digitales conectados a un ordenador personal que visualiza los valores de medida. El software legalmente relevante del ordenador personal se separa de las partes legalmente no relevantes, compilando todos los procedimientos que desarrollan funciones legalmente relevantes en una biblioteca de enlaces dinámicos. Una o más aplicaciones legalmente no relevantes pueden solicitar procedimientos de programa en esta biblioteca. Estos procedimientos reciben los datos de medida de los sensores digitales, calculan el resultado de la medición y lo visualizan en una ventana del software. Cuando las funciones legalmente relevantes han finalizado, se devuelve el control a la aplicación legalmente no relevante.

5.2.1.2.b Si la parte legalmente relevante del software se comunica con otras partes del mismo, se debe definir una interfaz software. Toda la comunicación se debe desarrollar exclusivamente a través de esta interfaz. La parte legalmente relevante del software y la interfaz deben estar claramente documentadas. Todas las funciones y los dominios de datos legalmente relevantes del software se deben describir con el objeto de permitir a una autoridad de aprobación de modelo decidir si la separación del software es correcta.

La interfaz contiene un código de programa y dominios de datos dedicados. Los comandos definidos y codificados, así como los datos, se intercambian entre las partes del software a través del dominio de datos dedicado: una parte del software los almacena y otra los lee. El código del programa de escritura y de lectura forma parte de la interfaz software. El dominio de datos que constituye la interfaz software se debe definir y documentar claramente, incluidos el código que exporta de la parte legalmente relevante hacia el dominio de datos de la interfaz y el que importa de la interfaz a la parte legalmente relevante. No se debe poder eludir la interfaz software declarada.

El fabricante tiene la responsabilidad de respetar estas restricciones. No existen medios técnicos (como el precintado) para impedir que un programa eluda la interfaz ni la programación de comandos ocultos. El fabricante debe proporcionar instrucciones relativas a estos requisitos a los programadores de la parte legalmente relevante y de la no relevante del software.

5.2.1.2.c Debe asignarse cada comando de forma inequívoca a todas las funciones iniciadas o modificaciones de datos en la parte legalmente relevante del software. Los comandos comunicados a través de la interfaz software se deben declarar y documentar. Únicamente se pueden activar a través de la interfaz software los comandos documentados. El fabricante debe declarar que la documentación de comandos es completa.

Ejemplo:

(I) En el ejemplo descrito en el apartado 5.2.1.2.a la interfaz software se desarrolla a través de parámetros y valores de retorno de los procedimientos de la biblioteca. No se devuelven punteros a dominios de datos dentro de la biblioteca. La definición de la interfaz se fija en la biblioteca compilada, legalmente relevante sin que ninguna aplicación pueda modificarla. No es imposible eludir la interfaz software y acceder a los dominios de datos de la biblioteca directamente, pero esto no es una buena práctica de programación, es más bien complicado y podría considerarse piratería informática.

5.2.1.2.d Si un software legalmente relevante se ha separado de uno no relevante, el primero debe tener prioridad en la utilización de los recursos. Las funciones de medición (desarrolladas por la parte legalmente relevante) no se deben ver retrasada ni bloqueada por otros procesos.

El fabricante tiene la responsabilidad de respetar estas restricciones. Se deben proporcionar medios técnicos para evitar que un programa legalmente no relevante altere las funciones legalmente relevantes. El fabricante debe proporcionar instrucciones relacionadas con estos requisitos a los programadores de la parte legalmente relevante del software y de la parte legalmente no relevante.

Ejemplos:

(1) (I) En el ejemplo 5.2.1.2.a/.c la aplicación legalmente no relevante controla el inicio de los procedimientos legalmente relevantes de la biblioteca. Omitir la llamada a estos procedimientos inhibiría la función legalmente relevante del sistema. Por lo tanto, para cumplir el requisito 5.2.1.2.d se han establecido las siguientes consideraciones para el sistema de ejemplo: los sensores digitales envían los datos de medida en un formato cifrado. La clave para descifrarlos está oculta en la biblioteca. Únicamente los procedimientos de la biblioteca conocen la clave y son capaces de leer, descifrar y visualizar valores de medida. Si el programador de la aplicación desea leer y procesar estos valores, debe utilizar los procedimientos legalmente relevantes de la biblioteca que llevan a cabo todas las funciones legalmente relevantes requeridas cuando son llamados. La biblioteca contiene procedimientos que exportan los valores de medida descifrados, permitiendo al programador de la aplicación utilizarlos para sus propias necesidades después de que el procesamiento legalmente relevante haya finalizado.

(2) (I)/(II) El software de un contador de energía eléctrica electrónico lee los valores de medida sin procesar de un conversor analógico digital (ADC). Para calcular correctamente los valores de medida, el retraso entre el suceso «datos disponibles» del ADC al finalizar el almacenamiento en la

memoria intermedia de los valores de medida es crucial. Una rutina de interrupción iniciada por la señal de «datos disponibles» lee los valores sin procesar. El instrumento puede comunicarse en paralelo a través de una interfaz con otros dispositivos electrónicos mediante otra rutina de interrupción (comunicación legalmente no relevante). El resultado de interpretar el requisito del apartado 5.2.1.2 en una configuración de este tipo, conlleva que la prioridad de la rutina de interrupción para el procesamiento de valores de medida sea mayor que la de la rutina de comunicación.

Los ejemplos del apartado 5.2.1.2.a al 5.2.1.2.c y del apartado 5.2.1.2.d (1) son aceptables como solución técnica únicamente para el nivel de severidad normal (I). Si es necesario aumentar la protección contra el fraude o la conformidad (véase el apartado 8), la separación del software por sí sola no es suficiente. Se necesitan métodos complementarios o el software en su totalidad debe considerarse bajo control legal.

5.2.2 Indicaciones compartidas

La visualización o impresión pueden utilizarse para presentar la información de la parte legalmente relevante del software, además de otra información. El contenido y el diseño son específicos del tipo de instrumento y del área de aplicación, además deben estar definidos en la Recomendación correspondiente. Sin embargo, si la indicación se realiza mediante una interfaz de usuario de ventanas múltiples, se aplican los siguientes requisitos:

El software que produce la indicación de los valores de medida y de otra información legalmente relevante pertenece a la parte legalmente relevante. La ventana que contenga estos datos debe tener la máxima prioridad; es decir, ningún software debe poder eliminarla, no se le deben superponer ventanas generadas por otro software, ni se debe poder minimizar o hacer invisible mientras la medición esté en curso y los resultados presentados sean necesarios para el fin legalmente relevante.

Ejemplo:

En un sistema como el descrito en los ejemplos de los apartados del 5.2.1.2.a al 5.2.1.2.d los valores de medida se visualizan en una ventana de software separada. Los medios descritos en el apartado 5.2.1.2.d garantizan que únicamente la parte legalmente relevante del programa puede leer los valores de medida. En un sistema operativo con una interfaz de usuario de ventanas múltiples se utiliza un medio técnico complementario para cumplir el requisito del apartado 5.2.2: la ventana que visualiza los datos legalmente relevantes se genera y controla mediante procedimientos de la biblioteca de enlaces dinámicos legalmente relevante (véase el apartado 5.2.1.2). Durante la medición, estos procedimientos comprueban de forma cíclica que la ventana en cuestión siga sobre las demás ventanas abiertas; si no es así, la situarán encima.

Si se necesita un nivel alto de protección contra el fraude (II), puede que una impresión no sea suficiente como única indicación. Debe existir un subconjunto con mayores medios de seguridad capaces de visualizar los valores de medida.

No resulta adecuado utilizar un ordenador universal como parte de un sistema de medida si se necesita un nivel alto de protección contra el fraude (II). Cuando esto ocurra se deben considerar precauciones complementarias para evitar o minimizar el riesgo de fraude de hardware y de software, como cuando se utiliza un ordenador universal (por ejemplo PC, PDA, etc.).

5.2.3 Almacenamiento de datos, transmisión a través de sistemas de comunicación

Si los valores de medida se utilizan en otro lugar aparte del de la medición o en una fecha posterior a la misma, probablemente deban abandonar el instrumento de medida (dispositivo electrónico, subconjunto) y ser almacenados o transmitidos a un entorno desprotegido antes de ser utilizados con fines legales. En este caso se aplican los siguientes requisitos:

5.2.3.1 El valor de medida almacenado o transmitido irá acompañado de toda la información pertinente necesaria para su uso legalmente relevante en el futuro.

Ejemplo:

(I)/(II) Un conjunto de datos puede contener las siguientes entradas:

- valor de medida con su unidad incluida;
- registro de fecha y hora de la medición (véase el apartado 5.2.3.7);
- localización de la medición o identificación del instrumento de medida utilizado en la medición;
- identificación inequívoca de la medición, p. ej. números consecutivos que permiten asignar los valores impresos en una factura.

5.2.3.2 Los datos se protegerán mediante medios software para garantizar su autenticidad, integridad y, si procede, la exactitud de la información relativa al momento de la medición.

El software que visualiza o que posteriormente procesa los valores de medida y los datos complementarios comprobará el momento de la medición, la autenticidad y la integridad de los datos después de haberlos leído a partir de un almacenamiento inseguro o después de haberlos recibido por un canal de transmisión inseguro. Si se detecta una irregularidad, los datos se deben descartar o marcar como inservibles.

Los módulos de software que preparan los datos para almacenarlos o enviarlos, o que los verifican después de haberlos leído o recibido, pertenecen a la parte legalmente relevante del software.

Nota: Es recomendable exigir un nivel de severidad mayor cuando se trata de una red abierta.

Ejemplo:

(I) El programa del dispositivo emisor calcula la suma de comprobación del conjunto de datos (un algoritmo como BCC, CRC16, CRC32, etc.) y la añade al conjunto de datos. Para este cálculo utiliza un valor inicial secreto en lugar del valor dado en la norma. Este valor inicial se utiliza como clave y se almacena como una constante en el código del programa. El programa receptor o lector también ha almacenado este valor inicial en su código del programa. Antes de utilizar el conjunto de datos, el programa receptor calcula la suma de comprobación y la compara con aquella almacenada en el conjunto de datos. Si ambos valores coinciden, el conjunto de datos no ha sido falsificado. De otro modo, el programa asume la falsificación y descarta el conjunto de datos.

5.2.3.3 Para obtener un nivel de protección alto es necesario aplicar métodos criptográficos. Las claves confidenciales utilizadas para este fin se guardarán en secreto y protegidas en los instrumentos de medida, dispositivos electrónicos o subconjuntos correspondientes. Deberán proporcionarse métodos de forma que estas claves sólo se puedan leer o escribir rompiendo un precinto.

Ejemplo:

(II) El programa de almacenamiento o envío genera una «firma electrónica», primero calculando el valor *hash*[3)] y posteriormente cifrando el valor *hash* con la clave secreta de un sistema público de claves[4)]. El resultado es la firma que se añade al conjunto de datos almacenados o transmitidos. El receptor también calcula el valor *hash* del conjunto de datos y descifra la firma añadida al conjunto de datos con la clave pública. Se compara el valor *hash* calculado con el descifrado. Si coinciden, el conjunto de datos no ha sido falsificado (la integridad queda demostrada). Para demostrar el origen del conjunto de datos el receptor debe saber si la clave pública pertenece al emisor, es decir, al dispositivo emisor. Por lo tanto, la clave pública se visualiza en el dispositivo indicador del instrumento de medida y se puede registrar una vez, por ejemplo junto con el número de serie del dispositivo cuando esté verificado legalmente en campo. Si el receptor está seguro de que utilizó la clave pública correcta para decodificar la firma, la autenticidad del conjunto de datos también queda demostrada.

5.2.3.4 Almacenamiento automático

5.2.3.4.a Si, en función de la aplicación, es necesario almacenar datos, los datos de medida deben almacenarse de forma automática al concluir la medición, es decir, cuando se haya generado el valor final utilizado con fines legales.

El dispositivo de almacenamiento debe tener permanencia suficiente como para garantizar que los datos no son corrompidos en condiciones normales de almacenamiento. La capacidad de almacenamiento debe ser suficiente para cada aplicación particular.

Cuando el valor final utilizado con fines legales resulta de un cálculo, todos los datos necesarios para dicho cálculo se deben almacenar de forma automática con el valor final.

Nota: Los valores de medida acumulativos como, por ejemplo, la energía eléctrica o el volumen de gas se deben actualizar constantemente. Como siempre se utiliza el mismo dominio de datos (variable del programa), el requisito relativo a la capacidad de almacenamiento no se aplica en mediciones acumulativas.

3) Algoritmos aceptables: SHA-1, MD5, RipeMD160 o equivalente.

4) Algoritmos aceptables: RSA (longitud de clave de 1 024 bits), Curvas elípticas (longitud de clave de 160 bits) o equivalente.

5.2.3.4.b Se pueden eliminar los datos almacenados si:

- ya se ha concluido la transacción;
- estos datos se han impreso con un dispositivo de impresión sujeto al control legal.

Nota: Otras regulaciones generales a nivel nacional (por ejemplo la legislación fiscal) pueden incluir limitaciones estrictas en la eliminación de datos de medida almacenados.

5.2.3.4.c Una vez cumplidos los requisitos establecidos del apartado 5.2.3.4.b y cuando el almacenamiento está lleno, se pueden eliminar datos memorizados si se cumplen las dos condiciones siguientes:

- que se eliminen los datos en el mismo orden de registro respetando las normas establecidas en la aplicación particular;
- que se eliminen de forma automática o después de una operación manual específica.

Nota: El uso de derechos adicionales de acceso debería considerarse cuando se lleve a cabo la «operación manual específica» señalada en el segundo punto.

5.2.3.5 Retraso en la transmisión

La medición no debería verse influenciada de forma inadmisible por un retraso en la transmisión.

5.2.3.6 Interrupción de la transmisión

Si los servicios de red dejan de ser accesibles, los datos de medida no se perderán. El proceso de medición debería detenerse para evitar la pérdida de datos de medida.

Nota: Debería considerarse distinguir entre las mediciones estáticas y las dinámicas.

Ejemplo:

(I)/(II) El dispositivo emisor espera a que el receptor confirme la recepción correcta del conjunto de datos. El dispositivo emisor conserva el conjunto de datos en una memoria intermedia (*buffer*) hasta que se recibe la confirmación. La memoria intermedia puede tener capacidad para más de un conjunto de datos organizados como una cola FIFO[5)].

[5)] Sigla del inglés *first in-first out* (primero en entrar, primero en salir).

5.2.3.7 Registro de fecha y hora

El registro de fecha y hora se leerá del reloj del dispositivo. En función del tipo de instrumento, o del área de aplicación, ajustar el reloj puede ser legalmente relevante y se deben utilizar métodos de protección adecuados según el nivel de severidad aplicable (véase el apartado 5.1.3.2.c).

El reloj interno de un instrumento de medida autónomo tiende a tener una gran incertidumbre, ya que no existen medios para sincronizarlo con el reloj global. No obstante, si para un campo de aplicación específico se necesita información relativa al tiempo de medición, la fiabilidad del reloj interno del instrumento de medida se debe aumentar con medios específicos.

Ejemplo:

(II) La fiabilidad del dispositivo del reloj controlado por cuarzo del instrumento de medida se aumenta mediante redundancia: el reloj del microcontrolador, derivado de otro cristal de cuarzo, incrementa un temporizador. Cuando el valor del temporizador alcanza un valor preprogramado, p. ej. 1 segundo, se activa un *flag* específico del microcontrolador y una rutina de interrupción del programa incrementa un segundo contador. Al final de, por ejemplo un día, el software lee el dispositivo del reloj controlado por cuarzo y calcula la diferencia en los segundos contados por el software. Si la diferencia se encuentra dentro de los límites predefinidos, el contador de software se reestablece y el procedimiento se repite. Pero si la diferencia excede los límites, el software reacciona de forma adecuada ante el error.

5.2.4 Compatibilidad de los sistemas operativos y del hardware, portabilidad

5.2.4.1 El fabricante identificará el entorno adecuado de hardware y software. Éste establecerá los recursos mínimos y la configuración adecuada (p. ej. procesador, RAM, HDD, comunicación específica, versión de sistema operativo, etc.) necesarios para el correcto funcionamiento y se describirán en el certificado de aprobación de modelo.

5.2.4.2 Se deben incluir medios técnicos en el software legalmente relevante para evitar la operación si no se cumplen los requisitos mínimos de configuración. El sistema se utilizará únicamente en el entorno especificado por el fabricante para asegurar su buen funcionamiento.

Por ejemplo, si para el correcto funcionamiento del sistema se especifica un entorno invariante, se aplicarán métodos para mantener fijo el entorno operativo. En concreto, lo anterior se aplica a un ordenador universal que lleva a cabo funciones legalmente relevantes.

Se considerará fijar el hardware, el sistema operativo o la configuración del sistema de un ordenador universal, o incluso excluir el uso de un ordenador universal listo para usar en los siguientes casos:

- si se requiere un grado de conformidad alto (véase el apartado 5.2.5.d);
- si se requiere un software fijo (p. ej. el apartado 5.2.6.3.b en el caso de actualización de software rastreada);
- si se deben implementar algoritmos criptográficos o claves (véase el apartado 5.2.3).

5.2.5 Conformidad de los dispositivos fabricados con el modelo aprobado

El fabricante producirá los dispositivos y el software legalmente relevante según el modelo aprobado y la documentación remitida. Existen distintos niveles de conformidad exigibles:

(a) identidad de las «funciones legalmente relevantes» descritas en la documentación (6.1) de cada dispositivo con las del modelo (el código ejecutable puede ser distinto);

(b) identidad de las «partes del código fuente legalmente relevante» y el resto del software legalmente relevante cumpliendo con (a);

(c) identidad del «código fuente legalmente relevante íntegro»;

(d) identidad del «código ejecutable íntegro».

La Recomendación correspondiente especificará el grado de conformidad adecuado. Dicha Recomendación también puede definir un subconjunto de estos grados de conformidad.

Excepto para el nivel (d) puede existir una parte del software sin requisitos de conformidad, siempre que esté separada de la parte legalmente relevante de acuerdo con el apartado 5.2.1.2.

Para demostrar la conformidad se deben proporcionar los medios descritos en los apartados 5.1.1 y 5.2.1.

Nota: Los puntos (a) y (b) se deberían aplicar para el nivel de severidad normal, así como (c) y (d) para el nivel de severidad alto.

5.2.6 Mantenimiento y reconfiguración

La actualización del software legalmente relevante de un instrumento de medida en campo debería considerarse como:

- una modificación del instrumento de medida, cuando el software se sustituye por otra versión aprobada;
- una reparación del instrumento de medida, cuando se vuelve a instalar la misma versión.

En función de la normativa nacional puede ser necesaria una verificación inicial o periódica, si se modifica o repara un instrumento de medida en servicio.

El software que no sea necesario para el correcto funcionamiento del instrumento de medida no requiere verificación después de haber sido actualizado.

5.2.6.1 Únicamente se autoriza el uso de las versiones del software legalmente relevante que están en conformidad con el modelo aprobado (véase el apartado 5.2.5). La aplicabilidad de los siguientes requisitos depende del tipo de instrumento y se debe definir en la Recomendación OIML pertinente. Ésta puede diferir en función del tipo de instrumento en cuestión. Las opciones de los siguientes apartados 5.2.6.2 y 5.2.6.3 constituyen alternativas equivalentes. Todo lo anterior concierne a la verificación en campo. Véase el apartado 7 para consultar más limitaciones.

5.2.6.2 Actualización verificada

El software a actualizar se puede cargar a nivel local, es decir, directamente en el dispositivo de medida o remotamente a través de una red. La carga y la instalación pueden constituir dos etapas distintas (como se describe en la Figura 1) o pueden combinarse en una, en función de las necesidades de la solución técnica. Una persona debería estar presente en el lugar de instalación del instrumento de medida para verificar la eficacia de la actualización. Después de actualizar el software legalmente relevante de un instrumento de medida (sustitución por otra versión aprobada o nueva instalación), no está permitido utilizarlo con fines legales antes de haberlo verificado, tal y como se describe en el apartado 7, ni antes de haber renovado los medios de seguridad (si no consta de otro modo en la Recomendación OIML pertinente o en el certificado de aprobación).

5.2.6.3 Actualización rastreada

El software se implementa en el instrumento según los requisitos de la Actualización rastreada (véanse los apartados del 5.2.6.3.a al 5.2.6.3.g), si cumple con la Recomendación OIML pertinente. La Actualización rastreada es aquel proceso de modificación del software de un instrumento o dispositivo verificado, después del cual no es necesario que una persona responsable realice la verificación periódica in situ. El software a actualizar se puede cargar localmente, es decir, directamente en el instrumento de medida o remotamente a través de una red. La actualización del software queda registrada en un registro de actividades (véase el apartado 3.1.2). El proceso de Actualización rastreada comprende diversas etapas: carga, comprobación de integridad, comprobación del origen (autenticación), instalación, registro y activación.

5.2.6.3.a La Actualización rastreada del software será automática. Al finalizar el proceso de actualización el entorno de protección del software estará al mismo nivel que el requerido en la aprobación de modelo.

5.2.6.3.b El instrumento de medida de destino (dispositivo electrónico, subconjunto) tendrá un software legalmente relevante fijo que no se puede

actualizar e incluirá cada una de las funciones de comprobación necesarias para cumplir todos los requisitos de la Actualización rastreada.

5.2.6.3.c Se deben utilizar medios técnicos para garantizar la autenticidad del software cargado, es decir, que este proviene del propietario del certificado de aprobación de modelo. Si el software cargado no supera el control de autenticidad, el instrumento lo descartará y utilizará la versión anterior del software o cambiará a un modo inoperante.

Ejemplo:

(II) La comprobación de autenticidad se lleva a cabo con métodos criptográficos, como un sistema de clave pública. El propietario del certificado de aprobación de modelo (por lo general el fabricante del instrumento de medida) genera una firma electrónica del software a actualizar utilizando la «clave secreta» en las instalaciones. La «clave pública» se almacena en la parte del software fijo del instrumento de medida. La firma se comprueba utilizando la «clave pública» cuando el software se carga en el instrumento de medida. Si la firma del software cargado es correcta, se instala y activa; si no supera la comprobación, el software fijo la descarta y utiliza la versión anterior del software o cambia a un modo inoperante.

5.2.6.3.d Se deben utilizar medios técnicos para asegurar la integridad del software cargado, es decir, que no ha sido modificado de forma inadmisible antes de la carga. Esta operación puede llevarse a cabo añadiendo una suma de comprobación o un código *hash* del software cargado y comprobándolo durante el procedimiento de carga. Si el software cargado no supera este ensayo, el instrumento lo descartará y utilizará la versión anterior del software o cambiará a un modo inoperante. En este modo, se inhiben las funciones de medición. Únicamente será posible reanudar el procedimiento de descarga, sin omitir ningún paso del diagrama de flujo de la Actualización rastreada.

5.2.6.3.e Se deben utilizar medios técnicos adecuados, por ejemplo un registro de actividades, con el fin de garantizar que la trazabilidad en el instrumento de las Actualizaciones rastreadas del software legalmente relevante es adecuada para verificaciones periódicas, vigilancia o inspección.

El registro de actividades incluirá como mínimo la siguiente información: proceso de actualización aprobado/rechazado, identificación del software de la versión instalada, identificación del software de la versión previamente instalada, registro de fecha y hora del suceso, identificación de la parte que realiza la descarga. Para cada intento de actualización se genera una entrada, independientemente del resultado.

El dispositivo de almacenamiento utilizado para la Actualización rastreada tendrá capacidad suficiente para garantizar la trazabilidad de las Actualizaciones rastreadas del software legalmente relevante entre al menos dos verificaciones sucesivas in situ/ inspección. Tras alcanzar el límite de almacenamiento para el

registro de actividades, se garantizará con medios técnicos la imposibilidad de realizar descargas posteriores sin romper un precinto.

Nota: Este requisito permite a las autoridades de vigilancia, responsables de la supervisión metrológica de los instrumentos controlados legalmente, hacer un seguimiento de las Actualizaciones rastreadas del software legalmente relevante durante un período de tiempo adecuado (en función de la legislación nacional).

5.2.6.3.f En función de las necesidades y de la legislación nacional, puede ser necesario que el usuario o propietario del instrumento de medida dé su consentimiento para realizar la descarga. El instrumento de medida debe disponer de un dispositivo electrónico / subconjunto que permita al usuario o al propietario expresar su consentimiento, p. ej. un botón a pulsar antes de iniciar la descarga. Se debe poder habilitar y deshabilitar este dispositivo electrónico / subconjunto, p. ej. mediante un interruptor que se pueda precintar o mediante un parámetro. Si el dispositivo electrónico / subconjunto está habilitado, serán el usuario o el propietario quienes inicien las descargas. Si está deshabilitado no es necesario que el usuario o el propietario lleven a cabo ninguna acción para realizar la descarga.

5.2.6.3.g Si los requisitos del apartado 5.2.6.3.a al apartado 5.2.6.3.f no pueden cumplirse, sigue siendo posible actualizar la parte legalmente no relevante del software. En tal caso, deben cumplirse los siguientes requisitos:

- existe una separación definida entre el software legalmente relevante y el no relevante de acuerdo con el apartado 5.2.1;
- la parte legalmente relevante del software no se puede actualizar sin romper un precinto;
- en el certificado de aprobación de modelo consta que la actualización de la parte legalmente no relevante es posible.

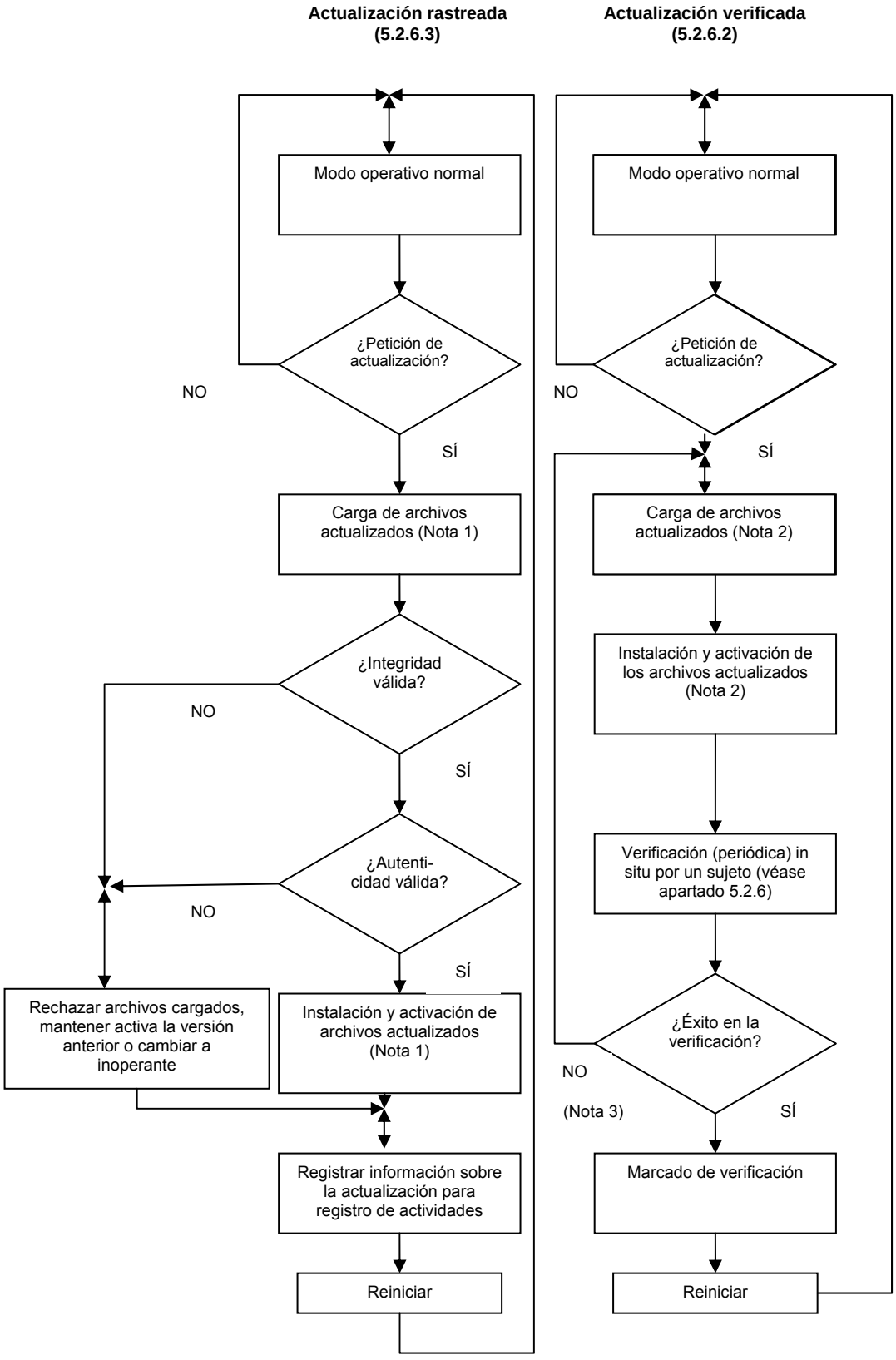

Figura 1 Procedimiento de actualización del software

Notas: (1) El proceso de Actualización rastreada consta de dos etapas: «carga» e «instalación/activación». Ello implica que el software se almacene temporalmente tras la carga sin ser activado, ya que si la comprobación falla debe ser posible descartar el software cargado y recuperar la versión antigua.

(2) En una Actualización verificada, el software también se puede cargar y almacenar temporalmente antes de su instalación, pero en función de la solución técnica la carga y la instalación también pueden realizarse en un solo paso.

(3) En este caso, únicamente se consideran aquellos fallos de verificación resultantes de la actualización del software. Los fallos debidos a otros motivos no requieren la recarga o reinstalación del software, que se simbolizan con la bifurcación NO.

5.2.6.4 La Recomendación OIML pertinente puede requerir que el usuario tenga la posibilidad de realizar el ajuste de ciertos parámetros específicos del dispositivo. En tal caso, el instrumento de medida debe disponer de herramienta con el objeto de registrar automática y permanentemente cualquier ajuste del parámetro específico del dispositivo, p. ej. un registro de actividades. El instrumento debe tener capacidad para presentar los datos registrados.

Nota: Un contador de sucesos no se considera una solución aceptable.

5.2.6.5 Los medios y los registros de la trazabilidad forman parte del software legalmente relevante y deberían protegerse como tales. El software utilizado para visualizar el registro de actividades (véanse los apartados 5.2.6.2; 5.2.6.3) pertenece al software fijo legalmente relevante.

6 Aprobación de modelo

6.1 Documentación necesaria para la aprobación de modelo

Para llevar a cabo la aprobación de modelo, el fabricante del instrumento de medida debe declarar y documentar todas las funciones del programa, las estructuras de datos relevantes, así como las interfaces del software de la parte legalmente relevante implementadas en el instrumento. No deben existir funciones ocultas sin documentar.

Los comandos y sus efectos deben describirse por completo en la documentación del software con el objeto de remitirlos en la aprobación de modelo. El fabricante debe declarar la completitud de la documentación de los comandos. Si éstos pueden introducirse a través de la interfaz de usuario, se deben describir íntegramente en la documentación del software a comprobar en la aprobación de modelo.

Además, la solicitud de la aprobación de modelo debe ir acompañada de un documento, u otras pruebas, que fundamenten que el diseño y las características del software del instrumento de medida cumplen los requisitos de la

Recomendación OIML pertinente en la que se han incorporado los requisitos generales de este Documento.

6.1.1 La documentación habitual (para cada instrumento de medida, dispositivo electrónico o subconjunto) consiste básicamente en:

- una descripción del software legalmente relevante y del modo en que se cumplen los requisitos:
  - una enumeración de los módulos de software que pertenecen a la parte legalmente relevante (Anexo B), incluyendo una declaración de que todas la funciones legalmente relevantes constan en la descripción;
  - una descripción de las interfaces del software de la parte legalmente relevante del mismo, así como de los comandos y el flujo de datos a través de esta interfaz, incluyendo una declaración de completitud (Anexo B);
  - una descripción de la generación de la identificación del software;
  - en función del método de validación escogido en la Recomendación OIML pertinente (véanse los apartado 6.3 y 6.4), la autoridad responsable de la inspección dispondrá del código fuente si la Recomendación OIML relevante requiere de un grado alto de conformidad o protección;
  - una lista de parámetros que se deben proteger y una descripción de los medios de protección;
- una descripción de la configuración del sistema adecuada y de los mínimos recursos necesarios (véase el apartado 5.2.4);
- una descripción de los medios de seguridad del sistema operativo (contraseña, etc., si procede);
- una descripción del método o los métodos de precintado (del software);
- una visión general del hardware del sistema, p. ej. diagrama topológico de bloques, tipo de ordenador(es), tipo de red, etc. También se debería identificar si un componente del hardware se considera legalmente relevante o si lleva a cabo funciones legalmente relevantes;
- una descripción de la exactitud de los algoritmos (p. ej. filtrado de los resultados de conversión A/D, cálculo de precios, algoritmos de redondeo, etc.);
- una descripción de la interfaz de usuario, los menús y los diálogos;
- la identificación del software y las instrucciones para obtenerla en un instrumento en servicio;

- listado de comandos de cada interfaz hardware del instrumento de medida / dispositivo electrónico / subconjunto incluyendo una declaración de completitud;

- listado de errores de durabilidad detectados por el software y, si es necesario para su entendimiento, una descripción de los algoritmos de detección;

- una descripción de los conjuntos de datos almacenados o transmitidos;

- una lista de fallos detectados y una descripción del algoritmo de detección, si en el software se dispone de un sistema de detección de fallos;

- manual de uso.

6.2 Requisitos del procedimiento de aprobación de modelo

En el marco de la aprobación de modelo, los procedimientos de ensayo, los descritos en la OIML D 11:2004, se basan en configuraciones y condiciones de ensayo bien definidas que además pueden contar con mediciones comparativas precisas. El «ensayo» y la «validación» del software son actividades distintas. En general, la exactitud o adecuación del software no puede medirse en un sentido metrológico, aunque existen normas que indican el modo de «medir» la calidad del software (p. ej. ISO/IEC 14598). Los procedimientos aquí descritos consideran tanto las necesidades de la metrología legal como los ya conocidos métodos de validación y de ensayo de la ingeniería del software, aunque estos últimos no tengan la misma finalidad (p. ej. un desarrollador de software que busca errores y que a su vez optimiza el rendimiento). Como se muestra en el apartado 6.4, todo requisito de software necesita la adaptación individual de los procedimientos de validación adecuados. El esfuerzo dedicado al procedimiento debería reflejar la importancia del requisito en cuanto a precisión, fiabilidad y protección ante la corrupción.

La finalidad consiste en validar que el instrumento a aprobar cumple con los requisitos de la Recomendación OIML pertinente. En el caso de instrumentos controlados por software el procedimiento de validación comprende exámenes, análisis y ensayos, y además la Recomendación OIML pertinente debe incluir una selección apropiada de métodos descritos más adelante.

A continuación se describen métodos cuyo enfoque se centra en el examen de modelo. Estos no cubren las verificaciones in situ de cada instrumento individual en servicio. Para más información, consúltese el apartado 7 *Verificación*.

Los métodos especificados para la validación del software se describen en el apartado 6.3. En el apartado 6.4 se describen las combinaciones de dichos métodos, que constituyen un procedimiento de validación completo adaptado a todos los requisitos definidos en el apartado 5.

6.3 Métodos de validación (examen del software)

6.3.1 Visión general de los métodos y su aplicación

La selección y la secuencia de los siguientes métodos no están establecidas y pueden variar, en función del caso, en un procedimiento de validación.

Siglas	Descripción	Aplicación	Condiciones previas, herramientas de aplicación	Características especiales para llevar a cabo el proceso
AD	Análisis de la documentación y validación del diseño (6.3.2.1)	Siempre	Documentación	-
VFTM	Validación mediante ensayo funcional de funciones metrológicas (6.3.2.2)	Adecuación de los algoritmos, incertidumbre, algoritmos de compensación y corrección, normas para calcular el precio	Documentación	-
VFTSw	Validación mediante ensayo funcional de funciones software (6.3.2.3)	Funcionamiento correcto de la comunicación, indicación, protección contra el fraude y errores operativos, protección de parámetros, detección fallos	Documentación, herramientas comunes de software	-
DFA	Análisis de flujo metrológico de datos (6.3.2.4)	Separación del software, evaluación de los efectos de los comandos sobre las funciones del instrumento	Código fuente, herramientas comunes de software (procedimiento simple), herramientas (procedimiento sofisticado)	Conocimiento de lenguajes de programación. Necesidad de formación para aplicar el método.
CIWT	Inspección del código y revisión (6.3.2.5)	Todas las finalidades	Código fuente, herramientas comunes de software	Conocimiento de lenguajes de programación, protocolos y otros temas de las TIC.
SMT	Ensayo del módulo de software (6.3.2.6)	Toda finalidad en que la entrada y la salida puedan definirse claramente	Código fuente, entorno de ensayo, herramientas especiales de software	Conocimiento de lenguajes de programación, protocolos y otros temas de las TIC. Necesidad de formación para el uso de herramientas.

Cuadro 1: Visión general de los métodos de validación propuestos y seleccionados

Nota: Los editores de texto, los editores hexadecimales, etc., se consideran «herramientas comunes de software».

6.3.2 Descripción de los métodos de validación seleccionados

6.3.2.1 Análisis de la documentación y la especificación, y validación del diseño (AD)

Aplicación:

Se trata del procedimiento básico aplicable en cualquier situación.

Condiciones previas:

El procedimiento se basa en la documentación del fabricante del instrumento de medida. En función de los requisitos, esta documentación debe tener el enfoque adecuado:

(1) especificación de las funciones del instrumento accesibles externamente de forma general. (Adecuada en instrumentos simples sin interfaces excepto un visualizador, todas las características son verificables mediante ensayos funcionales, riesgo de fraude bajo);

(2) especificación de las funciones del software y las interfaces (necesaria en instrumentos con interfaces y en funciones de instrumentos que no pueden someterse a ensayo de forma funcional y cuando el riesgo de fraude es alto). La descripción mostrará y explicará toda función del software que pueda repercutir en las características metrológicas;

(3) en lo relativo a las interfaces, la documentación incluirá una lista completa de comandos o señales que el software puede interpretar. El efecto de cada comando se debe documentar detalladamente. Se describirá la reacción del instrumento ante comandos no documentados.

(4) si resulta necesario para comprender y evaluar las funciones del software, se aportará documentación adicional del mismo para comprender y evaluar algoritmos de medida complejos, funciones criptográficas o restricciones de tiempo determinantes;

(5) cuando el modo de validación de la función de un programa de software no sea evidente, el fabricante tiene la responsabilidad de desarrollar un método de ensayo. Además, los servicios del programador deberían estar a disposición del evaluador con la finalidad de dar respuesta a las preguntas.

Una condición previa general para llevar a cabo el examen es la completitud de la documentación y la identificación clara del EUT; es decir, de los paquetes de software que contribuyen a las funciones metrológicas (véase el apartado 6.1.1).

Descripción:

El examinador evalúa las funciones y las características del instrumento de medida utilizando la descripción verbal y las representaciones

gráficas, y decide si éstas cumplen con los requisitos de la Recomendación OIML pertinente. Los requisitos metrológicos, así como los requisitos funcionales del software definidos en el apartado 5 (p. ej. protección contra el fraude, protección de los parámetros de ajuste, funciones anuladas, comunicación con otros dispositivos, actualización del software, detección de fallos, etc.) se deben considerar y evaluar. El Formato del informe de evaluación de software puede facilitar esta tarea (véase el Anexo B).

Resultado

El procedimiento da un resultado para todas las características del instrumento de medida, siempre que el fabricante haya remitido la documentación adecuada. El resultado debería ir documentado en una sección relacionada con el software en un Informe de evaluación de software (véase el Anexo B) incluido en el Formato de informe de evaluación de la Recomendación OIML pertinente.

Procedimientos complementarios:

Si el examen de la documentación no puede aportar resultados de validación corroborados, deberían aplicarse procedimientos adicionales. En la mayoría de los casos “Validar las funciones metrológicas por análisis funcional” (véase el apartado 6.3.2.2.) es un procedimiento complementario.

Referencias:

FDA, Guidance for FDA Reviewers and Industry Guidance for the Content of Premarket Submissions for Software Container in Medical Devices, 29 de mayo de 1998 [10]; IEC 61508-7, 2000-3[9].

6.3.2.2 Validación mediante ensayo funcional de las funciones metrológicas (VFTM)

Aplicación:

Adecuación de algoritmos para el cálculo del valor de medida de datos sin procesar, para la linealización de una característica, compensación de influencias medioambientales, redondeo en el cálculo del precio, etc.

Condiciones previas:

Manual de funcionamiento, patrón de funcionamiento, referencias metrológicas y equipamiento de ensayo.

Descripción:

La mayoría de los métodos de aprobación de modelo y de ensayo descritos en las Recomendaciones OIML se basan en medidas de referencia en diversas condiciones. Su aplicación no está restringida a

una tecnología en particular del instrumento. Aunque en principio no esté destinada a validar el software, el resultado del ensayo se puede interpretar como una validación de algunas partes del mismo, suele ser incluso la más importante desde el punto de vista metrológico. Si los ensayos descritos en la Recomendación OIML pertinente abarcan todas las características metrológicamente relevantes del instrumento, las partes del software correspondientes pueden considerarse validadas. Por lo general, no se debe aplicar ningún análisis o ensayo de software adicional para validar las características metrológicas de los instrumentos de medida.

Resultado:

La adecuación de los algoritmos es válida cuando los valores de medida están dentro del EMP bajo cualquier condición, de lo contrario es inválida.

Procedimientos complementarios:

El método suele ser una mejora del apartado 6.3.2.1. En ciertos casos puede resultar más fácil o efectivo combinar el método con exámenes basados en el código fuente (6.3.2.5) o simulando las señales de entrada (6.3.2.6); p. ej. en mediciones dinámicas.

Referencias:

Varias Recomendaciones OIML específicas.

6.3.2.3 Validación mediante el ensayo funcional de las funciones del software (VFTSw)

Aplicación:

Validación, por ejemplo, de la protección de parámetros, la indicación de una identificación del software, la detección de fallos mediante software, la configuración del sistema (especialmente del entorno del software), etc.

Condiciones previas:

Manual de funcionamiento, documentación del software, patrón de funcionamiento, equipo de ensayo.

Descripción:

En la práctica se comprueban las características requeridas descritas en el manual de funcionamiento, en la documentación del instrumento o en la documentación del software. Si están controladas por software, deben considerarse como validadas si su funcionamiento es correcto sin análisis de software posteriores. Las características a las que se hace referencia son, por ejemplo:

- el funcionamiento normal del instrumento, si el funcionamiento está controlado por software. Se deberían utilizar todos los interruptores o las teclas, así como las combinaciones descritas, y evaluar la reacción del instrumento. En las interfaces gráficas del usuario, se deberían activar y comprobar todos los menús y otros elementos gráficos;

- la efectividad de la protección de parámetros puede comprobarse activando los medios de protección e intentando modificar un parámetro;

- la efectividad de la protección de los datos almacenados puede comprobarse modificando algunos datos del archivo y, posteriormente, comprobando si el programa lo detecta;

- la generación y la indicación de la identificación del software se pueden validar mediante una comprobación práctica;

- si la detección de fallos se realiza mediante software, las partes relevantes del software se pueden validar provocando, implementando o simulando un fallo y comprobando si la reacción del instrumento es correcta;

- si se afirma que la configuración o el entorno del software legalmente relevante es fijo, se pueden comprobar los métodos de protección realizando modificaciones no autorizadas. El software las debería inhibir o detener el funcionamiento.

Resultado:

La característica controlada por software en cuestión es correcta o no.

Procedimientos complementarios:

En la práctica, algunas características o funciones de un instrumento controlado por software no se pueden validar como se describe. Si el instrumento tiene interfaces, por lo general, no es suficiente probar comandos aleatoriamente para detectar comandos no autorizados. Además es necesario que un emisor los genere. Para un nivel de validación normal, el método del apartado 6.3.2.1, junto con una declaración del fabricante, puede satisfacer este requisito. Para incrementar el nivel de examen, es necesario realizar un análisis del software como el de los apartados 6.3.2.4 ó 6.3.2.5.

Referencia:

FDA Guidance for Industry Parte 11, agosto de 2003 [11]; *WELMEC Guide 2.3* [12]; *WELMEC Guide 7.2* [13].

6.3.2.4 Análisis del flujo de datos metrológicos (DFA)

Aplicación:

Configuración del flujo de valores de medida a través de los dominios de datos sujetos al control legal. Examen de la separación del software.

Condiciones previas:

Documentación del software, código fuente, editor, buscador de texto o herramientas especiales. Conocimiento de lenguajes de programación.

Descripción:

Este método pretende localizar todas las partes del software involucradas en el cálculo de valores de medida o con posibles repercusiones sobre el mismo. A partir del puerto hardware, donde se puede acceder a los datos de medida sin procesar del sensor, se busca la subrutina que los lee. Esta subrutina los almacenará en una variable, probablemente después de haber realizado algunos cálculos. A partir de esta variable, una subrutina distinta lee un valor intermedio y así sucesivamente, hasta que el valor de medida completo aparece en el dispositivo indicador. Todas las variables utilizadas como almacenamiento para valores de medida intermedios, así como todas las subrutinas que transportan dichos valores, pueden encontrarse en el código fuente utilizando únicamente un editor de texto y un buscador para localizar los nombres de la variable o de la subrutina en otros archivos del código fuente distintos al que está abierto en el editor de texto.

Con este método se pueden encontrar otros flujos de datos; por ejemplo, de las interfaces al intérprete de los comandos recibidos. Además, es posible detectar si se ha eludido la interfaz de un software (véase el apartado 5.2.1.2).

Resultado:

Se puede validar si la separación del software según el apartado 5.2.1.2 es correcta o no.

Procedimientos complementarios:

Este método se recomienda si se ha realizado la separación del software y si se requieren conformidad o protección altas ante la manipulación. Es una mejora de los apartados del 6.3.2.1 al 6.3.2.3 y del 6.3.2.5.

Referencia:

IEC 61131-3.

6.3.2.5 Inspección y revisión del código (CIWT)

Aplicación:

Con este método se puede validar cualquier característica del software si se necesita una intensidad del examen alta.

Condiciones previas:

Código fuente, editor de texto, herramientas. Conocimiento de lenguajes de programación.

Descripción:

El examinador revisa el código fuente de instrucción en instrucción, evaluando la parte respectiva del código para determinar si se cumplen los requisitos y si las funciones del programa y las características están en conformidad con la documentación.

El examinador también puede centrarse en funciones o algoritmos que haya identificado como complejos, proclives a los errores, insuficientemente documentados, etc., e inspeccionar la parte respectiva del código fuente mediante análisis y control.

Antes de llevar a cabo el examen, el examinador habrá identificado la parte legalmente relevante del software; por ejemplo, aplicando el análisis del flujo de datos metrológicos (véase el apartado 6.3.2.4). Por lo general, la inspección del código o la revisión se limitan a esta parte. Combinando ambos métodos, el esfuerzo de examen es mínimo en comparación con la aplicación de los mismos en la producción normal de software con el objetivo de producir programas sin fallos u optimizar el rendimiento.

Resultado:

Implementación compatible con la documentación de software y en conformidad, o no, con los requisitos.

Procedimientos complementarios:

Se trata de un método mejorado, complementario a los apartados 6.3.2.1 y 6.3.2.4. Habitualmente sólo se aplica en los controles en puntos concretos.

Referencia:

IEC 61508-7:2000 – 3 [9].

6.3.2.6 Ensayo de módulo del software (SMT)

Aplicación:

Únicamente si se requiere un nivel alto de conformidad y protección contra el fraude. Este método se aplica cuando las funciones de un programa no se pueden examinar exclusivamente a partir de la información escrita. En la validación de algoritmos de medida dinámicos resulta adecuado y ventajoso económicamente.

Condiciones previas:

Código fuente, herramientas de desarrollo (al menos un compilador), entorno de funcionamiento del módulo de software sometido a ensayos, conjuntos de datos de entrada y el correspondiente conjunto de datos de salida de referencia correcta o herramientas para la automatización. Habilidades TIC, conocimiento de lenguajes de programación. Se recomienda la cooperación con el programador del módulo sometido a ensayo.

Descripción:

El módulo de software sometido a ensayo está integrado en un entorno de pruebas; es decir, un programa de pruebas específico que llama al programa sometido a ensayos y le aporta todos los datos de entrada necesarios. El programa de pruebas recibe datos de salida del módulo sometido a ensayos y los compara con los valores de referencia esperados.

Resultado:

Las funciones o el algoritmo de medición sometidos a ensayo son correctos o no.

Procedimientos complementarios:

Se trata de un método mejorado, complementario a los apartados 6.3.2.2 ó 6.3.2.5. Únicamente es útil en casos excepcionales.

Referencia:

IEC 61508-7:2000 – 3 [9].

6.4 Procedimiento de validación

El procedimiento de validación consiste en una combinación de métodos de análisis y ensayos. La Recomendación OIML pertinente puede especificar detalles relativos al procedimiento de validación, incluyendo los siguientes:

(a) el método de validación de los descritos en el apartado 6.3 que se deberá aplicar para cumplir el requisito en cuestión;

(b) el modo de realizar la evaluación de los resultados del ensayo;

(c) los resultados que deben incluirse en el informe de ensayos y los que deben integrarse en el certificado de ensayos (véase el Anexo B).

En el Cuadro 2 se definen dos niveles alternativos de los procedimientos de validación, denominados A y B. El nivel B implica un nivel de examen más alto en comparación con el A. En la Recomendación OIML pertinente —diferente o igual en cada requisito— se puede hacer una selección entre los procedimientos de validación de modelo A y B, en función de lo que se espere en cuanto a:

- el riesgo de fraude;
- el área de aplicación;
- la conformidad requerida con el modelo aprobado;
- el riesgo de obtener un resultado de medición erróneo debido a errores funcionamiento.

Requisito		Procedimiento de validación A (nivel de examen normal)	Procedimiento de validación B (nivel de examen alto)	Comentarios
5.1.1	Identificación del software	AD + VFTSw	AD + VFTSw + CIWT	Seleccionar “B” si se requiere conformidad alta
5.1.2	Adecuación de algoritmos y funciones	AD + VFTM	AD + VFTM + CIWT/SMT	
Protección del software				
5.1.3.1	Prevención del uso incorrecto	AD + VFTSw	AD + VFTSw	
5.1.3.2	Protección contra el fraude	AD + VFTSw	AD + VFTSw + DFA/CIWT/SMT	Seleccionar “B” en caso de riesgo de fraude alto
Características de hardware				
5.1.4.1	Detección de fallos	AD + VFTSw	AD + VFTSw + CIWT + SMT	Seleccionar “B” si se requiere fiabilidad alta
5.1.4.2	Protección de durabilidad	AD + VFTSw	AD + VFTSw + CIWT + SMT	Seleccionar “B” si se requiere fiabilidad alta
Especificación y separación de las partes relevantes y especificación de las interfaces de las mismas				
5.2.1.1	Separación de dispositivos electrónicos y subconjuntos	AD	AD	
5.2.1.2	Separación de partes del software	AD	AD + DFA/CIWT	
5.2.2	Indicaciones compartidas	AD + VFTM/VFTSw	AD + VFTM/VFTSw + DFA/CIWT	
5.2.3	Almacenamiento de datos, transmisión a través de sistemas de comunicación	AD + VFTSw	AD + VFTSw + CIWT/SMT	Seleccionar “B” si se prevé la transmisión de datos de medida en un sistema abierto
5.2.3.1	El valor de medida almacenado o transmitido irá acompañado de toda la información pertinente que sea necesaria para su uso legalmente relevante en el futuro	AD + VFTSw	AD + VFTSw + CIWT/SMT	Seleccionar “B” en caso de riesgo de fraude alto

Requisito		Procedimiento de validación A (nivel de examen normal)	Procedimiento de validación B (nivel de examen alto)	Comentarios
5.2.3.2	Los datos se protegerán mediante medios software para garantizar su autenticidad, integridad y, si procede, la adecuación de la información relativa al momento de la medición	AD + VFTSw	/	
5.2.3.3	Para obtener un nivel de protección alto es necesario aplicar métodos criptográficos	/	AD + VFTSw + SMT	
5.2.3.4	Almacenamiento automático	AD + VFTSw	AD + VTFSw + SMT	
5.2.3.5	Retraso en la transmisión	AD + VFTSw	AD + VFTSw + SMT	Seleccionar “B” en caso de riesgo de fraude alto, p. ej. transmisión en sistemas abiertos
5.2.3.6	Interrupción de la transmisión	AD + VFTSw	AD + VFTSw + SMT	Seleccionar “B” en caso de riesgo de fraude alto, p. ej. transmisión en sistemas abiertos
5.2.3.7	Registro de fecha y hora	AD + VFTSw	AD + VFTSw + SMT	
5.2.4	Compatibilidad de los sistemas operativos y del hardware, portabilidad	AD + VFTSw	AD + VFTSw + SMT	
Mantenimiento y reconfiguración				
5.2.6.2	Actualización verificada	AD	AD	
5.2.6.3	Actualización rastreada	AD + VFTSw	AD + VFTSw + CIWT/SMT	

Cuadro 2: Recomendaciones para combinar los métodos de análisis y de ensayo aplicables a los diversos requisitos del software (las siglas se definen en el Cuadro 1)

6.5 Equipo sometido a ensayo (EUT)

Por lo general, los ensayos se realizan sobre el instrumento de medida completo (prueba funcional). Si el tamaño o la configuración del instrumento de medida no le permiten realizar el ensayo sobre una unidad completa o si únicamente afecta a un dispositivo (módulo) separado del instrumento de medida, la Recomendación OIML pertinente puede indicar que los ensayos, o algunos en concreto, se lleven a cabo sobre los dispositivos electrónicos o módulos de software por separado, siempre que, cuando los ensayos se realizan sobre dispositivos en funcionamiento, estos formen parte de una simulación lo suficientemente representativa del funcionamiento normal. El solicitante de la aprobación de modelo tiene la responsabilidad proporcionar todo el equipamiento y los componentes requeridos.

7 Verificación

Si el control metrológico de instrumentos de medida es obligatorio en un país determinado, se establecerán métodos para la verificación in situ de la identidad del software durante el funcionamiento, la validez del ajuste y la conformidad con el modelo aprobado.

La Recomendación OIML pertinente puede requerir que la verificación del software se realice en una o más etapas según la naturaleza de instrumento de medida en cuestión.

La verificación del software incluirá:

- un examen de la conformidad del software con la versión aprobada (p. ej. la verificación del número de versión y de la suma de comprobación);
- un examen de la compatibilidad de la configuración con la configuración mínima declarada, si así consta en el certificado de aprobación;
- un examen de la configuración correcta de las entradas/salidas del instrumento de medida en el software cuando su asignación sea un parámetro específico de dispositivo;
- un examen para verificar si los parámetros específicos del dispositivo (especialmente los parámetros de ajuste) son correctos.

Los procedimientos para actualizar el software se describen en los apartados 5.2.6.2 y 5.2.6.3.

8. Evaluación de los niveles de (riesgo) severidad

8.1 En este apartado se pretende proporcionar una guía a la hora de determinar un conjunto de niveles de severidad que generalmente se aplicarán en los ensayos sobre instrumentos de medida electrónicos. El objetivo no consiste en

establecer una clasificación con límites estrictos que conduzcan a requisitos especiales, como en el caso de una clasificación de exactitud.

Además, en esta guía no se impide a los Comités y Subcomités Técnicos crear niveles de severidad distintos de aquellos resultantes de las directrices establecidas en este Documento. Pueden utilizarse distintos niveles de severidad en conformidad con los límites especiales establecidos en las Recomendaciones OIML pertinentes.

8.2 El nivel de severidad de un requisito se debe seleccionar independientemente de un requisito a otro.

8.3 Si se seleccionan niveles de severidad para una categoría en particular de instrumentos y un área de aplicación (el comercio, la venta directa al público, la salud, la aplicación de la ley, etc.), se pueden tener en cuenta los siguientes aspectos:

(a) el riesgo de fraude:

- la consecuencia y el impacto social del mal funcionamiento;
- el valor de los bienes a medir;
- la plataforma utilizada (específica para la aplicación u ordenador universal);
- exposición a fuentes potenciales de fraude (dispositivo de autoservicio).

(b) la conformidad requerida:

- las posibilidades de la industria para cumplir con el nivel establecido en la práctica.

(c) la fiabilidad requerida:

- condiciones medioambientales;
- la consecuencia y el impacto social de los errores.

(d) el interés del defraudador:

- simplemente ser capaz de cometer el fraude puede ser un factor de motivación suficiente.

(e) la posibilidad de repetir una medición o de interrumpirla.

En los requisitos del apartado 5 se presentan varios ejemplos de soluciones técnicas aceptables que ilustran un nivel básico de protección contra el fraude, la conformidad, la fiabilidad y el tipo de medición (marcado con (I)). Cuando procede, también se presentan ejemplos de medidas preventivas mejoradas que consideran un nivel de severidad alto de los aspectos descritos más arriba (marcados con (II)).

El procedimiento de validación y el nivel de (riesgo) severidad están vinculados de forma indefectible. Debe realizarse un análisis profundo del software cuando se requiera un nivel de severidad alto para detectar las deficiencias del propio software o los puntos débiles de la protección. Por otro lado, el precintado mecánico (p. ej. precintado del puerto de comunicación o de la carcasa) debería tenerse en cuenta a la hora de escoger un procedimiento de validación.

Anexo A

Bibliografía

En el momento de la publicación las siguientes ediciones estaban en vigor. Todo documento normativo está sujeto a revisión, no obstante, se invita a los usuarios de este Documento a investigar si existen ediciones más recientes de los documentos normativos y la posibilidad de aplicarlas. Los miembros de la IEC y de la ISO mantienen registros de las Normas Internacionales vigentes.

El estado actual de las Normas señaladas también se puede comprobar en Internet:

Publicaciones de la IEC: http://www.iec.ch/searchpub/cur_fut.htm

Publicaciones de la ISO: http://www.iso.org/iso/iso_catalogue.htm

Publicaciones de la OIML: http://www.oiml.org/publications/

(se pueden descargar archivos PDF gratuitamente).

A fin de evitar cualquier malentendido, se recomienda encarecidamente que toda referencia a las Normas de las Recomendaciones OIML y de los Documentos Internacionales se consulte en la versión indicada (por lo general el año o la fecha).

Ref.	**Normas y documentos de referencia**	**Descripción**
[1]	*International Vocabulary of Basic and General Terms in Metrology (VIM)* (1993)[6)] Vocabulario internacional de términos fundamentales y generales de metrología (VIM) (1994)	Vocabulario elaborado por un grupo de trabajo conjunto de expertos seleccionados por la BIPM, la IEC, la IFCC, la ISO, la IUPAC, la IUPAP y la OIML.
[2]	OIML B 3:2003 *The OIML Certificate System for Measuring Instruments*	El Sistema de certificados OIML para instrumentos de medida es un sistema para emitir, registrar y utilizar Certificados de conformidad OIML para modelos de instrumentos de medida basados en los requisitos de las Recomendaciones OIML.
[3]	OIML D 11:2004 *General requirements for electronic measuring instruments*	Guía para establecer requisitos metrológicos en la realización de ensayos en las magnitudes de influencia que pueden afectar a los instrumentos de medida incluidos en las Recomendaciones Internacionales.

[6)] La JCGM revisó el VIM en 2007. La edición en español se publicó en 2008.

Ref.	Normas y documentos de referencia	Descripción
[4]	ISO/IEC 9594-8:2001 *Information technology -- Open Systems Interconnection -- The Directory: Public key and attribute certificate frameworks*	La ISO/IEC 9594-8:2005 señala tres marcos de trabajo y un número de objetos que pueden utilizarse para autenticar y proteger la comunicación entre dos entidades; p. ej. entre dos entidades de servicio de directorio o entre un buscador web y un servidor web. Los objetos también pueden utilizarse para demostrar la fuente y la integridad de las estructuras de datos como documentos con firma digital.
[5]	ISO 2382-9:1995 *Information technology – Vocabulary Part 9: Data communication*	Su objetivo es facilitar la comunicación internacional de datos. Presenta términos y definiciones de conceptos seleccionados, importantes en el campo de comunicación de datos e identifica relaciones entre las entradas.
[6]	IEC 61508-4:1998-12 *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*	Contiene las definiciones y explicaciones de términos que se utilizan en las partes 1 y 7 de esta Norma. Va dirigida a los Comités técnicos para la elaboración de Normas según los principios incluidos en la Guía IEC 104 y la Guía ISO/IEC 51. La IEC 61508 también se considera una Norma independiente.
[7]	Serie ISO/IEC 14598 *Information technology – Software product evaluation*	La serie de Normas ISO/IEC 14598 aporta métodos de medición, valoración y evaluación de la calidad del producto software. En ella no se describen métodos para la evaluación de los procesos de producción software ni métodos para la predicción de costes (la medición de la calidad de los productos de software puede, evidentemente, utilizarse para ambos objetivos).
[8]	V 1:2000 International vocabulary of terms in legal metrology (VIML)	El VIML contiene únicamente aquellos conceptos utilizados en el campo de la metrología legal. Están relacionados con las actividades, los documentos relevantes y otros temas vinculados a los servicios de metrología legal. Además este Vocabulario incluye ciertos conceptos de carácter general extraídos del VIM.
[9]	IEC 61508-7:2000 – 3 *Functional safety of electrical/electronic/programmable electronic safety related systems - Part 5: Examples of methods for the determination of safety integrity levels* Seguridad funcional de los sistemas eléctricos/electrónicos/electrónicos programables relacionados con la seguridad. Parte 7: Presentación de técnicas y medidas.	Contiene información sobre los conceptos subyacentes del riesgo y la relación de riesgo con la integridad de seguridad (véase el Anexo A); un número de métodos que permite determinar los niveles de integridad de seguridad para los sistemas relacionados con la seguridad E/E/PE, otros sistemas tecnológicos relacionados con la seguridad e instalaciones de reducción de riesgo externo (véanse los Anexos B, C, D y E). Va dirigida a los Comités técnicos a la hora de elaborar Normas de acuerdo con los principios de la Guía IEC 104 y de la Guía ISO/IEC 51.
[10]	*FDA, Guidance for FDA Reviewers and Industry Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices*, 29 de mayo de 1998	Con este documento guía se pretende proporcionar información a la industria con respecto a la documentación que la FDA recomienda incluir en las propuestas previas a la comercialización de dispositivos software, incluyendo aplicaciones de software autónomas y dispositivos basados en hardware que incorporan software.

Ref.	Normas y documentos de referencia	Descripción
[11]	*FDA Guidance for Industry* Parte 11, agosto de 2003	En este documento se pretende proporcionar información a personas que han escogido mantener registros o remitir información designada electrónicamente y, como resultado, la Parte 11 se aplica a registros en formato electrónico que se crean, modifican, mantienen, archivan, recuperan o transmiten con cualquier requisito de registro establecido en la normativa de la US Agency
[12]	*WELMEC Guide* 2.3, mayo de 2005(3ª edición) *Guide for Examining Software (Weighing Instruments)*	
[13]	*WELMEC Guide* 7.2, mayo de 2008 (3ª edición) *Software Guide (Measuring Instruments Directive 2004/22/EC)*	En este documento se presenta una guía para todas aquellas personas relacionadas con la aplicación de la Directiva relativa a Instrumentos de Medida (Directiva Europea 2004/22/CE; MID), en particular para los instrumentos de medida equipados con software. Va dirigida a fabricantes de instrumentos de medida y organismos notificados responsables de la evaluación de conformidad de los instrumentos de la MID. Siguiendo la Guía, puede asumirse el cumplimiento de los requisitos relacionados con el software de la MID.

Anexo B

Ejemplo de informe de evaluación de un software (Informativo)

Nota: Los Comités y Subcomités técnicos que elaboran las Recomendaciones OIML deberían decidir la información que se incluirá en el Informe de ensayos y el Certificado de conformidad OIML. Por ejemplo, el Certificado de ensayos debería incluir el nombre, la versión y la suma de comprobación del archivo ejecutable del siguiente ejemplo.

Informe de ensayo nº XYZ122344

Validación del software del caudalímetro Tournesol Metering **modelo** TT100

El software del instrumento de medida se validó para demostrar el cumplimiento de los requisitos de la Recomendación OIML R-xyz.

La validación se basó en el informe del Documento internacional OIML D 31:2008, donde se interpretan y explican los requisitos principales del software. Este informe describe el examen del software necesario para cumplir con la R-xyz.

Fabricante	Solicitante
Tournesol Metering	New Company
P.O Box 1120333	Nova Street 123
100 Klow	1000 Las Dopicos
Referencia: Mr. Tryphon Tournesol	Referencia: Archibald Haddock

Objeto del ensayo

El caudalímetro Tournesol Metering TT100 es un instrumento de medida cuya función consiste en medir el caudal de líquidos. El rango de medida va desde 1 l/s y 2000 l/s. Las funciones básicas del instrumento son las siguientes:

- medición del caudal de líquidos,
- indicación del volumen medido,
- interfaz con el transductor.

El caudalímetro se describe como un instrumento de medida desarrollado específicamente (sistema integrado) con un dispositivo de almacenamiento de datos legalmente relevantes.

El caudalímetro TT100 es un instrumento independiente con un transductor conectado. El transductor incorpora compensación de temperatura. Es posible ajustar el caudal con parámetros de calibración almacenados en una memoria permanente del transductor. Está fijado al instrumento y no puede desconectarse. El volumen medido se indica en un visualizador. No es posible establecer comunicación con otros dispositivos.

El software integrado del instrumento de medida ha sido desarrollado por:

Tournesol Meterin, P.O. Box 112033, 100 Klow, Syldavie.

El nombre ejecutable del archivo es **"tt100_12.exe"**.

La versión validada de este software es **V1.2c**. La versión del software se presenta en el dispositivo indicador durante el arranque del dispositivo y pulsando el botón de "nivel" durante 4 segundos.

El código fuente contiene los siguientes archivos legalmente relevantes:

- main.c 12301 bytes 23 de nov. de 2003;
- int.c 6509 bytes 23 de nov. de 2003;
- filter.c 10897 bytes 20 de oct. de 2003;
- input.c 2004 bytes 20 de oct. de 2003;
- display.c 32000 bytes 23 de nov. de 2003;
- ethernet.c 23455 bytes 15 de junio de 2002;
- driver.c 11670 bytes 15 de junio de 2002;
- calculate.c 6788 bytes 23 de nov. de 2003.

El archivo ejecutable **"tt100_12.exe"** está protegido contra modificaciones mediante una suma de comprobación. El valor de esta suma de comprobación por algoritmo **XYZ** es **1A2B3C**.

La validación se ha basado en los siguientes documentos del fabricante:

- Manual de usuario 1.6 del TT100;
- Manual de mantenimiento 1.1 del TT100;
- Descripción del software del TT100 (documento de diseño interno, con fecha del 22 de noviembre de 2003);
- Diagrama del circuito electrónico TT100 (dibujo nº 222-31, con fecha del 15 de octubre de 2003).

La versión definitiva del objeto de ensayo se entregó al National Testing & Measurement Laboratory el 25 de noviembre de 2003.

Realización de la validación

La validación se llevó a cabo según la OIML D 31:2008 y se realizó entre el 1 de noviembre y el 23 de diciembre de 2003. El Dr. K. Fehler dirigió una revisión de diseño el 3 de diciembre en la oficina central de Tournesol Metering en Klow. En el National Testing & Measurement Laboratory el Dr. K. Fehler y el Sr. S. Problème llevaron a cabo otro proceso de validación.

Se validaron los siguientes requisitos:

- identificación del software;
- adecuación de algoritmos y funciones;
- protección del software;
- prevención contra el uso incorrecto;
- protección contra el fraude;
- características de software;
- almacenamiento de datos, transmisión por sistemas de comunicación.

Se aplicaron los siguientes métodos de validación:

- análisis de la documentación y validación del diseño;
- validación por ensayo funcional de las características metrológicas;
- revisión, inspección del código;
- ensayo del módulo de software del módulo calculate.c con SDK XXX.

Resultado

Se han validado sin encontrar fallos los siguientes requisitos de la OIML D 31:2008:

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.

Se encontraron dos comandos que no se habían descrito inicialmente en el manual de funcionamiento. Ambos se han incluido en el manual del 10 de diciembre de 2003.

En el paquete informático V1.2b se localizó un fallo de software que limitaba el mes de febrero a 28 días, incluidos los años bisiestos. Este fallo se ha corregido en el paquete V1.2c.

El resultado sólo se aplica al ítem sometido a ensayo con número de serie 1188093-B-2004.

Conclusión

El software de **Tournesol Metering TT100 V1.2c** cumple con los requisitos de la OIML R-xyz.

National Testing & Measurement Lab.

Software Department

Dr. K.E.I.N. Fehler Sr. S.A.N.S. Problème

Director técnico Responsable técnico

Lista de comprobación

Apartado	Requisito	Aceptado	Rechazado	Comentarios
5.1	**Requisitos generales**			
5.1.1	**Identificación del software** El software legalmente relevante se debe identificar claramente.			
5.1.2	**Adecuación de algoritmos y funciones** Los algoritmos de medida y las funciones de un dispositivo deben ser adecuados.			
5.1.3	**Protección del software**			
5.1.3.1	**Prevención del uso incorrecto** Un instrumento de medida debe fabricarse de modo que las posibilidades de hacer un uso incorrecto intencionado, accidental o no intencionado sean mínimas.			
5.1.3.2 **a)**	**Protección contra el fraude** El software legalmente relevante se protegerá contra modificaciones no autorizadas, cargas o cambios derivados de la sustitución del dispositivo de memoria. Además del precintado mecánico, con el objeto de proteger instrumentos de medida con un sistema operativo o con una opción para la carga de software, se pueden necesitar medios técnicos.			
b)	La interfaz de usuario únicamente puede activar aquellas funciones claramente documentadas (véase el apartado 6.1). La interfaz de usuario se implementará de modo que no facilite el uso fraudulento. La presentación de la información cumplirá con lo establecido en el apartado 5.2.2.			
c)	Los parámetros que fijan las características legalmente relevantes del instrumento de medida deben estar protegidos contra modificaciones no autorizadas. Si es necesario para llevar a cabo la verificación, el valor actual de los parámetros se debe poder visualizar o imprimir.			
d)	La protección del software incluye un precintado adecuado a través de medios mecánicos, electrónicos y/o criptográficos, que imposibilita o muestra una intervención no autorizada.			
5.1.4	**Características del hardware**			

Apartado	Requisito	Aceptado	Rechazado	Comentarios
5.1.4.1	**Detección de fallos** Se requerirá al fabricante del instrumento diseñar herramientas de comprobación en las partes del software o del hardware, o bien aportar medios a través de los cuales partes del software del instrumento puedan ayuda al funcionamiento de las partes del hardware.			
5.1.4.2	**Protección de la durabilidad** El fabricante puede elegir implementar los sistemas de protección de la durabilidad bien en el software o en el hardware, o permitir que el software respalde el funcionamiento de los sistemas hardware.			
5.2 **5.2.1**	**Requisitos específicos** **Especificación y separación de las partes relevantes y especificación de las interfaces de las mismas** Las partes de un sistema de medida críticas en cuanto a la metrología no se deben ver influenciadas más allá de lo admisible por otras partes del sistema de medida.			
5.2.1.1 **a)**	**Separación de dispositivos electrónicos y subconjuntos** Los subconjuntos o dispositivos electrónicos de un sistema de medida que lleva a cabo funciones legalmente relevantes se deben identificar, definir claramente y documentar.			
b)	Durante el ensayo de modelo, se debe demostrar que los comandos recibidos a través de la interfaz no pueden influir de forma inadmisible en los datos y las funciones relevantes de los subconjuntos y dispositivos electrónicos.			
5.2.1.2 **a)**	**Separación de partes del software** El requisito de conformidad se aplica a la parte legalmente relevante del software de un instrumento de medida (véase el apartado 5.2.5) y debe identificarse como se describe en el apartado 5.1.1.			
b)	Si la parte legalmente relevante del software se comunica con otras partes del mismo, se debe definir una interfaz software. Toda la comunicación se debe desarrollar exclusivamente a través de esta interfaz. La parte legalmente relevante del software y la interfaz deben estar claramente documentadas. Todas las funciones y los dominios de datos legalmente relevantes del software se deben describir con el objeto de permitir a una autoridad de aprobación de modelo decidir si la separación del software es correcta.			

Apartado	Requisito	Aceptado	Rechazado	Comentarios
c)	Cada comando debe asignarse de forma inequívoca a funciones iniciadas o modificaciones de datos en la parte legalmente relevante del software. Los comandos comunicados a través de la interfaz software se deben declarar y documentar. Únicamente se pueden activar a través de la interfaz software los comandos documentados. El fabricante debe declarar que la documentación de comandos es completa.			
d)	Si un software legalmente relevante se ha separado de uno no relevante, el primero debe tener prioridad en la utilización de los recursos.			
5.2.2	**Indicaciones compartidas** Si la indicación se realiza mediante una interfaz de usuario de ventanas múltiples, se aplican los siguientes requisitos: El software que produce la indicación de los valores de medida y de otra información legalmente relevante pertenece a la parte legalmente relevante. La ventana que contenga estos datos debe tener la máxima prioridad.			
5.2.3 **5.2.3.1**	**Almacenamiento de datos, transmisión a través de sistemas de comunicación** El valor de medida almacenado o transmitido irá acompañado de toda la información relevante necesaria para su uso legalmente relevante en el futuro.			
5.2.3.2	Los datos se protegerán mediante medios software para garantizar su autenticidad, integridad y, si procede, la exactitud de la información relativa al momento de la medición. El software que visualiza o que posteriormente procesa los valores de medida y los datos complementarios comprobará el momento de la medición, la autenticidad y la integridad de los datos después de haberlos leído de un almacenamiento inseguro o después de haberlos recibido por un canal de transmisión inseguro. Si se detecta una irregularidad, los datos se deben descartar o marcar como inservibles.			
5.2.3.3	Para obtener un nivel de protección alto es necesario aplicar métodos criptográficos.			

Apartado	Requisito	Aceptado	Rechazado	Comentarios
5.2.3.4 **a)**	**Almacenamiento automático** Los datos de medida deben almacenarse de forma automática al concluir la medición, es decir, cuando se haya generado el valor final utilizado con fines legales. El dispositivo de almacenamiento debe tener permanencia suficiente como para garantizar que los datos no son corrompidos en condiciones normales de almacenamiento. La capacidad de almacenamiento debe ser suficiente para cada aplicación particular. Cuando el valor final utilizado con fines legales resulta de un cálculo, todos los datos necesarios para dicho cálculo se deben almacenar de forma automática con el valor final.			
b)	Se pueden eliminar los datos almacenados si: • ya se ha concluido la transacción; • estos datos se han impreso con un dispositivo de impresión sujeto al control legal.			
c)	Una vez cumplidos los requisitos establecidos del apartado 5.2.3.4.b y cuando el almacenamiento está lleno, se pueden eliminar datos memorizados si se cumplen las condiciones siguientes: – que se eliminen los datos en el mismo orden de registro respetando las normas establecidas en la aplicación particular; – que se eliminen de forma automática o después de una operación manual específica.			
5.2.3.5	**Retraso en la transmisión** La medición no debería verse influenciada de forma inadmisible por un retraso en la transmisión.			
5.2.3.6	**Interrupción de la transmisión** Si los servicios de red dejan de ser accesibles, los datos de medida no se perderán. El proceso de medición debería detenerse para evitar la pérdida de datos de medida.			
5.2.3.7	**Registro de fecha y hora** El registro de fecha y hora se leerá del reloj del dispositivo. Se deben utilizar métodos de protección adecuados según el nivel de severidad aplicable (véase el apartado 5.1.3.2.c). Si se necesita información relativa al tiempo de medición, la fiabilidad del reloj interno del instrumento de medida se debe mejorar con medios específicos.			

Apartado	Requisito	Aceptado	Rechazado	Comentarios
5.2.4	**Compatibilidad de los sistemas operativos y del hardware, portabilidad**			
5.2.4.1	El fabricante identificará el entorno adecuado de hardware y software. Además, establecerá los recursos mínimos y la configuración adecuada necesarios para el correcto funcionamiento.			
5.2.4.2	Se deben incluir medios técnicos en el software legalmente relevante para evitar la operación si no se cumplen los requisitos mínimos de configuración.			
5.2.6	**Mantenimiento y reconfiguración**			
5.2.6.1	Únicamente se autoriza el uso de las versiones del software legalmente relevante que están en conformidad con el modelo aprobado.			
5.2.6.2	**Actualización verificada** Después de actualizar el software legalmente relevante de un instrumento de medida (cambio por otras versiones aprobadas o nueva instalación), no está permitido utilizarlo con fines legales antes de haberlo verificado y haber renovado los medios de seguridad.			
5.2.6.3	**Actualización rastreada**			
a)	La Actualización rastreada del software será automática. Al finalizar el proceso de actualización el entorno de protección del software estará al mismo nivel que el requerido en la aprobación de modelo.			
b)	En instrumento de medida de destino tendrá un software legalmente relevante fijo.			
c)	Se deben utilizar medios técnicos para garantizar la autenticidad del software cargado. Si el software cargado no supera el control de autenticidad, el instrumento lo descartará y utilizará la versión anterior del software o cambiará a un modo inoperante.			
d)	Se deben utilizar medios técnicos para asegurar la integridad del software cargado, es decir, que no ha sido modificado de forma inadmisible antes de la carga.			
e)	Se deben utilizar medios técnicos adecuados con el fin de garantizar que la trazabilidad de las Actualizaciones rastreadas es adecuada en el instrumento.			

Apartado	Requisito	Aceptado	Rechazado	Comentarios
f)	El instrumento de medida debe disponer de un dispositivo electrónico / subconjunto que permita al usuario o al propietario expresar su consentimiento. Se debe poder habilitar y deshabilitar este dispositivo electrónico / subconjunto, p. ej. mediante un interruptor que se pueda precintar o mediante un parámetro. Si el dispositivo electrónico / subconjunto está habilitado, serán el usuario o el propietario quienes inicien las descargas. Si está deshabilitado no es necesario que el usuario o el propietario lleven a cabo ninguna acción para realizar la descarga.			
g)	Si los requisitos del apartado 5.2.6.3.a al apartado 5.2.6.3.f no pueden cumplirse, sigue siendo posible actualizar la parte legalmente no relevante del software. En tal caso, deben cumplirse los siguientes requisitos: • existe una separación definida entre el software legalmente relevante y el no relevante de acuerdo con el apartado 5.2.1; • la parte legalmente relevante del software no se puede actualizar sin romper el precinto; • en el certificado de aprobación de modelo consta que la actualización de la parte legalmente no relevante es posible.			
5.2.6.4	El instrumento de medida debe disponer de una herramienta con el objeto de registrar automática y permanentemente cualquier ajuste del parámetro específico del dispositivo, p. ej. un registro de actividades. El instrumento tendrá capacidad para presentar los datos registrados.			
5.2.6.5	Los medios y los registros de trazabilidad forman parte del software legalmente relevante y deberían protegerse como tales.			

Anexo C

Índice

NIPO 706-10-013-3