DOCUMENTO
INTERNACIONAL

OIML D 31

Edición 2008 (E)

Requerimientos generales para instrumentos de medición controlados por software

Exigences générales pour les instruments de mesure contrôlés par logiciel

ORGANISATION INTERNATIONALE
DE MÉTROLOGIE LÉGALE

ORGANIZACIÓN INTERNACIONAL
DE METROLOGÍA LEGAL

Traducido para CAFIPEM por Dilva Leunda Tosi
Marzo 2022

Contenidos

Prólogo

La Organización Internacional de Metrología Legal (OIML) es una organización mundial, e intergubernamental, cuyo objetivo primario es armonizar las regulaciones y los controles metrológicos, de sus Estados Miembros, aplicados por los servicios metrológicos nacionales u organizaciones relacionadas. Las categorías principales de las publicaciones de OIML son:

- **Recomendaciones Internacionales (OIML R)**: son regulaciones modelo, que establecen las características metrológicas requeridas por ciertos instrumentos de medición y, que especifican métodos y equipamiento para verificar su conformidad. Los Estados Miembro de OIML implementarán estas Recomendaciones, en la mayor medida posible;

- **Documentos Internacionales (OIML D)**: son documentos de naturaleza informativa, que pretenden armonizar y mejorar el trabajo en el campo de la metrología legal;

- **Guías Internacionales (OIML G)**: son documentos de naturaleza informativa, como los anteriores, que pretenden dar directrices para la aplicación de ciertos requerimientos de la metrología legal; y

- **Publicaciones Básicas Internacionales (OIML B)**: definen las reglas operativas de los varios sistemas y estructuras de OIML.

Los Proyectos de Recomendaciones, Documentos y Guías, son desarrollados por Comisiones Técnicas o Subcomisiones, que incluyen representantes de los Estados Miembros. Algunas instituciones internacionales y regionales también participan de una consulta base. Se han establecido acuerdos cooperativos entre OIML y ciertas instituciones, tales como ISO y la IEC, con el objetivo de evitar requisitos contradictorios. Consecuentemente, los fabricantes y usuarios de instrumentos de medida, laboratorios de ensayo, etc… pueden aplicar de manera simultánea las publicaciones OIML y las de otras instituciones.

Las Recomendaciones Internacionales, los Documentos, las Guías y las Publicaciones Básicas se publican en inglés (E) y se traducen al francés (F), y están sujetas a revisiones periódicas.

Adicionalmente la OIML publica o participa en las publicaciones de Vocabularios (OIML V) y periódicamente comisiona a expertos en metrología legal para escribir Reportes de Expertos (OIML E). Los Reportes de Expertos tienen como objetivo proporcionar información y asesoramiento, y están escritos solamente desde el punto de vista de su autor, sin la participación de una Comisión o de una Subcomisión Técnica, ni de la Comisión Internacional de Metrología Legal (CIML). Por lo tanto, no necesariamente representan el punto de vista de la OIML.

Esta publicación – referencia OIML D 31, edición 2008 (E) - fue desarrollada por la Subcomisión Técnica de la OIML TC 5/SC 2 Software. Fue aprobada para su publicación final, por la Comisión Internacional de Metrología Legal en el año 2008.

Las Publicaciones OIML se puede descargar de la página web de la OIML con formato de archivos PDF. Se puede solicitar Información adicional sobre Publicaciones de OIML, a la Jefatura de la Organización.

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

Requerimientos generales para instrumentos de medición controlados por software

1 Introducción

El objetivo primario de este Documento Internacional es proveer a las Comisiones y Subcomisiones Técnicas de la OIML, de una guía para establecer requerimientos apropiados, para funcionalidades relacionadas con software en los instrumentos de medición cubiertos por las Recomendaciones OIML.

Adicionalmente, este Documento Internacional puede proveer a los miembros plenos de OIML, de una guía para la implementación de las Recomendaciones de OIML, en sus leyes nacionales.

2 Alcance y campo de aplicación

2.1 Este Documento International especifica los requerimientos generales aplicables a las funcionalidades relacionadas con software, en los instrumentos de medición y provee de una guía para verificación del cumplimiento de un instrumento con esos requerimientos.

2.2 Este Documento se tendrá en cuenta por parte de los Comisiones y Subcomisiones Técnicas de la OIML, como base para establecer requerimientos y procedimientos específicos de software, en las Recomendaciones de OIML aplicables a categorías particulares de instrumentos de medición (de aquí en adelante denominadas como “Recomendaciones relevantes de OIML”).

2.3 Las instrucciones que se dan en este Documento, aplican solamente a los instrumentos de medición controlados por software o a los dispositivos electrónicos.

Notas:

- Este Documento no cubre todos los requerimientos técnicos específicos a los instrumentos de medición controlados por software; estos requerimientos deben figurar en la Recomendación relevante correspondiente de la OIML, por ejemplo: para instrumentos de pesar, medidores de agua, etc.

- Este Documento tiene en cuenta algunos aspectos concernientes a la seguridad de los datos. Adicionalmente en esta área, se deben considerar las regulaciones nacionales.

- Como los dispositivos controlados por software son siempre electrónicos, también es necesario tener en cuenta el Documento D11 de OIML: *Requerimientos generales para instrumentos de medición electrónicos.*

3 Terminología

Algunas de las definiciones utilizadas en este Documento están en conformidad con el Vocabulario Internacional de Términos Generales y Básicos de Metrología (VIM:1993 [1]), con el Vocabulario Internacional de Términos de Metrología Legal (OIML V 1:2000 [8]), con el Documento Internacional de OIML *Requerimientos generales para instrumentos de medición electrónicos* (OIML D 11:2004 [3]) y con varios Estándares Internacionales ISO/IEC. Con el propósito de este Documento, se aplican las siguientes abreviaturas y definiciones.

3.1 Terminología General

3.1.1 Solución aceptable

Diseñar o definir condiciones para el diseño de un módulo de software o una unidad de hardware, o diseñar o definir condiciones para el diseño de una característica que se considera que cumple con un requerimiento particular. Una solución aceptable provee un ejemplo de como se puede cumplir un requerimiento particular. Esta solución no implica que exista alguna otra que pueda cumplir ese requerimiento.

3.1.2 Registro de auditoría

Archivo de datos continuos que contiene un registro de sello de tiempo de eventos, por ejemplo: cambios en los valores de los parámetros de un dispositivo o actualizaciones de software, u otras actividades que son legalmente relevantes y que pueden influenciar a las características metrológicas.

3.1.3 Autenticación

Chequeo de la identidad declarada o presunta, de un usuario, proceso o dispositivo, (por ejemplo: chequeo de que el software descargado se realiza por parte del dueño del certificado de aprobación de modelo).

3.1.4 Autenticidad

Resultado del proceso de autentificación (aprobado o fallido).

3.1.5 Funcionalidad de verificación [OIML D 11:2004, 3.18]

Funcionalidad que posee un instrumento de medición y que le permite detectar y actuar sobre fallas significativas.

> *Nota:* "Actuar" se refiere a cualquier respuesta adecuada por parte del instrumento de medición (señal luminosa, impedimento del proceso de medición, etc.).

3.1.6 Red cerrada

Red conformada por un número fijo de participantes, con identidad conocida, funcionalidad y ubicación (ver también *Red abierta*).

3.1.7 Comandos

Los comandos pueden ser o una secuencia de señales eléctricas (ópticas, electromagnéticas, etc.) en las interfaces de entrada o códigos en los protocolos de transmisión de datos. Pueden ser generados por el software del instrumento de medición / dispositivo electrónico / subconjunto (comandos de software) o generados por el usuario a través de la interfaz de usuario del instrumento de medición (comandos de usuario).

3.1.8 Comunicación

Intercambio de información entre dos o más unidades (por ejemplo: módulos de software, dispositivos electrónicos, subconjuntos, etc.), que se realiza siguiendo reglas específicas.

3.1.9 Interfaz de comunicación

Interfaz electrónica, óptica, de radio u otro tipo de interfaz técnica, que permite el intercambio de información entre los componentes de un instrumento de medición (por ejemplo: dispositivos electrónicos) o entre subconjuntos.

3.1.10 Certificado criptográfico

Conjunto de datos que contienen la llave pública de un instrumento de medición o de una persona y también una única identificación del instrumento o de la persona, por ejemplo: número de serie del instrumento de medición o nombre o PIN (número de identificación personal) de la persona. El conjunto de datos es firmado por una institución confiable con firma electrónica. La asignación de una llave pública ya sea a un instrumento de medición o a una persona, puede ser verificada usando la llave pública de la institución confiable y desencriptando la firma del certificado.

3.1.11 Métodos criptográficos

Encriptado de datos por parte del transmisor (programa de transmisión o almacenamiento) y desencriptado por parte del receptor (programa de lectura) con el propósito de mantener en resguardo la información, de personas no autorizadas.

Firma electrónica de datos, con el propósito de permitir al receptor o usuario de éstos, la verificación del origen de los datos, es decir: probar que son auténticos.

> *Nota:* En general, para firma electrónica se utiliza un Sistema de llave pública, es decir: el algoritmo necesita un par de llaves de las cuales solo una debe ser mantenida en secreto; la otra puede ser pública.
>
> El transmisor (programa de transmisión o almacenamiento) genera un Código hash (ver 3.1.25) de los datos y lo encripta con su *llave secreta*. El resultado es la firma. El receptor (programa de lectura o receptor) desencripta la firma con la llave pública del transmisor y compara el resultado con el Código hash real de los datos. En el caso en que se verifique la igualdad, los datos se consideran autenticados.
>
> El receptor puede requerir un certificado criptográfico del transmisor (ver 3.1.10), para asegurarse de que la llave pública es auténtica.

3.1.12 Dominio de datos

Ubicación en la memoria que cada programa necesita para procesar los datos. Dependiendo del tipo de lenguaje de programación utilizado, esta ubicación está definida por direcciones de hardware o por nombres simbólicos (nombres de variables). El tamaño del dominio direccionable más pequeño es típicamente de un byte, pero casi no está limitado: su rango va desde un bit (por ejemplo: un registro de estado) hasta estructuras de datos arbitrarias que pueden ser tan grandes como lo sean las necesidades del programador.
El dominio de datos puede pertenecer solo a un módulo de *software*, o a varios. Para lenguajes de alto nivel (tales como JAVA, C/C++, etc.) es fácil separar el dominio de datos de un módulo de software, del acceso de cualquier otro módulo de software por medio del lenguaje.

3.1.13 Parámetro específico de dispositivo

Parámetro legalmente relevante cuyo valor depende del instrumento en particular. Los parámetros específicos de dispositivo comprenden parámetros de ajuste (por ejemplo: ajuste de span u otros ajustes o correcciones) y parámetros de configuración (por ejemplo: valor máximo, valor mínimo, unidades de medida, etc.).

3.1.14 Durabilidad [OIML D 11:2004, 3.17]

Capacidad del instrumento de medición de mantener sus características de desempeño durante un período de uso.

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

Instrumento de medición destinado a medir una cantidad eléctrica o no eléctrica, utilizando medios electrónicos y/o equipado con dispositivos electrónicos.

Nota: Para el propósito de este Documento, el equipamiento auxiliar, mientras esté sujeto a control metrológico legal, se considera parte del instrumento de medición.

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

Dispositivo que emplea subconjuntos y que realiza una función específica. Un dispositivo electrónico se fabrica usualmente como una unidad separada y es capaz de ser ensayado individualmente.

Notas: Un dispositivo electrónico puede ser un instrumento de medición completo (por ejemplo: una balanza contadora, un medidor de consumo de electricidad) o parte de un instrumento de medición (por ejemplo: impresora, indicador).

Un dispositivo electrónico puede ser un módulo, en el sentido en que el término módulo se utiliza en OIML B 3 *OIML Certificate System for Measuring Instruments* [2].

3.1.17 Error (de indicación) [VIM:1993, 5.20; OIML D 11:2004, 3.5]

Indicación de un instrumento de medición menos el valor verdadero de la cantidad de entrada correspondiente.

3.1.18 Registro de error

Archivo de datos continuos que contiene un registro de información de fallas/averías que tienen influencia en las características metrológicas. Ésto aplica especialmente a fallas volátiles, que no se pueden reconocer más tarde, cuando se utilizan los valores de medición.

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

Examen y ensayo sistemático del funcionamiento de una o más muestras de un modelo identificado de instrumentos de medición contra requerimientos documentados. Los resultados de estos exámenes y ensayos están contenidos en el reporte de evaluación, con el fin de determinar si el modelo puede ser aprobado.

3.1.20 Evento

Acción mediante la cual se realiza una modificación de un parámetro de un instrumento de medición, de un factor de ajuste o una actualización del módulo de software.

3.1.21 Contador de evento

Contador no reiniciable, que se incrementa cada vez que ocurre un evento.

3.1.22 Código ejecutable

Archivo instalado en el Sistema informático del instrumento de medición, dispositivo electrónico, o subconjunto (EPROM, disco duro, etc.). Este código es interpretado por el microprocesador y transpuesto (transformado) en ciertas operaciones lógicas, aritméticas, de decodificación o de transporte de datos.

3.1.23 Falla [adaptado de OIML D 11:2004, 3.9]

Defecto que provoca un impacto en las propiedades o funciones de un instrumento de medición o que causa un error de indicación mayor que el EMT (error máximo tolerado).

3.1.24 Parte invariable del software legalmente relevante

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

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

Función (matemática) que mapea valores de un dominio grande (posiblemente muy grande) a un rango menor. Una "buena" función hash es aquella que al ser aplicada a un (gran) conjunto de valores del dominio, dará como resultado valores distribuidos equitativamente (y aparentemente de manera aleatoria) en el rango.

3.1.26 Integridad de programas, datos o parámetros

Garantía de que programas, datos o parámetros, no han sido sometidos a ningún cambio no autorizado o involuntario mientras están en proceso de uso, transferencia, almacenamiento, reparación o mantenimiento.

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

Límite compartido entre dos unidades funcionales, definido por características varias correspondientes a las funciones, interconexiones físicas, intercambios de señal y otras características de las unidades, según sea apropiado.

3.1.28 Error intrínseco [VIM:1993, 5.24; OIML D 11:2004, 3.7]

Error de un instrumento de medición, determinado bajo condiciones de referencia.

3.1.29 Legalmente relevante

Software/hardware/datos o parte del software/hardware/datos de un instrumento de medición, que interfiere con las propiedades reguladas por la metrología legal, por ejemplo: la precisión de la medición o el correcto funcionamiento del instrumento de medición.

3.1.30 Parámetro legalmente relevante

Parámetro de un instrumento de medición, de un dispositivo electrónico o de un subconjunto, que es objeto de control legal. Se pueden distinguir los siguientes tipos de parámetros legalmente relevantes: *parámetros específicos de modelo* y *parámetros específicos de dispositivo*.

3.1.31 Parte del software legalmente relevante

Parte de todos los *módulos de software* de un instrumento de medición, de un dispositivo electrónico, o de un subconjunto, que es legalmente relevante.

---

1) Esta parte es responsable del monitoreo de la actualización del software (carga del software, autenticación, chequeo de la integridad, instalación y activación)

3.1.32 Error máximo permitido (de un instrumento de medición) [VIM:1993, 5.21; OIML D 11:2004, 3.6]

Valor máximo de un error permitido por las especificaciones, regulaciones, etc. para un instrumento de medición dado.

3.1.33 Instrumento de medición [VIM:1993, 4.1]

Dispositivo destinado a ser usado para realizar mediciones, solo o en conjunto con dispositivo/s suplementario/s.

3.1.34 Medición No interrumpible / Interrrumpible

Una medición No interrumpible es un proceso de medición continuo acumulativo con un final no definido. El proceso de medición no puede ser detenido y luego continuado por un usuario u operador, sin que se altere inadmisiblemente la medición o la alimentación con mercancías o con energía.

Si la medición acumulativa de la cantidad de una substancia se puede detener de manera simple y rápida durante la operación normal- no solo en caso de emergencia- sin falsificar el resultado de la medición, se denomina Interrumpible.

3.1.35 Red abierta

Red de participantes arbitrarios (dispositivos electrónicos con funciones arbitrarias). El número, la identidad y la ubicación de cada participante puede ser dinámico y ser desconocido para los otros participantes (ver también *Red cerrada*).

3.1.36 Performance (desempeño) [OIML D 11:2004, 3.16]

Capacidad de un instrumento de medición de realizar las funciones que se espera que lleve a cabo.

3.1.37 Código de programa

Código Fuente o Código ejecutable.

3.1.38 Sellado

Medios destinados a proteger al instrumento de medición de cualquier modificación no autorizada, reajuste, remoción de partes, software, etc. Se puede lograr por hardware, software o una combinación de ambos.

3.1.39 Protección

Prevenir el acceso no autorizado a las partes del hardware o del software del dispositivo.

3.1.40 Software

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

3.1.41 Examen del software

Operación técnica que consiste en determinar una o más características del software de acuerdo con el procedimiento específico (por ejemplo: análisis de documentación técnica o funcionamiento del programa bajo condiciones controladas).

3.1.42 Identificación del software

Secuencia de caracteres legibles (por ejemplo: número de versión, checksum) unida inseparablemente al software o módulo de software, que está siendo considerado. Se puede chequear en un instrumento, mientras éste esté en uso.

3.1.43 Interfaz de software

Conformada por el código de programa y un dominio de datos dedicado. Recibe, filtra o transmite datos entre los *módulos de software* (no necesariamente relevantes).

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

Entidades lógicas tales como programas, subrutinas, bibliotecas y objetos que incluyen sus *dominios de datos* que pueden estar en relación con otras entidades. El software de los instrumentos de medición, dispositivos electrónicos o subconjuntos consiste en uno o más módulos de software.

3.1.45 Protección del software

Protección del software del instrumento de medición o del dominio de datos, mediante un sello implementado por hardware o software. El sello debe ser removido, dañado o roto, para obtener acceso a realizar el cambio del software.

3.1.46 Separación del software

El software en instrumentos de medición/dispositivos electrónicos/subconjuntos, se puede dividir en una parte legalmente relevante y una parte no legalmente relevante. Estas partes se comunican a través de una *interfaz de software.*

3.1.47 Código fuente

Programa de computación escrito de forma tal (lenguaje de programación) que sea legible y editable. El código fuente se compila o interpreta como *código ejecutable*.

3.1.48 Dispositivo de almacenamiento

Espacio de almacenamiento de los datos de medición, utilizado para que estos datos estén disponibles luego que se haya completado la medición y para propósitos legalmente relevantes (por ejemplo: la finalización de una transacción comercial).

3.1.49 Subconjunto [OIML D 11:2004, 3.3]

Parte de un dispositivo electrónico que emplea componentes electrónicos y que tiene una función identificable que le es propia.

Ejemplos: Amplificadores, comparadores, convertidores de potencia, etc.

3.1.50 Ensayo [OIML D 11:2004, 3.20]

Serie de operaciones destinadas a verificar el cumplimiento del equipo bajo ensayo (IBE) con los requerimientos específicos.

3.1.51 Sello de tiempo

Valor único de tiempo monótonamente creciente, por ejemplo: en segundos, o de una fecha y una cadena de datos de tiempo, que indica la fecha y/o la hora a la cual ocurrió un cierto evento o falla. Este dato se presenta en un formato consistente, que permite la comparación simple de dos registros diferentes y el seguimiento del progreso a lo largo del tiempo.

3.1.52 Transmisión de datos de medición

Transmisión de datos de medición por medio de redes de comunicación u otros medios, hacia un dispositivo electrónico alejado, en donde son además procesados y/o utilizados con propósitos legalmente regulados.

3.1.53 Parámetro específico de modelo

Parámetro legalmente relevante cuyo valor depende solo del modelo del instrumento. Los parámetros específicos de modelo son parte del software legalmente relevante.

Ejemplo: Si consideramos un sistema de medición de líquidos diferente al agua, el rango de la viscosidad cinemática de una turbina es un parámetro específico de modelo, fijado en la aprobación de modelo de la turbina. Todas las turbinas del mismo modelo tienen el mismo rango de viscosidad.

3.1.54 Computadora universal

Computadora que no está construida para un propósito específico, pero que puede ser adaptada a la tarea metrológica, mediante software. En general este software se basa en un sistema operativo que permite la carga y la ejecución del software con propósitos específicos.

3.1.55 Interfaz de usuario

Interfaz que permite intercambio de información entre una persona y el instrumento de medición o con sus componentes de hardware o software, por ejemplo: interruptores, teclado, mouse, pantalla, monitor, impresora, pantalla táctil, ventana de software en una pantalla que incluye el software que lo genera.

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

Confirmación por examen y obtención de una evidencia objetiva (es decir: información que puede ser demostrada como cierta, basada en hechos obtenidos a partir de observaciones, medición, ensayo, etc.) de que se cumplen los requerimientos particulares para el uso específico previsto. En este caso, los requerimientos relacionados son los de este Documento.

3.1.57 Verificación [V 1: 2000, 2.13]

Procedimiento (diferente al de aprobación de modelo) que incluye el examen y marcado y/o emisión de un certificado de verificación que asegure y confirme, que el instrumento de medición cumple con los requerimientos estatutarios[2)].

3.2 Abreviaturas

IBE/EUT	Instrumento bajo ensayo
IEC	Comisión Electrotécnica Internacional
I/O	Input / Output (Entrada/Salida se refiere a los puertos)
ISO	Organización Internacional para la Estandarización
TI/IT	Tecnología de la Información
EMT/MPE	Error Máximo Tolerado
OIML	Organización Internacional de Metrología Legal
PCB	Plaqueta de circuito impreso

2) Nota: definición diferente de otros estándares, por ejemplo: ISO/IEC 14598, cláusula 4.23 o IEC 61508-4, cláusula 3.8.1.

PIN	Número de Identificación Personal
TC	(OIML) Comité Tecnico
SC	(OIML) Subcomité

4 Instrucciones para el uso de este Documento en la redacción de las Recomendaciones OIML

4.1 Las disposiciones de este Documento aplican solo a las nuevas Recomendaciones OIML y a los Documentos OIML bajo revisión. Los TCs (Comités Técnicos) y los SCs (Subcomités) deben usar este Documento guía, para establecer los requerimientos relacionados con software, en adición a otros requerimientos técnicos y metrológicos de la Recomendación relevante de OIML.

4.2 Todos los documentos normativos están sujetos a revisión y se impulsa a los usuarios de este Documento a investigar la posibilidad de aplicar las ediciones más recientes de los documentos normativos.

4.3 Es el objetivo de este Documento el proveer a los TCs (Comités Técnicos) o a los SCs (Subcomités), responsables de la redacción de las Recomendaciones OIML, de un conjunto de requerimientos-en parte con diferentes niveles -que sean apropiados para cubrir las demandas de todo tipo de instrumentos de medición y de todas las áreas de aplicación. El TC o el SC debe determinar que nivel es el apropiado para protección, conformidad o problemas de rigurosidad de validación y como incorporar la parte relevante de este Documento en la Recomendación OIML que se está redactando. En la sección 8 se brinda ayuda para realizar esta tarea.

5 Requerimientos para instrumentos de medición con respecto a la aplicación de software

5.1 Requerimientos generales

Al momento de la publicación de este Documento, los requerimientos generales representan la última tecnología en tecnología de la información (IT). En principio son aplicables a todo tipo de instrumentos de medición controlados por software, dispositivos electrónicos y subconjuntos y deberían ser considerados en todas las Recomendaciones OIML. En contraste con estos requerimientos generales, los requerimientos específicos para configuración (5.2), lidian con características técnicas que no son comunes para algunos tipos de instrumentos o algunas áreas de aplicación.

En los ejemplos, en donde es aplicable, se muestran tanto los niveles normales de severidad como los elevados. La notación en este Documento es como sigue abajo:

(I) Solución técnica aceptable, en el caso de nivel de severidad normal;

(II) Solución técnica aceptable, en el caso de nivel de severidad elevado (ver 8).

5.1.1 Identificación del software

El software legalmente relevante de un instrumento de medición/dispositivo electrónico/subconjunto debe ser claramente identificado con la versión del software u otro identificador (token). La identificación puede consistir en más de una parte, pero al menos una parte debe estar dedicada al propósito legal.

La identificación debe estar inseparablemente unida al software en sí mismo y debe ser mostrada o impresa cuando se lo requiera o mostrada en la pantalla durante la operación o en la puesta en marcha de un instrumento de medición que puede ser apagado y encendido nuevamente. Si un subconjunto/dispositivo electrónico no tiene ni pantalla ni impresora, la identificación se debe enviar a través de una interfaz de comunicación, con el objeto de ser mostrada en pantalla/impresa en otro subconjunto/dispositivo electrónico.

Como excepción se considera una solución aceptable, la colocación de un sello/marca con la identificación del software en el instrumento/dispositivo electrónico, si satisface las siguientes condiciones:

1) La interfaz de usuario no tiene ninguna capacidad de control para activar la indicación de la identificación del software en la pantalla, o la pantalla no permite técnicamente que se muestre la identificación del software (dispositivo de indicación analógico o contador electromecánico).
2) El instrumento/dispositivo electrónico no tiene una interfaz para transmitir la identificación del software.
3) Luego que el instrumento/dispositivo electrónico haya sido fabricado, no es posible un cambio del software, o solo es posible si el hardware o un componente del hardware también se cambia.

El fabricante del hardware o del componente correspondiente del hardware es responsable de asegurar que la identificación del software esté correctamente marcada en el instrumento/dispositivo electrónico en cuestión.

La identificación del software y el medio de identificación debe figurar en el certificado de aprobación de modelo.

La Recomendación OIML relevante debe permitir o no permitir esta excepción.

Nota: Cada instrumento de medición en uso, debe ser conforme al modelo aprobado. La identificación del software permite al personal de vigilancia y a las personas afectadas por la medición, determinar si el instrumento en consideración es conforme al modelo aprobado.

Ejemplo:

(I) El software contiene una cadena de texto o un número, que de manera no ambigua identifica la versión instalada. La cadena (string) se transfiere a la pantalla del instrumento cuando se presiona un botón, cuando se enciende el instrumento, o es controlado cíclicamente por un temporizador.

Un número que indique la versión puede tener la siguiente estructura A.Y.Z. Si consideramos una computadora de flujo, la letra A representará la versión del software principal que está contando pulsos, la letra Y representará la versión de la función de conversión (ninguna, a 15 °C, a 20 °C) y la letra Z representará el lenguaje de la interfaz de usuario.

(II) El software calcula un checksum del código ejecutable y presenta el resultado como la identificación, en lugar de o además del string especificado en (I). El algoritmo de checksum debe ser un algoritmo normalizado, por ejemplo: el algoritmo CRC16 es una solución aceptable para este cálculo.

La solución (II) es apropiada, si se requiere una conformidad incrementada (ver 5.2.5.(d) y 8.).

5.1.2 Corrección de los algoritmos y de las funciones

Los algoritmos y las funciones de medición de un dispositivo electrónico, deben ser apropiados y funcionalmente correctos para la aplicación dada y para el modelo de dispositivo (precisión de los algoritmos, cálculo de precio de acuerdo a ciertas reglas, algoritmos de redondeo, etc).

El resultado de la medición y la información que lo acompaña, requeridos por las Recomendaciones específicas de la OIML o por la Legislación Nacional, deben ser mostrados en pantalla o impresos de manera correcta.

Debe ser posible examinar los algoritmos y funciones ya sea por medio de ensayos metrológicos, ensayos de software o por examen del software (como se describe en 6.3).

5.1.3 Protección del software

5.1.3.1 Prevención de mal uso

Un instrumento de medición debe ser construido de tal forma que las posibilidades de su mal uso sean mínimas, ya sea un mal uso no intencional, accidental o intencional. En el marco de referencia de este Documento OIML, ésto aplica especialmente al software. La presentación de los resultados de medición debe ser no ambigua, para todas las partes afectadas.

Nota: Los instrumentos controlados por software son a menudo complejos en su funcionalidad. El usuario necesita una buena guía para hacer buen uso del instrumento y para alcanzar resultados de medición correctos.

Ejemplo:

El usuario es guiado por menús. Las funciones legalmente relevantes se combinan en una rama en este menú. Si cualquiera de los valores de medición pudiera perderse por efecto de una acción, el usuario debe ser advertido y se le debe requerir la realización de otra acción antes que la función sea ejecutada. Ver también 5.2.2.

5.1.3.2 Protección contra fraude

5.1.3.2.a El software legalmente relevante debe estar asegurado contra una modificación no autorizada, descarga, o cambios producidos por reemplazo del dispositivo de memoria. Adicionalmente a los sellos mecánicos, pueden ser necesarios medios técnicos para asegurar los instrumentos de medición que tienen un sistema operativo o que permiten una opción de carga de software.

Nota: Cuando el software está almacenado en un dispositivo de memoria inviolable (en el cual los datos son inalterables, por ejemplo: una memoria ROM- memoria de solo lectura- sellada), las necesidades de medios técnicos se reducen de manera acorde.

Ejemplo:

(I)/(II) El gabinete que contiene los dispositivos de memoria está sellado o el dispositivo de memoria está sellado en el PCB -placa de circuito impreso-.

(II) Si se usa un dispositivo que permite la reescritura, la entrada de habilitación de escritura se inhibe por acción de un interruptor que puede ser sellado. Se diseña el circuito de manera tal que la protección contra escritura no se puede anular mediante un cortocircuito de contactos.

(I) Un sistema de medición consiste en dos subconjuntos, el que contiene las funciones metrológicas principales está incorporado en un alojamiento o gabinete que puede sellarse. El otro subconjunto es una computadora universal con un sistema operativo. Algunas funciones tales como la indicación, están ubicadas en el software de esta computadora. Una manipulación relativamente sencilla- especialmente si se usa un protocolo estándar para comunicación entre ambas partes del software- podría estar cambiando el software en la computadora universal. Esta manipulación puede inhibirse por medio de simples medios criptográficos, por ejemplo: encriptado de la transferencia de datos entre el subconjunto y la computadora universal. La llave para el desencriptado está oculta en el programa legalmente relevante de la computadora universal. Solo este programa conoce la llave y es capaz de leer, desencriptar y utilizar los valores de medición. No se pueden usar otros programas con este propósito, ya que no pueden desencriptar los valores de medición. (ver también ejemplo en 5.2.1.2.d).

5.1.3.2.b Solo funciones claramente documentadas (ver 6.1), pueden ser activadas por la inferfaz de usuario. Esto deberá hacerse de tal manera que no facilite el uso fraudulento. La presentación de la información debe cumplir con 5.2.2.

Nota: El encargado de realizar el examen decide si todos los comandos documentados son aceptables.

Ejemplo:

(I)/(II) Todas las entradas que vienen de la interfaz de usuario se redireccionan a un programa que filtra los comandos de entrada. Solo permite que pasen los documentados y descarta todos los otros. Este programa o módulo de software es parte del software legalmente relevante.

5.1.3.2.c Los parámetros que fijan las características legalmente relevantes del instrumento de medición, deben ser protegidos contra modificaciones no autorizadas. Si es necesario para el propósito de la verificación, debe ser factible mostrar en pantalla o imprimir, las configuraciones de los parámetros actuales.

Nota: Los parámetros específicos de dispositivo deben ser ajustables o seleccionables, solo en un modo de operación especial del instrumento. Pueden ser clasificados como aquellos que deben ser protegidos (inalterables) y aquellos que pueden ser accedidos (parámetros configurables) por una persona autorizada, por ejemplo: el propietario del instrumento o el vendedor del producto.

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

Ejemplo:

(I)/(II) Los parámetros específicos de dispositivo, para ser protegidos, se almacenan en una memoria no volátil. La entrada que habilita la escritura de la memoria, se inhibe mediante un interruptor que puede ser sellado.

Referirse a los ejemplos 5.1.3.2.d (1) a (3) en esta sección.

5.1.3.2.d La protección del software comprende un sellado apropiado utilizando medios mecánicos, electrónicos y/o criptográficos. Ésto hace que una intervención no autorizada sea imposible o evidente.

Ejemplo:

1. (I) Sellado electrónico. Los parámetros metrológicos de un instrumento pueden ingresarse y ajustarse a través de un ítem del menú. El software reconoce cada cambio, e incrementa un contador de eventos con cada evento de este tipo. Se puede indicar el valor de este contador de eventos. Debe registrarse el valor inicial del contador de eventos. Si el valor indicado difiere del registrado, el instrumento está en un estado de no verificado (equivalente a que se ha roto un sello).

2. (I)/(II) El software de un instrumento de medición se construye de manera tal (ver ejemplo 5.1.3.2.a) que no hay manera de modificar los parámetros y la configuración legalmente relevantes excepto mediante un menú protegido por un interruptor. Este interruptor está mecánicamente sellado en su posición inactiva, lo cual hace que sea imposible modificar los parámetros y la configuración legalmente relevantes.

   Para modificar los parámetros y la configuración, el interruptor debe ser accionado, para lo cual inevitablemente, se debe romper el sello.

3. (II) El software de un instrumento de medición se construye de manera tal (ver ejemplo (a)), que no hay manera de acceder a los parámetros y a la configuración legalmente relevantes, excepto por personas autorizadas. Si una persona desea ingresar en el ítem del menú de parámetros, debe colocar su tarjeta inteligente que contiene un PIN como parte de un certificado criptográfico. El software del instrumento es capaz de verificar la autenticidad del PIN por medio del certificado y permite el ingreso al ítem del menú de parámetros. El acceso se registra en una pista de auditoría, incluyendo la identidad de la persona (o al menos de la tarjeta inteligente utilizada).

   El nivel (II) de los ejemplos para soluciones técnicas aceptables es apropiado, si es necesaria una protección mayor contra fraude (ver 8).

5.1.4 Soporte de las características del hardware

5.1.4.1 Soporte de detección de fallas

La Recomendación relevante de OIML puede requerir funciones de detección de fallas, para ciertas fallas del instrumento (indicadas en OIML D 11:2004 (5.1.2 (b) y 5.3)). En este caso, se le podrá solicitar al fabricante del instrumento, el diseño de funcionalidades de verificación en las partes del software o del hardware o que provea medios mediante los cuales las partes del hardware puedan ser soportadas por las partes del software del instrumento.

Si el software está involucrado en la detección de fallas, se requiere una respuesta apropiada. La recomendación OIML relevante, puede indicar que el instrumento/dispositivo electrónico se desactive, o que se genere una alarma/registro de error en el caso en que se detecte una condición de falla.

La documentación que se envía para aprobación de modelo, contendrá una lista de las fallas que detecta el software y su reacción esperada. También si es necesario para una mejor comprensión, una descripción del algoritmo de detección.

Ejemplo:

(I)/(II) En cada arranque (encendido) el programa legalmente relevante calcula un checksum del Código del programa y de los parámetros legalmente relevantes. El valor nominal de estos checksums, han sido calculados de antemano y almacenados en el instrumento. Si los valores calculados y almacenados no coinciden, el programa detiene su ejecución.

Si la medición no se puede interrumpir, el checksum se calcula de manera cíclica y se controla por medio de un temporizador de software. En el caso en que se detecte una falla, el software muestra un mensaje de error o enciende un indicador de falla registrando el momento en que se produce la falla en un archivo de registro de errores (si es que existe uno).

Un algoritmo de checksum aceptable es el CRC16.

5.1.4.2 Soporte de protección de la durabilidad

Es la elección del fabricante materializar en su diseño unidades de protección de durabilidad en el software o en el hardware (referidas en OIML D 11:2004 (5.1.3 (b) y 5.4), o permitir que las unidades de hardware sean soportadas por software. La Recomendación relevante de OIML puede aconsejar soluciones apropiadas.

Si el software está involucrado en la protección de la durabilidad, se requiere de una acción apropiada. La Recomendación relevante de OIML puede indicar que el instrumento/dispositivo electrónico se desactive o que una alarma/reporte se genere en el caso en que la durabilidad esté comprometida.

Ejemplo:

(I)/(II) Algunos tipos de instrumentos de medición, requieren un ajuste luego que haya prescripto un intervalo de tiempo, para garantizar la durabilidad de la medición. El software da una advertencia cuando el intervalo de mantenimiento ha transcurrido e incluso detiene la medición, si se ha excedido en más de un cierto intervalo de tiempo.

5.2 Requerimientos específicos para configuraciones

Los requerimientos dados en esta sección están basados en soluciones típicas en Tecnología de la Información (IT), aunque pueden no ser comunes a todas las áreas de aplicaciones legales. Siguiendo estos requerimientos, son posibles soluciones técnicas que muestran el mismo grado de seguridad y conformidad con un modelo, que los instrumentos que no están controlados por software.

Los siguientes requerimientos específicos son necesarios cuando se emplean ciertas tecnologías en los sistemas de medición. Deben ser considerados además de los que se describen en 5.1.

En los ejemplos, en donde es aplicable, se muestran tanto los niveles normales de severidad como los elevados. La notación en este Documento es como sigue abajo:

(I) Soluciones técnicas aceptables, en el caso de nivel de severidad normal;

(II) Soluciones técnicas aceptables, en el caso de nivel de severidad elevado (ver 8).

5.2.1 Especificando y separando las partes relevantes y especificando las interfaces de las partes

Las partes metrológicamente críticas de un sistema de medición- ya sean las partes del software o del hardware- no deben ser influenciadas inadmisiblemente por otras partes del sistema de medición.

Este requerimiento aplica si el instrumento de medición (o el dispositivo electrónico o subconjunto), tiene interfaces para comunicarse con otros dispositivos electrónicos, con el usuario, o con otras partes del software, además de las partes metrológicamente críticas de un instrumento de medición (o el 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 medición, que realizan funciones legalmente relevantes, deben ser identificados, claramente definidos y documentados. Forman la parte legalmente relevante de un sistema de medición.

Nota: El examinador decide si esta parte está completa o si otras partes del sistema de medición pueden ser excluidas de evaluación posterior.

Ejemplo:

1. (I)/(II) Un medidor de electricidad está equipado con una interfaz óptica, para conectarse con un dispositivo electrónico que lea los valores medidos. El medidor almacena todas las cantidades relevantes y mantiene los valores disponibles para que puedan ser leídos durante un período de tiempo suficiente. En este sistema, solo el medidor de electricidad es el dispositivo legalmente relevante. Otros dispositivos no legalmente relevantes pueden existir y pueden ser conectados a la interfaz del instrumento, siempre que se cumplan los requisitos de 5.2.1.1.b. No se requiere proteger la transmisión de los datos (ver 5.2.3).

2. (I)/(II) Un sistema de medición está formado por los siguientes subconjuntos:

   - un sensor digital que calcula el peso o el volumen;
   - Una computadora universal que calcula el precio;
   - Una impresora que imprime el valor de medición y el precio a pagar.

   Todos los subconjuntos están conectados por medio de una red de área local. En este caso el sensor digital, la computadora universal y la impresora son subconjuntos legalmente relevantes y pueden estar conectados opcionalmente a un sistema de mercaderías, que no es legalmente relevante. Los subconjuntos legalmente relevantes, tienen que cumplir los requerimientos de 5.2.1.1.b y -debido a la transmisión por intermedio de la red- también los requerimientos 5.2.3. No hay requerimientos relativos al sistema de gestión de mercaderías.

5.2.1.1.b Durante los ensayos de aprobación de modelo, se debe demostrar que las funciones relevantes y los datos de los subconjuntos y dispositivos electrónicos no pueden ser influenciados inadmisiblemente, por comandos recibidos por la interfaz.

Ésto implica que hay una asignación no ambigua de cada comando, para todas la funciones iniciadas o cambios de datos en los subconjuntos o dispositivos electrónicos.

Nota: Si los subconjuntos o dispositivos electrónicos “legalmente relevantes” interactúan con otros subconjuntos o dispositivos electrónicos “legalmente relevantes”, referirse a 5.2.3.

Ejemplo:

1. (I)/(II) El software del medidor de electricidad (ver ejemplo (1) de 5.2.1.1.a, más arriba) es capaz de recibir comandos para seleccionar las cantidades requeridas. Combina el valor medido con información adicional- por ejemplo: sello de tiempo, unidad- y envía estos datos de vuelta al dispositivo que los solicita. El software solo acepta comandos para la selección de cantidades permitidas válidas y descarta cualquier otro comando devolviendo solo un mensaje de error. Puede haber medios de protección para los contenidos del conjunto de datos, pero no son requeridos, ya que el juego de datos transmitidos no está sujeto a control legal.

2. (I)/(II) En el interior del gabinete, que puede sellarse, hay un interruptor que define el modo de operación del medidor de electricidad: una posición del interruptor indica el modo verificado y la otra el modo no verificado (son factibles otros medios de protección, además de un sello mecánico; ver los ejemplos en 5.1.3.2.a/.d). Cuando se interpretan los comandos recibidos, el software chequea la posición del interruptor: en el modo no verificado el juego de comandos que el software acepta es un juego extendido (más amplio), comparado con el modo descripto arriba; por ejemplo: puede ser posible el ajuste del factor de calibración por medio de un comando que se descarta en el modo verificado.

5.2.1.2 Separación de partes del software

Los TCs y los SCs de la OIML pueden especificar en la Recomendación relevante, el software / hardware/ datos o parte del software/ hardware/datos, que son legalmente relevantes.

Las regulaciones nacionales pueden prescribir que un software específico/hardware/ datos o parte del software/hardware/ datos, es/son legalmente relevante/s.

5.2.1.2.a Todos los módulos de software (programas, subrutinas, objetos, etc.). que realicen funciones legalmente relevantes o que contengan dominio de datos legalmente relevantes, forman la parte legalmente

relevante del software de un instrumento de medición (dispositivo electrónico o subconjunto). El requerimiento de conformidad aplica a esta parte (ver 5.2.5) y debe ser identificable como se describe en 5.1.1.

Si la separación del software no es posible ni necesaria, el software es legalmente relevante en su totalidad.

Ejemplo:

(I) Un sistema de medición consiste en varios sensores digitales conectados a una computadora personal, que muestra los valores de la medición. El software legalmente relevante en la computadora personal se separa de las partes no legalmente relevantes, por compilación de todos los procedimientos que realizan funciones legalmente relevantes en una biblioteca dinámicamente vinculable. Una o varias aplicaciones no legalmente relevantes, puede/n llamar procedimientos de programa de esta biblioteca. Estos procedimientos reciben los datos de medición de los sensores digitales, calculan el resultado de la medición y lo muestran en una ventana de software. Cuando las funciones legalmente relevantes han concluido, el control se devuelve a la aplicación no legalmente relevante.

5.2.1.2.b Si la parte legalmente relevante del software se comunica con otras partes del software, se debe definir una interfaz de software. Toda comunicación se debe realizar exclusivamente utilizando esta interfaz. La parte del software legalmente relevante y la interfaz deben ser claramente documentadas. Todas las funciones legalmente relevantes y dominios de datos del software deben ser descriptos, para permitir a la autoridad de aprobación de modelo decidir si la separación del software es correcta.

La interfaz consiste en código de programa y dominios de datos dedicados. Los comandos o datos codificados definidos, se intercambian entre las partes del software, almacenándolos en el dominio de datos dedicados en una parte del software y leyéndolos desde la otra parte. El Código de programa de lectura y escritura es parte de la interfaz del software. El dominio de datos que conforma la interfaz del software incluyendo el código que exporta desde la parte legalmente relevante al dominio de datos de la interfaz y el código que importa desde la interfaz a la parte legalmente relevante deben ser claramente definidos y documentados. La interfaz de software declarada no debe ser eludida.

El fabricante es responsable de respetar estas restricciones. No es posible utilizar medios técnicos (como el sellado) para prevenir que un programa eluda la interfaz y tampoco para prevenir la programación de comandos ocultos. El programador de la parte del software legalmente relevante tanto como el de la parte legalmente no relevante, deben recibir instrucciones con estos requerimientos por parte del fabricante

5.2.1.2.c Debe haber una asignación no ambigua de cada comando, para todas las funciones invocadas o para los cambios de datos, en la parte del software legalmente relevante. Los comandos que se envían a través de la interfaz de software, deben ser declarados y documentados. Solo se pueden activar a través de la interfaz del software, los comandos que hayan sido documentados. El fabricante debe declarar la integridad de la documentación de los comandos.

Ejemplo:

(I) En el ejemplo descripto en 5.2.1.2.a, la interfaz de software se realiza mediante los parámetros y valores de retorno de los procedimientos en la biblioteca. No se devuelven punteros a los dominios de datos dentro de la biblioteca. La definición de la interfaz se fija en la biblioteca legalmente relevante compilada y ninguna aplicación puede cambiarla. No es imposible eludir la interfaz del software y direccionar dominios de datos de la biblioteca directamente, pero esto no es una buena práctica de programación, es bastante complicada y puede ser clasificada como hackeo.

5.2.1.2.d En los casos en que el software legalmente relevante haya sido separado del software no relevante, el software legalmente relevante debe tener prioridad en el uso de recursos sobre el software no relevante. La tarea de medición (realizada por la parte legalmente relevante del software) no debe ser demorada o bloqueada por otras tareas.

El fabricante es responsable de respetar estas restricciones. Se deben proveer medios técnicos, que prevengan que un programa no legalmente relevante, altere las funciones legalmente relevantes. El programador de la parte del software legalmente relevante tanto como el programador de la parte no legalmente relevante, deben tener instrucciones del fabricante, concernientes a estos requerimientos.

Ejemplos:

1. (I) En el ejemplo 5.2.1.2.a/.c, la aplicación no legalmente relevante, controla el arranque de los procedimientos legalmente relevantes que se realizan en la biblioteca. Omitir una llamada a esos procedimientos podría por supuesto inhibir la función legalmente relevante del sistema. Por lo tanto, se han tomado las siguientes provisiones en el sistema del ejemplo, para cumplimentar el requerimiento 5.2.1.2.d: los sensores digitales, envían los datos de medición de manera encriptada. La llave para el desencriptado está oculta en la biblioteca. Solo los procedimientos que están en la biblioteca conocen la llave y son capaces de leer, desencriptar y mostrar en pantalla los valores medidos. Si el programador de la aplicación desea leer y procesar los valores medidos, está forzado a utilizar los procedimientos legalmente relevantes de la biblioteca, que llevan a cabo todas las funciones legalmente requeridas, cuando son llamadas. La biblioteca contiene procedimientos que exportan los valores de medición desencriptados, permitiendo al programador de la aplicación usarlos para sus propias necesidades, luego de que haya concluido el procesamiento legalmente relevante.

2. (I)/(II) El software de un medidor de electricidad electrónico, lee valores de medición brutos (no procesados) de un conversor analógico-digital (CAD). Para el cálculo correcto de los valores de medición, el retardo entre el evento “datos listos” del CAD y la finalización del almacenamiento en búfer de los valores medidos es crucial. Los valores brutos (no procesados) son leídos por una rutina de servicio de interrupción (ISR), que es iniciada por la señal de “datos listos”. El instrumento es capaz de comunicarse por intermedio de una interfaz con otros dispositivos electrónicos en paralelo, usando otra rutina de servicio de interrupción (comunicación legalmente no relevante). Si interpretamos el requerimiento 5.2.1.2 para una configuración como ésta, se concluye que la rutina de interrupción para procesamiento de los valores de medición, debe tener un orden de prioridad mayor al de la rutina de comunicación.

Los ejemplos considerados desde 5.2.1.2.a á 5.2.1.2.c y 5.2.1.2.d (1) son aceptables como una solución técnica solo para un nivel de severidad normal (I). Si se necesita mayor protección contra fraude o mayor conformidad (ver 8), no es suficiente solo la separación del software y se requieren medios adicionales (o el software completo debe ser considerado bajo control legal).

5.2.2 Indicaciones compartidas

Se puede utilizar una pantalla o una salida de impresión, para presentar tanto la información de la parte legalmente relevante del software y otra información. Los contenidos y el diseño son específicos para el tipo de instrumento y área de aplicación y tienen que estar definidos en la Recomendación relevante. Sin embargo, si la indicación se realiza utilizando una interfaz de usuario de ventanas múltiples, aplican los siguientes requerimientos:

el software que ejecuta la indicación de los valores de medición y otra información legalmente relevante, pertenece a la parte legalmente relevante. La ventana que contiene estos datos debe tener la más alta prioridad, es decir: no debe ser borrada por otro software, o solapada por ventanas generadas por otro software o minimizada o invisibilizada mientras la medición se esté realizando y los resultados presentados sean necesarios para propósitos legalmente relevantes.

Ejemplo:

(I) En un sistema como el descripto en los ejemplos 5.2.1.2.a á 5.2.1.2.d, los valores medidos se muestran en una ventana de software separada. Los medios descriptos en 5.2.1.2.d, garantizan que solo la parte del programa legalmente relevante puede leer los valores medidos. En un sistema operativo con una interfaz de ventanas múltiples, se utiliza un medio técnico adicional para cumplir el requerimiento de 5.2.2: la ventana que muestra los datos legalmente relevantes es generada y controlada por procedimientos de la biblioteca vinculable dinámicamente legalmente relevante (ver 5.2.1.2). Durante la medición, estos procedimientos chequean cíclicamente que la ventana relevante esté siempre sobre todas las otras ventanas abiertas, si así no sucede los procedimientos la colocan arriba de todas.

Si se necesita mayor protección contra fraude (II), una salida de impresión como única indicación, puede no ser apropiada. Debería existir un subconjunto con un medio que incremente la seguridad, que sea capaz de mostrar en pantalla los valores medidos.

El uso de una computadora universal no es apropiado como parte de un sistema de medición, si se necesita mayor protección contra fraude (II). Cuando se necesita prevenir o minimizar el riesgo de fraude se deberían considerar precauciones adicionales, en forma de hardware y software, como cuando se usa una computadora universal (por ejemplo: PC, PDA, etc).

5.2.3 Almacenamiento de datos, transmisión por medio de sistemas de comunicación

Si los valores de medición se utilizan en un lugar diferente al del lugar de medición o no se usan en el momento de la medición, si no después, posiblemente deban salir del instrumento de medición (dispositivo electrónico, subconjunto) y ser almacenados o transmitidos en un medio no seguro antes de ser usados para propósitos legales. En este caso aplican los siguientes requerimientos:

5.2.3.1 El valor de medición almacenado o transmitido debe estar acompañado por toda la información relevante necesaria para uso futuro legalmente relevante.

Ejemplo:

(I)/(II) Un juego de datos puede incluir los siguientes registros:

- Valor de la medición incluyendo la unidad;
- Sello de tiempo de la medición (ver 5.2.3.7);
- Lugar en donde se realizó la medición o identificación del instrumento de medición que se usó para realizar la medición;
- Identificación no ambigua de la medición, por ejemplo: números consecutivos que permitan asignaciones a valores impresos en una factura.

5.2.3.2 Los datos estarán protegidos por recursos de software para garantizar la autenticidad, integridad y si es necesario la veracidad de la información concerniente al momento (tiempo) en que se hizo la medición. El software que muestra en pantalla o que además procesa los valores de medición y los datos que los acompañan, deberá verificar: el momento en que se realizó la medición y la autenticidad e integridad de los datos, luego de haberlos leído del lugar de almacenamiento no seguro o después de haberlos recibido de una canal de transmisión no seguro. Si se detecta una irregularidad, se deben descartar los datos o se los debe marcar como datos no utilizables.

Los módulos de software que preparan los datos para almacenamiento o envío, o que verifican datos luego de leerlos o recibirlos, forman parte de la parte legalmente relevante del software.

Nota: Es apropiado requerir un nivel de severidad más alto, cuando se está considerando una red abierta.

Ejemplo:

(I) El programa del dispositivo transmisor, calcula un checksum del juego de datos (algoritmos tales como BCC, CRC16, CRC32, etc.) y lo agrega al conjunto de datos. Utiliza un valor inicial secreto para este cálculo, en vez del valor dado en el estándar. Este valor inicial se emplea como una llave y se almacena como una constante en el código del programa. El programa receptor o de lectura, también ha almacenado este valor inicial en su código de programa. Antes de usar el juego de datos, el programa receptor calcula el checksum y lo compara con el que está almacenado en el juego de datos. Si ambos valores coinciden, el juego de datos no está falsificado. De otra forma, el programa asume la falsificación y descarta el juego de datos.

5.2.3.3 Para un nivel de protección más alto es necesario aplicar métodos criptográficos. Las llaves confidenciales empleadas para este propósito deben mantenerse en secreto y estar aseguradas en los instrumentos de medición, los dispositivos electrónicos o los subconjuntos involucrados. Se deben proveer medios para que estas llaves puedan ser ingresadas o leídas, solo cuando se rompa un sello.

Ejemplo:

(II) El programa de almacenamiento o de transmisión, genera una "firma electrónica" calculando primero un valor hash[3)] y luego encriptando el valor hash con la llave secreta de un sistema de llave pública [4)]. El resultado es la firma que se adjunta al juego de datos almacenados o transmitidos. El receptor también calcula el valor hash del juego de datos y desencripta la firma adjunta al juego de datos con la llave pública. Se comparan los valores desencriptados y calculados del valor hash. Si son iguales, el juego de datos no ha sido falsificado (está probada la integridad). Para verificar el origen del juego de datos, el receptor debe saber si la llave pública realmente pertenece al transmisor, es decir: al dispositivo transmisor. Para ésto, la llave pública se muestra en la pantalla del instrumento de medición y se puede registrar previamente, por ejemplo: en conjunto con el número de serie del dispositivo, cuando éste se verifica legalmente en el campo. Si el receptor está seguro de que ha usado la llave pública correcta para desencriptar la firma, entonces la autenticidad del juego de datos también está probada.

5.2.3.4 Almacenamiento automático

5.2.3.4.a Cuando al considerar la aplicación, se requiere almacenamiento de datos, los datos de medición deben ser almacenados automáticamente cuando se concluye la medición, es decir: cuando ha sido generado el valor final utilizado para el propósito legal.

El dispositivo de almacenamiento debe tener la suficiente inalterabilidad, para asegurar que los datos no se corrompan en condiciones normales de almacenamiento. Debe haber suficiente memoria de almacenamiento para cualquier aplicación particular

Cuando el valor final utilizado con propósitos legales es el resultado de un cálculo, todos los datos que son necesarios para el cálculo deben ser almacenados automáticamente con el valor final.

Nota: Valores de medición acumulativos tales como, por ejemplo: energía eléctrica o volumen de gas, deben ser actualizados constantemente. Como siempre se usa el mismo dominio de datos (variable de programa), el requerimiento concerniente a la capacidad de almacenamiento no es aplicable a las mediciones acumulativas.

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

4) Algoritmos aceptables: RSA (llave de 1024 bit de longitud), Elliptic Curves (llave de 160 bit de longitud), o equivalente.

5.2.3.4.b Los datos almacenados pueden borrarse si:

- la transacción ya ha sido liquidada; o bien
- estos datos son imprimidos por un dispositivo impresor sujeto a control legal.

Nota: Otras regulaciones nacionales generales (por ejemplo: para propósitos impositivos) pueden incluir limitaciones estrictas en relación con borrado de datos de medición.

5.2.3.4.c Luego que se hayan cumplido los requerimientos de la sección 5.2.3.4.b y cuando la memoria está llena, se permite el borrado de los datos memorizados cuando se cumplen las dos condiciones que siguen:

- los datos se borran en el mismo orden en que fueron grabados y se respetan las reglas establecidas para la aplicación en cuestión;
- el borrado se realiza o automáticamente o al realizar una operación manual especial.

Nota: Se debe considerar el uso de derechos de acceso adicionales, cuando se implementa la "operación manual especial" prescripta en la segunda viñeta.

5.2.3.5 Retardo de la transmisión

La medición no debe ser inadmisiblemente influenciada por un retardo de la transmisión.

5.2.3.6 Interrupción de la transmisión

Si los servicios de la red no están disponibles, no se deben perder datos de medición. El proceso de medición debería detenerse para evitar la pérdida de datos de medición.

Nota: Se debe considerar que hay que distinguir entre mediciones estáticas y dinámicas.

Ejemplo:

(I)/(II) El dispositivo transmisor espera hasta que el receptor haya enviado una afirmación de recepción correcta del juego de datos. El dispositivo transmisor mantiene el juego de datos en un búfer hasta que esta afirmación haya sido recibida. El búfer puede tener la capacidad para más de un juego de datos, organizado como una fila FIFO[5)]

5.2.3.7 Sello de tiempo

El sello de tiempo debe leerse del reloj del dispositivo. Dependiendo del tipo de instrumento o del área de aplicación, configurar el reloj puede ser legalmente relevante y se deben tomar medidas de protección apropiadas de acuerdo con el nivel de severidad que se va a aplicar (ver 5.1.3.2.c).

El reloj interno de un instrumento de medición autónomo tiende a tener una gran incertidumbre porque no hay manera de sincronizarlo con el reloj global. Si la información concerniente a los datos de tiempo (momento) en que se realiza la medición es necesaria para un campo específico de aplicación, se debe aumentar la confiabilidad del reloj interno del instrumento de medición utilizando medios específicos.

5) FIFO: First in – first out

Ejemplo:

(II) La fiabilidad del dispositivo reloj interno (controlado por cuarzo) del instrumento de medición está mejorada por redundancia: un temporizador es incrementado por el reloj del microcontrolador que proviene de otro cristal de cuarzo. Cuando el valor del temporizador alcanza un valor preconfigurado, por ejemplo: 1 segundo, se fija un marcador 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 reloj (controlado por cuarzo) y calcula la diferencia en los segundos contados por el software. Si la diferencia está entre los límites predefinidos, el contador de software se reinicia y el procedimiento se repite; pero si la diferencia excede los límites, el software dispara una reacción de error apropiada.

5.2.4 Compatibilidad de los sistemas operativos y el hardware, portabilidad

5.2.4.1 El fabricante definirá el entorno adecuado de software y de hardware. Los recursos mínimos y una configuración adecuada (por ejemplo: procesador, RAM, HDD, comunicación específica, versión del sistema operativo, etc) necesaria para un correcto funcionamiento, deben ser declarados por el fabricante y registrados en el certificado de aprobación de modelo.

5.2.4.2 Se deben proveer recursos técnicos en el software legalmente relevante para impedir la operación, si no se cumplen los requerimientos mínimos de configuración. El sistema debe ser operado solo en el entorno especificado por el fabricante, para su correcto funcionamiento.

Por ejemplo: en el caso en que se especifique para el correcto funcionamiento del sistema un entorno invariable, se deben proveer los medios que mantengan fijo el marco de operación. Esto aplica especialmente a una computadora universal que lleva a cabo funciones legalmente relevantes.

Fijar el hardware, el sistema operativo o la configuración del sistema de una computadora universal o incluso excluir el uso de una computadora universal estándar, debe considerarse en los siguientes casos:

- si se requiere alto nivel de conformidad (ver 5.2.5 (d));
- si se requiere un software fijo (por ejemplo 5.2.6.3.b para actualización trazable del software);
- si se tienen que implementar algoritmos criptográficos o llaves (ver 5.2.3).

5.2.5 Conformidad de los dispositivos fabricados con el modelo aprobado

El fabricante debe producir los dispositivos y el software legalmente relevante que sean conformes al modelo aprobado y a la documentación presentada para la aprobación. Hay diferentes niveles de requerimientos de conformidad:

a) identidad de las *funciones legalmente relevantes* descriptas en la documentación (6.1) de cada dispositivo con aquellas del modelo (el código ejecutable puede diferir);

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

c) identidad de *todo el código fuente legalmente relevante*; y

d) identidad de *todo el código ejecutable*.

La Recomendación relevante especificará cual es el grado apropiado de conformidad. Esta Recomendación puede definir también un subconjunto a partir de esos grados de conformidad.

Con excepción del requerimiento (d) puede haber una parte del software que no tenga requerimientos de conformidad, si está separada de la parte legalmente relevante de acuerdo con 5.2.1.2.

Los medios descriptos en 5.1.1 y 5.2.1 serán provistos para que la conformidad sea evidente.

Nota: (a) y (b) se deben aplicar en el caso de un nivel de severidad normal, (c) y (d) deben aplicarse en el caso de un nivel de severidad elevado.

5.2.6 Mantenimiento y reconfiguración

La actualización en campo del software legalmente relevante de un instrumento de medición debe ser considerada como:

- una modificación del instrumento de medición, cuando se cambia el software por otra versión aprobada;
- una reparación del instrumento de medición, cuando se reinstala la misma versión.

Un instrumento de medición que ha sido modificado o reparado mientras está en servicio, puede requerir verificación inicial o posterior, dependiendo de las regulaciones nacionales.

El software que no es necesario para el correcto funcionamiento del instrumento de medición no requiere verificación luego de ser actualizado.

5.2.6.1 Solo se permite el uso de versiones del software legalmente relevante, que sean conformes al modelo aprobado. (ver 5.2.5). La aplicación de los requerimientos siguientes depende del tipo de instrumento y se elaborará en la Recomendación OIML relevante. Puede diferir incluso, dependiendo del tipo de instrumento en consideración. Las siguientes opciones 5.2.6.2 y 5.2.6.3 son alternativas equivalentes. Este tema se refiere a la verificación en campo. Referirse a la Sección 7 para restricciones adicionales.

5.2.6.2 Actualización verificada

El software que debe ser actualizado se puede cargar localmente, es decir directamente en el dispositivo de medición o de manera remota utilizando una red. La carga y la instalación pueden ser dos pasos diferentes (como se muestra en la Fig. 1) o combinados en uno, dependiendo de las necesidades de la solución técnica. Una persona debe estar en el lugar de instalación del instrumento de medición para verificar la efectividad de la actualización. Luego de la actualización del software legalmente relevante de un instrumento de medición (cambio por otra versión aprobada o reinstalación) el instrumento de medición no puede ser empleado para propósitos legales antes de que se le realice una verificación, como se describe en la Sección 7 y se hayan renovado los medios de protección (si no se indica lo contrario en la Recomendación de OIML relevante o en el certificado de aprobación).

5.2.6.3 Actualización trazable

El software se implementa en el instrumento de acuerdo a los requerimientos para Actualización Trazable (5.2.6.3.a 5.2.6.3.g), si cumple con la Recomendación OIML relevante. La Actualización Trazable es el procedimiento de cambiar el software en un instrumento o en un dispositivo verificado, luego de lo cual no es necesario la subsecuente verificación en campo por parte de una persona responsable. El software a actualizar puede ser cargado localmente, es decir directamente en el dispositivo de medición o de manera remota utilizando una red. La actualización del software se graba en un registro de auditoría (ver 3.1.2.). El procedimiento de Actualización Trazable comprende varios pasos: carga, verificación de integridad, verificación del origen (autentificación), instalación, logueo y activación.

5.2.6.3.a La Actualización Trazable del software debe ser automática. Al completar el procedimiento de actualización, el entorno de protección del software debe estar en el mismo nivel que el requerido por la aprobación de modelo.

5.2.6.3.b El instrumento de medición de objetivo (dispositivo electrónico, subconjunto) debe tener un software legalmente relevante fijo, que no pueda ser actualizado y que contenga todas las funciones de verificación necesarias para cumplimentar los requerimientos de Actualización Trazable.

5.2.6.3.c Se deben emplear medios técnicos para garantizar la autenticidad del software cargado, es decir que éste proviene del propietario del certificado de aprobación de modelo. Si el software cargado falla en la verificación de autenticidad, el instrumento debe descartarlo y utilizar la versión previa del software o cambiar su modo de operación a no utilizable.

Ejemplo:

(II) El chequeo de autenticidad se realiza utilizando medios criptográficos como por ejemplo un sistema de llave pública. El propietario del certificado de aprobación de modelo (en general el fabricante del instrumento de medición) genera una firma electrónica del software que debe ser actualizado, utilizando su llave secreta. La llave pública se almacena en la parte fija del software del instrumento de medición. La firma se verifica utilizando llave pública cuando se carga el software en el instrumento de medición. Si la firma del software cargado es la correcta, el software se instala y se activa; si la verificación falla, el software fijo descarta el software que ha cargado y utiliza la versión previa del software o cambia el modo de operación del instrumento a no utilizable.

5.2.6.3.d Se deben utilizar medios técnicos para asegurar la integridad del software a cargar, es decir que antes de ser cargado, no ha sido inadmisiblemente cambiado. Esto se puede realizar agregando un checksum o un código hash del software a cargar y verificándolo durante el procedimiento de carga. Si el software cargado falla esta prueba, el instrumento debe descartarlo y utilizar la versión previa del software o cambiar su modo de operación a no utilizable. En este modo, las funciones de medición deben estar inhibidas. Solo será posible retomar el proceso de descarga, sin omitir ningún paso del diagrama de flujo para Actualización Trazable.

5.2.6.3.e Se deben utilizar medios técnicos apropiados, por ejemplo: un registro de auditoría, para asegurar que las Actualizaciones Trazables del software legalmente relevante sean adecuadamente trazables en el instrumento, para verificación posterior y vigilancia o inspección.

El registro de auditoria debe contener mínimamente la siguiente información: éxito/falla del procedimiento de actualización, identificación del software de la versión instalada, identificación del software de la versión instalada previamente, sello de tiempo del evento, identificación de la parte descargada. Se genera una entrada por cada intento de actualización, sin tener en cuenta si ha sido o no exitoso.

El dispositivo de almacenamiento que soporta la Actualización Trazable debe tener una capacidad suficiente para asegurar la trazabilidad de las Actualizaciones Trazables del software legalmente relevante, entre al menos dos verificaciones sucesivas en el campo/inspección. Luego de haber alcanzado el límite de almacenamiento para el registro de auditoría, deberá estar asegurado por medios técnicos, que no sean posibles más descargas sin romper un sello.

Nota: Este requerimiento permite a las autoridades de inspección, que son responsables de la vigilancia metrológica de los instrumentos legalmente controlados, rastrear las Actualizaciones Trazables del software legalmente relevante, a lo largo de un período de tiempo adecuado (que depende de la legislación nacional).

5.2.6.3.f Dependiendo de las necesidades y de la legislación jurídica nacional, puede ser necesario para el usuario o el propietario del instrumento de medición, tener que dar su consentimiento para una descarga. El instrumento de medición deberá tener un subconjunto/dispositivo electrónico para que el usuario o propietario exprese su consentimiento, por ejemplo: una tecla de presión que accione antes de que comience la descarga. Debe ser posible habilitar y deshabilitar este subconjunto/dispositivo electrónico, por ejemplo: por medio de un interruptor que pueda ser sellado o por medio de un parámetro. Si el subconjunto/dispositivo electrónico está habilitado, cada descarga debe ser iniciada por el usuario o el propietario. Si está deshabilitado el usuario o el propietario no necesitan realizar ninguna acción para llevar a cabo una descarga.

5.2.6.3.g Si no se pueden cumplir los requerimientos de 5.2.6.3.a á 5.2.6.3.f, igual es posible actualizar la parte del software no legalmente relevante. En este caso se deben cumplir los siguientes requerimientos:

- hay una separación inconfundible entre el software legalmente relevante y el no legalmente relevante de acuerdo con 5.2.1;
- la parte legalmente relevante del software (en su totalidad) no puede ser actualizada sin romper un sello;
- está establecido en el certificado de aprobación de modelo, que es aceptable la actualización de las partes no legalmente relevantes.

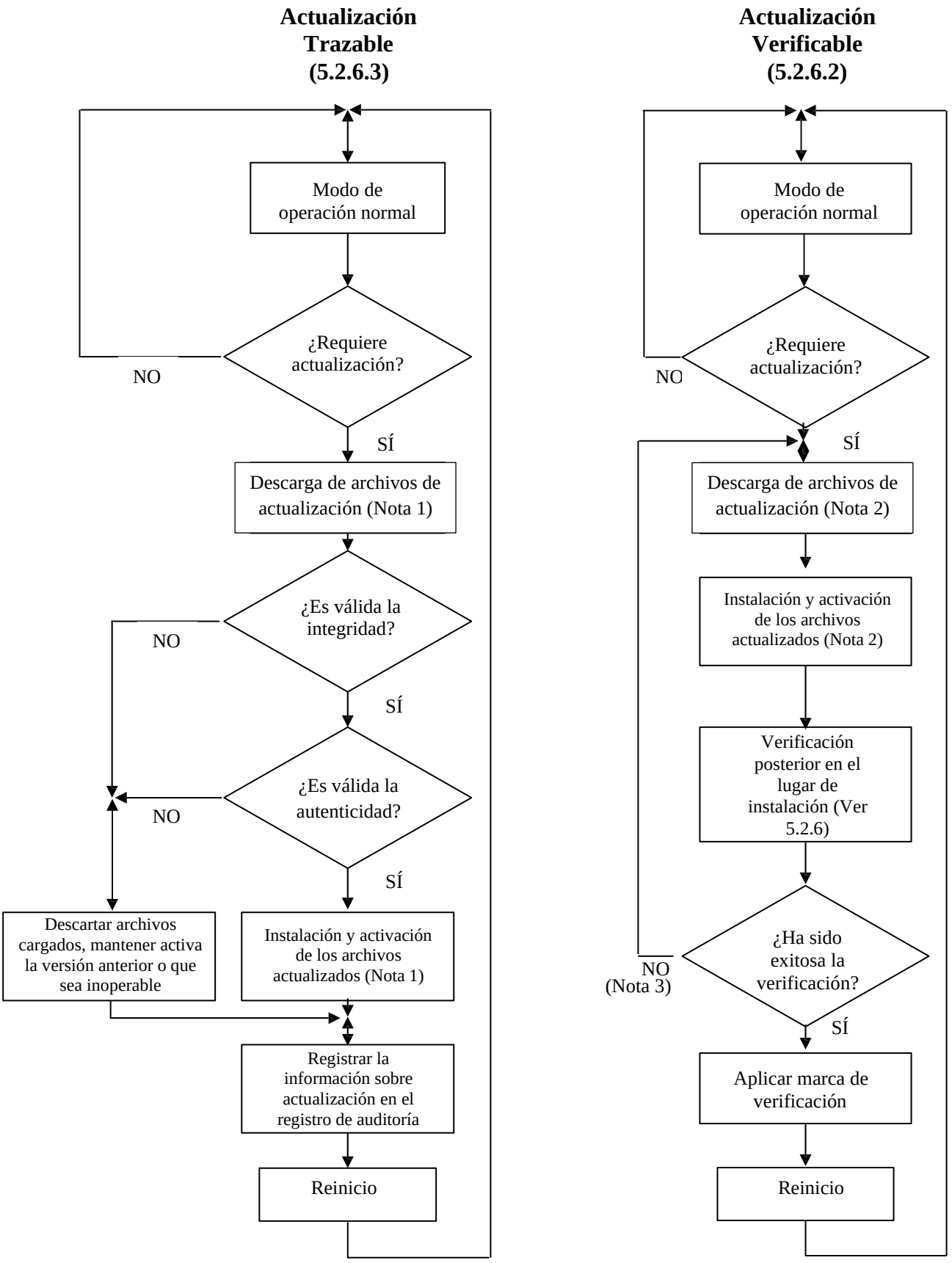

Figura 1 Procedimiento de actualización del software

Notas: (1) En el caso de una Actualización Trazable, la actualización se separa en dos pasos: “carga” e “instalación/activación”. Esto implica que el software es almacenado temporalmente luego de ser cargado, sin ser activado, porque debe ser posible descartarlo y volver a la versión anterior, si la verificación falla.

(2) En el caso de una Actualización Verificada, el software puede también cargarse y almacenarse temporalmente antes de la instalación, pero dependiendo de la solución técnica, la carga y la instalación pueden además realizarse en un solo paso.

(3) En este caso, solo se considera la falla de la verificación debida a la actualización del software. Las fallas debidas a otras razones no requieren recarga y reinstalación del software. Ésto se simboliza por la rama NO, del diagrama.

5.2.6.4 La Recomendación relevante de OIML puede requerir, que la configuración de ciertos parámetros específicos de dispositivo esté disponible para el usuario. En este caso, el instrumento de medición debe poseer una función, que registre de forma automática e imborrable, cualquier ajuste del parámetro específico del dispositivo, por ejemplo: un registro de auditoría. El instrumento debe ser capaz de mostrar los datos registrados.

Nota: Un contador de eventos no es una solución aceptable.

5.2.6.5 Los medios de trazabilidad y los registros son parte del software legalmente relevante y deben ser protegidos como tales. El software empleado para mostrar el registro de auditoria (5.2.6.2; 5.2.6.3) pertenece al software fijo legalmente relevante.

6 Aprobación de modelo

6.1 Documentación a remitir para la aprobación de modelo

Para la aprobación de modelo el fabricante del instrumento de medición deberá declarar y documentar todas las funciones del programa, las estructuras de datos relevantes e interfaces de software de la parte del software legalmente relevante, que están implementadas en el instrumento. No deben existir funciones indocumentadas ocultas.

Los comandos y sus efectos deberán ser descriptos de manera completa, en la documentación del software que se envíe para la aprobación de modelo. El fabricante declarará la totalidad de la documentación de los comandos. Si los comandos se pueden enviar por una interfaz de usuario, se deberán describir de manera completa en la documentación del software que se enviará para la aprobación de modelo.

Además, la presentación de la documentación para aprobación de modelo debe estar acompañada por un documento o por alguna otra evidencia que sostenga la premisa de que el diseño y las características del software del instrumento de medición, cumplen con los requerimientos de la Recomendación relevante de OIML en la cual han sido incorporados los requerimientos generales de este Documento.

6.1.1 La documentación típica (para cada instrumento de medición, dispositivo electrónico o subconjunto) incluye básicamente:

- una descripción del software legalmente relevante y de cómo se cumplen los requerimientos:
  - lista de los módulos de software que pertenecen a la parte legalmente relevante (Anexo B) incluyendo una declaración de que todas las funciones legalmente relevantes están incluidas en la descripción;
  - descripción de las interfaces de software de la parte del software legalmente relevante y de los comandos y flujos de datos que utilizan esta interfaz, incluyendo una declaración de completitud (Anexo B);

  - descripción de la generación de la identificación del software;
  - dependiendo del método de validación elegido en la Recomendación relevante de OIML (ver 6.3 and 6.4) el código fuente debe ser accesible para la autoridad de ensayo, si la Recomendación relevante de OIML requiere alto nivel de conformidad o alto grado de protección;
  - listado de los parámetros que deben ser protegidos y descripción de los medios de protección;

- una descripción de la configuración adecuada del sistema y de los recursos mínimos que se requieren (ver 5.2.4);
- una descripción de los medios de seguridad del sistema operativo (contraseña, etc. si es aplicable);
- una descripción del/ de los método/s de sellado del software;
- un resumen del hardware del sistema, por ejemplo: diagrama en bloque de la topología, tipo/s de computadora/s, tipo de red, etc. Cuando un componente del hardware se considera legalmente relevante, o cuando realiza funciones legalmente relevantes, también se debe identificar;
- una descripción de la exactitud de los algoritmos, (por ejemplo: filtrado de los resultados de la conversión A/D, cálculo del precio, algoritmos de redondeo, etc.);
- una descripción de la interfaz de usuario, de los menús y de la comunicación;
- la identificación del software y las instrucciones para poder leerla de un instrumento en uso;
- la lista de los comandos de cada interfaz de hardware del instrumento de medición/dispositivo electrónico/subconjunto incluyendo una declaración de completitud;
- la lista de los errores de durabilidad que son detectados por el software y si es necesario para una mejor comprensión, una descripción de los algoritmos de detección;
- una descripción de los juegos de datos almacenados o transmitidos;
- si el software realiza una detección de fallas, una lista de las fallas que son detectadas y una descripción del algoritmo de detección;
- el manual de operación.

6.2 Requerimientos del proceso de aprobación

Los procedimientos de ensayo en el marco de la aprobación de modelo, por ejemplo: los que se describen en OIML D 11:2004, se basan en configuraciones y condiciones de ensayo bien definidas y también en mediciones comparativas precisas. El “ensayo” y la “validación” del software son procesos diferentes. En general la exactitud o la corrección del software, no se pueden medir en un sentido metrológico, aunque hay estándares que prescriben como “medir” la calidad del software [por ejemplo: ISO/IEC 14598]. Los procedimientos que aquí se describen, tienen en cuenta tanto las necesidades de la metrología legal como también las de los bien conocidos métodos de validación y ensayo de la ingeniería del software, pero que no tienen los mismos fines (por ejemplo: un desarrollador de software que busca errores pero que también optimiza el desempeño). Como se muestra en 6.4, cada requerimiento del software necesita una adaptación individual de los procedimientos de validación apropiados. El empeño por el procedimiento debe reflejar la importancia del requerimiento en términos de exactitud, confiabilidad y protección contra la corrupción.

El objetivo es validar el hecho de que el instrumento a ser aprobado, cumple con los requerimientos de la Recomendación relevante de OIML. Para los instrumentos controlados por software el procedimiento de validación comprende exámenes, análisis y ensayos; la Recomendación relevante de OIML incluirá una selección apropiada de los métodos descriptos más abajo.

Los métodos descriptos abajo, se enfocan en el examen de modelo. Las verificaciones de cada instrumento individual, que está en uso en campo, no están cubiertas por estos métodos de validación. Para más información, referirse a la Sección 7 “*Verificación*”.

Los métodos especificados para la validación del software se describen en 6.3. Las combinaciones de estos métodos conformando un procedimiento de validación completo, adaptado a todos los requerimientos definidos en la Sección 5, se especifican en 6.4.

6.3 Métodos de validación (examen del software)

6.3.1 Resumen de los métodos y su aplicación

La selección y secuencia de los métodos siguientes no están prescriptas y pueden variar en un procedimiento de validación de caso a caso.

Abreviatura	**Descripción**	**Aplicación**	**Precondiciones, herramientas para la aplicación**	**Habilidades Requeridas para realización**
AD	Análisis de la documentación y validación del diseño (6.3.2.1)	Siempre	Documentación	-
VFTM	Validación por ensayo funcional de funciones metrológicas (6.3.2.2)	Exactitud de los algoritmos, incertidumbre, algoritmos de compensación y corrección, reglas para el cálculo de precio	Documentación	-
VFTSw	Validación por ensayo funcional de funciones del software (6.3.2.3)	Funcionamiento correcto de: comunicación/indicación/protección contra fraude. Protección: errores de operación/de parámetros. Detección de fallas	Documentación, herramientas comunes de software	-
DFA	Análisis del flujo de datos metrológicos (6.3.2.4)	Separación del software, evaluación del impacto de los comandos en las funciones del instrumento	Código fuente, herramienta común del software (procedimiento simple), herramientas (procedimiento sofisticado)	Conocimiento de lenguajes de programación. Aprendizaje del método (necesario).
CIWT	Inspección del Código y guía (tutorial) (6.3.2.5)	Para todos los usos	Código fuente, herramienta común del software	Conocimiento de lenguajes de programación, protocolos y otros temas de TI
SMT	Ensayo de módulo de software (6.3.2.6)	Para todos los usos cuando la entrada y la salida pueden ser claramente definidas	Código fuente, entorno de ensayo, herramientas especiales de software	Conocimiento de lenguajes de programación, protocolos y otros temas de TI. Aprendizaje del uso de herramientas (necesario).

Tabla 1: Resumen de los métodos de validación seleccionados propuestos

Nota: Editores de texto, editores hexadecimales, etc, son considerados como “herramientas comunes de software”

6.3.2 Descripción de los métodos de validación seleccionados

6.3.2.1 Análisis de la Documentación y de la Especificación/Validación del Diseño (AD)

Aplicación:

Éste es el procedimiento básico que debe ser aplicado, en cualquier caso.

Precondiciones:

El procedimiento está basado en la documentación del fabricante del instrumento de medición. Dependiendo de las exigencias, esta documentación deberá tener el alcance adecuado:

(1) especificación de forma general, de las funciones del instrumento accesibles desde el exterior (apropiado para: instrumentos simples sin interfaces excepto una pantalla, con todas las características verificables mediante pruebas funcionales y con bajo riesgo de fraude);

(2) especificación de las funciones de software y de las interfaces (necesario para instrumentos: con interfaces, con funciones que no pueden ser probadas funcionalmente y con riesgo de fraude incrementado). La descripción debe hacer evidente y explicar todas las funciones del software, que puedan tener un impacto en las características metrológicas;

(3) En lo que concierne a las interfaces: la documentación deberá incluir una lista completa de comandos o señales que el software es capaz de interpretar. El efecto de cada comando debe ser documentado en detalle. Se describirá la forma en que el instrumento reacciona a los comandos no documentados;

(4) Si es necesario para entender o evaluar las funciones del software, será sumistrada documentación adicional del software para: algoritmos de medición complejos, funciones criptográficas o restricciones de tiempo que sean cruciales;

(5) Cuando no es claro como validar una función de un programa de software, la responsabilidad de desarrollar un método de prueba será del fabricante. Adicionalmente, el programador deberá estar disponible para el examinador, en el caso en que sea necesario responder preguntas.

Una precondición general para el examen es la completitud de la documentación y la identificación clara del IBE, es decir de los paquetes de software que contribuyen a las funciones metrológicas (ver 6.1.1).

Descripción:

El examinador evalúa las funciones y características del instrumento de medición utilizando la descripción verbal y las representaciones gráficas y decide si cumplen con los requerimientos de la Recomendación relevante de OIML. Deben ser considerados y evaluados los requerimientos metrológicos como así también los requerimientos funcionales del software definidos en la Sección 5 (por ejemplo: protección contra fraude, protección de parámetros de ajuste, funciones no autorizadas, comunicación con otros dispositivos, actualización del software, detección de fallas, etc.). Esta tarea puede realizarse utilizando el Formato de Reporte de Evaluación de Software (ver Anexo B).

Resultado:

El procedimiento genera un resultado para todas las características del instrumento de medición, siempre y cuando el fabricante haya enviado la documentación apropiada. El resultado deberá estar documentado en una sección relacionada con el software, en un Reporte de Evaluación de Software (ver Anexo B) incluido en el Formato de Reporte de Evaluación de la Recomendación relevante de OIML.

Procedimientos Complementarios:

Se deben aplicar procedimientos adicionales, si el examen de la documentación no provee resultados de validación comprobados. En la mayoría de los casos “la validación de las funciones metrológicas por ensayos funcionales” (ver 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 Contained in Medical Devices, 29 May 1998 [10]; IEC 61508-7, 2000 - 3 [9].

6.3.2.2 Validación por Ensayos Funcionales de las Funciones Metrológicas (VFTM)

Aplicación:

Corrección de los algoritmos que calculan el valor de medición a partir de los datos brutos (no procesados) para: linealización de una característica, compensación de las influencias ambientales, redondeo en el cálculo del precio, etc.

Precondiciones:

Manual de operación, modelo en funcionamiento, referencias metrológicas y equipamiento de ensayo.

Descripción:

La mayoría de los métodos y ensayos de aprobación descriptos en las Recomendaciones OIML están basados en mediciones de referencia bajo diferentes condiciones. Su aplicación no está restringida a una cierta tecnología del instrumento. Aunque el resultado del ensayo no apunte primariamente a validar el software, se puede interpretar como una validación de algunas partes del software, en general incluso las más importantes en el sentido metrológico. Si los ensayos descriptos en la Recomendación relevante de OIML cubren todas las características metrológicamente relevantes del instrumento, las partes correspondientes del software pueden considerarse validadas. En general no se debe aplicar ningún ensayo o análisis adicional del software, para validar las características metrológicas del instrumento de medición.

Resultado:

La corrección de los algoritmos es válida o inválida. Los valores de medición bajo todas las condiciones están dentro del EMT o no.

Procedimientos complementarios:

El método es normalmente una mejora de 6.3.2.1. En ciertos casos puede ser más simple o efectivo, combinar el método con análisis basados en el código fuente (6.3.2.5) o simulando señales de entrada (6.3.2.6) por ejemplo: para mediciones dinámicas.

Referencias:

Recomendaciones específicas varias de OIML.

6.3.2.3 Validación por Ensayo Funcional de las Funciones de Software (VFTSw)

Aplicación:

Validación de, por ejemplo: protección de parámetros, indicación de la identificación de un software, detección de fallas soportada por el software, configuración del sistema (especialmente del entorno del software), etc.

Precondiciones:

Manual de operación, documentación del software, modelo en funcionamiento, equipamiento de ensayo.

Descripción:

Las funciones requeridas descriptas en el manual de operación, en la documentación del instrumento o en la documentación del software se chequean de manera práctica. Si éstas están controladas por software, se considerarán validadas si funcionan correctamente, sin ningún análisis de software adicional.

Las funciones aquí consideradas son, por ejemplo:

- la operación normal del instrumento, si su operación está controlada por software. Se debe actuar sobre todos los interruptores o llaves y sobre las combinaciones posibles de los mismos que se describieron y luego evaluar la reacción del instrumento. En interfaces gráficas de usuario, todos los menús y elementos gráficos deben ser activados y chequeados;
- la efectividad de protección de parámetro se puede verificar activando el medio de protección y tratando de cambiar un parámetro;
- la efectividad de protección de datos almacenados se puede verificar cambiando algunos datos en el archivo y luego verificando si ésto ha sido detectado por el programa;
- la generación y la indicación de la identificación del software se puede validar mediante verificación práctica;
- si la detección de fallas es soportada por el software, las partes relevantes del software se pueden validar provocando, implementando o simulando una falla y verificando la reacción correcta del instrumento;
- si se afirma que la configuración o el entorno del software legalmente relevantes son fijos, se pueden verificar los medios de protección realizando cambios no autorizados. El software debe inhibir esos cambios o debe dejar de funcionar.

Resultado:

La función controlada por software que se está considerando está bien o no está bien.

Procedimientos complementarios:

Algunas características o funciones de un instrumento controlado por software, no pueden validarse en la práctica como se describió. Si el instrumento tiene interfaces, en general no es posible detectar comandos no autorizados, solo mediante el envío aleatorio de comandos. Además de lo anterior, se necesita un transmisor para generar estos comandos. Para el método de nivel de validación normal 6.3.2.1, incluir una declaración del fabricante puede cubrir este requerimiento. Para el examen de nivel extendido, es necesario un análisis de software como en 6.3.2.4 o 6.3.2.5.

Referencias:

FDA Guidance for Industry Part 11, August 2003 [11]; WELMEC Guide 2.3 [12]; WELMEC Guide 7.2 [13].

6.3.2.4 Análisis del flujo de datos metrológicos

Aplicación:

Construcción del flujo de valores de medición, a través del dominio de datos sujetos a control legal. Examen de la separación del software.

Precondiciones:

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

Descripción:

El objetivo de este método es encontrar todas las partes del software, que están involucradas en el cálculo del valor de medición o que pueden tener un impacto sobre él.

El proceso comienza en el puerto de hardware en donde están disponibles los valores brutos de medición (sin procesar) que provienen del sensor y que son recibidos por una subrutina que lee estos valores brutos. Esta subrutina los almacenará en una variable luego de, posiblemente, haber hecho algunos cálculos. Desde esta variable otra subrutina lee el valor intermedio y así sucesivamente hasta que se muestre en la pantalla, el valor de medición final. Todas las variables que se usan para almacenar los valores de medición intermedios y todas las subrutinas que transportan estos valores se pueden encontrar en el código fuente, simplemente usando un editor de texto y un programa de búsqueda de texto para encontrar los nombres de la variable o subrutina, en otro archivo de código fuente que no sea el que está en ese momento abierto en el editor de texto.

Usando este método se pueden encontrar otros flujos de datos, por ejemplo: desde las interfaces al intérprete de los comandos recibidos. Además, se puede detectar si se ha tratado de eludir una interfaz de software (ver 5.2.1.2).

Resultado:

Se puede validar si la separación del software según 5.2.1.2 está bien o no está bien.

Procedimientos complementarios:

Se recomienda este método si se efectúa la separación del software y si se requiere un alto grado de conformidad o una fuerte protección contra la manipulación. Es una mejora a 6.3.2.1 hasta 6.3.2.3 y a 6.3.2.5.

Referencia:

IEC 61131-3.

6.3.2.5 Inspección del Código y guía (tutorial) (CIWT)

Aplicación:

Usando este método se puede validar cualquier característica del software, si es necesario un examen más exhaustivo.

Precondiciones:

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

Descripción:

El examinador recorre el código fuente asignación por asignación, evaluando la parte respectiva del código para determinar si se cumplen los requerimientos y si las funciones del programa y características cumplen con la documentación.

El examinador también puede concentrarse en algoritmos o funciones que ha identificado como complejos, propensos a errores, insuficientemente documentados, etc, e inspeccionar la parte respectiva del código fuente por medio de análisis y verificación.

Antes de estos pasos de análisis, el examinador habrá identificado la parte del software legalmente relevante, por ejemplo: aplicando el análisis del flujo de datos metrológicos (ver 6.3.2.4). En general la inspección (o recorrido) del código se limita a esta parte. Combinando ambos métodos el esfuerzo del examen es mínimo comparado con la aplicación de estos métodos en la producción normal de software, con el objetivo de producir programas libres de fallas y optimizar el desempeño.

Resultado:

Implementación compatible con la documentación del software y en cumplimiento con los requerimientos o no.

Procedimientos complementarios

Este es un método mejorado, adicional a 6.3.2.1 y 6.3.2.4. Normalmente solo se aplica en verificaciones al azar.

Referencia:

IEC 61508-7:2000 – 3 [9].

6.3.2.6 Ensayo de Módulos de Software (SMT)

Aplicación:

De aplicación solo si se requiere alta conformidad y protección elevada contra fraude. Este método se aplica cuando las funciones de un programa no se pueden examinar exclusivamente a partir de la información escrita. Es apropiado y económicamente ventajoso, en la validación de algoritmos de medición dinámicos.

Precondiciones:

Código fuente, herramientas de desarrollo (al menos un compilador), entorno de funcionamiento del módulo de software bajo ensayo, juego de datos de entrada y su correspondiente y correcto juego de datos de salida de referencia o herramientas para automatización. Habilidades en TI, conocimiento de lenguajes de programación. Se recomienda cooperación con el programador del módulo bajo ensayo.

Descripción:

El módulo de software bajo ensayo, se integra en un entorno de ensayo, es decir un módulo de programa de ensayo específico que llama al módulo bajo ensayo y lo provee con todos los datos necesarios de entrada. El programa de ensayo recibe los datos de salida del módulo bajo ensayo y los compara con los valores de referencia esperados.

Resultado:

Los algoritmos de medición u otras funciones ensayadas son correctas o no lo son.

Procedimientos complementarios:

Este es un método mejorado, adicional a 6.3.2.2 ó 6.3.2.5. Solo 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 relevante de OIML puede especificar detalles concernientes al proceso de validación, incluyendo:

a) cuál de los métodos de validación descriptos en 6.3 será llevado a cabo para el requerimiento en consideración;

b) cómo se realizará la evaluación de los resultados de ensayo;

c) qué resultado se incluirá en el reporte de ensayo y cuál se integrará en el certificado de ensayo (ver Anexo B).

En la Tabla 2 se definen dos niveles alternativos, A y B, para los procedimientos de validación. El nivel B implica un examen más extenso comparado con A. Se puede hacer una selección entre los procedimientos de validación tipo A y B en la Recomendación relevante de OIML- diferente o igual para cada requerimiento-de acuerdo con lo que se espere en relación con:

- riesgo o fraude;
- área de aplicación;
- conformidad requerida con el modelo aprobado;
- riesgo de resultados de medición erróneos debido a errores de operación.

	Requerimiento	Procedimiento de Validación A (examen de nivel normal)	Procedimiento de Validación B (examen de nivel extendido)	Comentario
5.1.1	Identificación del Software	AD + VFTSw	AD + VFTSw + CIWT	Seleccionar “B” si se requiere alta conformidad
5.1.2	Corrección de los algoritmos y de las funciones	AD + VFTM	AD + VFTM + CIWT/SMT	
Protección del Software				
5.1.3.1	Prevención de mal uso	AD + VFTSw	AD + VFTSw	
5.1.3.2	Protección contra fraude	AD + VFTSw	AD + VFTSw + DFA/CIWT/SMT	Seleccionar “B” en caso de riesgo de fraude alto
Soporte de las características del hardware				
5.1.4.1	Soporte de detección de fallas	AD + VFTSw	AD + VFTSw + CIWT + SMT	Seleccionar “B” si se requiere alta confiabilidad
5.1.4.2	Soporte de protección de durabilidad	AD + VFTSw	AD + VFTSw + CIWT + SMT	Seleccionar “B” si se requiere alta confiabilidad
Especificando y separando las partes relevantes y especificando las interfaces de las partes				
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 por medio de sistemas de comunicación	AD + VFTSw	AD + VFTSw + CIWT/SMT	Seleccione “B” si está prevista la transmisión de datos de medición en un sistema abierto
5.2.3.1	El valor de medición almacenado o transmitido debe estar acompañado por toda la información relevante necesaria para uso futuro legalmente relevante.	AD + VFTSw	AD + VFTSw + CIWT/SMT	Seleccione “B” en caso de riesgo alto de fraude
5.2.3.2	Los datos estarán protegidos por recursos de software para garantizar la autenticidad, integridad y si es necesario la veracidad de la información concerniente al momento (tiempo) en que se hizo la medición.	AD + VFTSw	/	
5.2.3.3	Para un nivel de protección más alto es necesario aplicar métodos criptográficos.	/	AD + VFTSw + SMT	
5.2.3.4	Almacenamiento automático	AD + VFTSw	AD + VFTSw + SMT	
5.2.3.5	Retardo de la transmisión	AD + VFTSw	AD + VFTSw + SMT	Seleccione “B” en caso de riesgo alto de fraude por ej. transmisión en sistemas abiertos
5.2.3.6	Interrupción de la transmisión	AD + VFTSw	AD + VFTSw + SMT	Seleccione “B” en caso de riesgo alto de fraude por ej. transmisión en sistemas abiertos
5.2.3.7	Sello de tiempo	AD + VFTSw	AD + VFTSw + SMT	
5.2.4	Compatibilidad de los sistemas operativos y el hardware, portabilidad	AD + VFTSw	AD + VFTSw + SMT	
Mantenimiento y reconfiguración				
5.2.6.2	Actualización verificada	AD	AD	
5.2.6.3	Actualización trazable	AD + VFTSw	AD + VFTSw + CIWT/SMT	Seleccione “B” en caso de riesgo alto de fraude

Tabla 2: Recomendaciones para combinaciones de análisis y métodos de prueba para los diversos requerimientos de software (acrónimos definidos en Tabla 1)

6.5 Instrumento bajo ensayo (IBE)

Normalmente los ensayos se realizan en el instrumento de medición completo (pruebas funcionales). Si el tamaño o la configuración del instrumento de medición, no le permiten ser ensayado como una unidad completa o si los ensayos solo le conciernen a un dispositivo separado (módulo) del instrumento de medición, la Recomendación relevante de OIML puede indicar que las pruebas o ciertas pruebas, se realicen a los dispositivos electrónicos o módulos de software de manera separada, siempre que en el caso de ensayos con dispositivos en operación, estos dispositivos estén incluidos en una configuración simulada, que sea suficientemente representativa de su operación normal. El solicitante de la aprobación es responsable de la provisión de todo el equipamiento y componentes requeridos.

7 Verificación

Si en un país se prescribe el control metrológico de los instrumentos de medición, deberá haber medios para verificar en campo durante la operación: la identidad del software, la validez del ajuste y la conformidad con el modelo aprobado.

La recomendación relevante OIML puede requerir realizar la verificación del software en una o más etapas, según sea la naturaleza del instrumento de medición considerado.

La verificación del software incluirá:

- una inspección de la conformidad del software con la versión aprobada (por ejemplo: verificación del número de versión y checksum);
- una inspección de que la configuración es compatible con la configuración mínima declarada, si figura en el certificado de aprobación;
- una inspección de que las entradas/salidas del instrumento de medición están bien configuradas en el software, cuando su asignación respectiva es un parámetro específico de dispositivo;
- una inspección de que los parámetros específicos de dispositivo (especialmente los parámetros de ajuste) son correctos.

Los procedimientos para actualización del software están descriptos en 5.2.6.2 y 5.2.6.3.

8 Evaluación de los niveles de severidad (riesgos)

8.1 Esta sección pretende ser una guía para determinar un conjunto de niveles de severidad, para ser aplicados generalmente en los ensayos realizados a los instrumentos de medición electrónicos. No pretende ser una clasificación con límites estrictos, que llevaría a requerimientos especiales como en el caso de una clasificación de precisión.

Además, esta guía no restringe a los Comités Técnicos y Subcomités de proveer niveles de severidad, que difieran de aquellos que resulten de las pautas establecidas en este Documento. Se pueden usar diferentes niveles de severidad de acuerdo con límites especiales prescriptos en la Recomendación relevante de OIML.

8.2 El nivel de severidad de un requerimiento debe seleccionarse independientemente de un requerimiento a otro.

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

(a) riesgo de fraude:

- la consecuencia y el impacto social del malfuncionamiento;
- el valor de los bienes a medir;
- la plataforma utilizada (construida especialmente o computadora universal);
- exposición a fuentes de fraude potencial (dispositivo de autoservicio desantendido).

(b) conformidad requerida:

- Las posibilidades prácticas para la industria de cumplir con el nivel prescripto.

(c) confiabilidad requerida:

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

(d) interés del defraudador:

- simplemente ser capaz de cometer fraude, puede ser un factor motivacional suficiente.

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

En la sección de requerimientos (ver 5), se dan diferentes ejemplos de soluciones técnicas aceptables, que ilustran el nivel básico de protección contra el fraude, conformidad, confiabilidad, y tipo de medición (marcado con (I)). Donde es apropiado, también se presentan ejemplos con medidas mejoradas, que consideran un nivel de severidad aumentada de los aspectos descriptos más arriba (indicado con (II)).

El procedimiento de validación y el nivel de severidad (riesgo) están inseparablemente unidos. Cuando se requiera un nivel de seguridad mayor, se realizará un análisis más profundo del software, con el objeto de detectar deficiencias del software o debilidades en la seguridad. Por otra parte, se deberá considerar el sellado mecánico (por ejemplo: sellado del puerto de comunicación o del gabinete) cuando se elija el procedimiento de validación.

Anexo A
Bibliografía

Al momento de la publicación, eran válidas las ediciones indicadas. Todos los documentos normativos están sujetos a revisión y los usuarios de este Documento son animados a investigar la posibilidad, de aplicar las ediciones más recientes de los documentos normativos indicados abajo. Los miembros de IEC e ISO, mantienen registros de los Estándares Internacionales de validez actual.

El estado actual de los Estándares referidos, también puede encontrarse en Internet:

Publicaciones IEC:	http://www.iec.ch/searchpub/cur_fut.htm
Publicaciones ISO:	http://www.iso.org/iso/iso_catalogue.htm
Publicaciones OIML:	http://www.oiml.org/publications/ (con descarga gratuita de archivos PDF).

Para evitar equívocos, es altamente recomendable, que todas las referencias a Estándares en las Recomendaciones OIML y en los Documentos Internacionales estén acompañadas de la versión a la que se hace referencia (generalmente el año o la fecha).

Ref.	Estándares y documentos de referencia	Descripción
[1]	International Vocabulary of Basic and General Terms in Metrology (VIM) (1993) [6)]	Vocabulario, preparado por un grupo de trabajo conjunto integrado por expertos designados por BIPM, IEC, IFCC, ISO, IUPAC, IUPAP, y OIML.
[2]	OIML B 3:2003 The OIML Certificate System for Measuring Instruments	El Sistema de Certificación OIML para Instrumentos de Medición es un sistema para emitir, registrar y utilizar Certificados de Conformidad OIML para modelos de instrumentos de medición basados en los requisitos de las Recomendaciones OIML.
[3]	OIML D 11:2004 General requirements for electronic measuring instruments	Guía para establecer requisitos de ensayo de desempeño metrológico apropiado para magnitudes de influencia, que pueden afectar a los instrumentos de medición considerados en las Recomendaciones Internacionales.
[4]	ISO/IEC 9594-8:2001 Information technology -- Open Systems Interconnection -- The Directory: Public-key and attribute certificate frameworks	ISO/IEC 9594-8:2005 especifica tres marcos y una cantidad de objetos de datos que se pueden usar para autenticar y asegurar la comunicación entre dos entidades, por ej: entre dos entidades de servicio de directorio o entre un navegador web y un servidor web. Los objetos de datos también se pueden utilizar para probar el origen y la integridad de las estructuras de datos, tales como documentos firmados digitalmente.
[5]	ISO 2382-9:1995 Information technology -- Vocabulary -- Part 9: Data communication	Destinado a facilitar la comunicación internacional en la comunicación de datos. Presenta términos y definiciones de conceptos seleccionados, relevantes para el campo de la comunicación de datos e identifica las relaciones entre las entradas.
[6]	IEC 61508-4:1998-12	Contiene las definiciones y explicaciones de los términos

[6)] El VIM fue revisado por el JCGM en 2007.
(JCGM: Comité Conjunto de Guías en Metrología)

Ref.	Estándares y documentos de referencia	Descripción
	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations	que se utilizan en las partes 1 a 7 de este Estándar. Destinado para uso de Comités Técnicos en la elaboración de Estándares de acuerdo con los principios contenidos en IEC Guía 104 e ISO/IEC Guía 51. IEC 61508 también está concebido, para ser un estándar independiente.
[7]	ISO/IEC 14598 series Information technology -- Software product evaluation	Las series de Estándares ISO/IEC 14598 proporciona métodos para la medición, análisis y evaluación, de la calidad del producto del software. No describen ni métodos para evaluar los procesos de producción de software, ni métodos para la predicción de costos (por supuesto, las mediciones de la calidad del producto del software, se pueden usar para ambos propósitos).
[8]	V 1:2000 International vocabulary of terms in legal metrology (VIML)	El VIML incluye solo los conceptos usados en el campo de la metrología legal. Estos conceptos se refieren a las actividades del servicio de metrología legal, a los documentos relevantes, así como a otros problemas relacionados con esta actividad. También se incluyen en este Vocabulario ciertos conceptos de carácter general, que se han extraído 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	Proporciona información sobre los conceptos subyacentes de riesgo y la relación del riesgo con la integridad de la seguridad (ver Anexo A). Se trata una serie de métodos que permitirán determinar: los niveles de integridad de la seguridad para los sistemas relacionados con la seguridad de los E/E/PE, otros sistemas relacionados con la seguridad tecnológica y las funcionalidades para la reducción de riesgo externo (ver Anexos, B, C, D y E). Diseñado para uso de los Comités Técnicos en la preparación de Estándares de acuerdo con los principios contenidos en IEC Guide 104 y ISO/IEC Guide 51.
[10]	FDA, Guidance for FDA Reviewers and Industry Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, 29 May 1998	Este documento - guía, tiene como objetivo proporcionar información a la industria, sobre la documentación que la FDA recomienda incluir en las presentaciones previas a la comercialización de dispositivos de software, incluyendo las aplicaciones de software autónomo y los dispositivos basados en hardware que incorporan software.
[11]	FDA Guidance for Industry Part 11, August 2003	Este documento brinda orientación a las personas que han optado por mantener registros o enviar electrónicamente determinada información. En consecuencia, la Parte 11 se aplica a los registros en formato electrónico que se crean, modifican, mantienen, archivan, recuperan o transmiten según los requerimientos de registros, establecidos en las regulaciones de la Agencia de EE.UU.
[12]	WELMEC Guide 2.3, May 2005 Issue 3 Guide for Examining Software (Weighing Instruments)	

Ref.	Estándares y documentos de referencia	Descripción
[13]	WELMEC Guide 7.2, May 2008 Issue 3 Software Guide (Measuring Instruments Directive 2004/22/EC)	Este documento brinda orientación a todos aquellos interesados en la aplicación de la Directiva de Instrumentos de Medición (Directiva europea 2004/22/EC; MID), especialmente para instrumentos de medición equipados con software. Está dirigido tanto a los fabricantes de instrumentos de medición como a los organismos notificados que son responsables de la evaluación de la conformidad de los instrumentos referidos en MID. Siguiendo la Guía, se puede asumir el cumplimiento de los requisitos relacionados con el software contenidos en la MID (Directiva de Instrumentos de Medición).

Anexo B
Ejemplo de un reporte de evaluación de software
(Informativo)

Nota: Los Comités Técnicos y los Subcomités que desarrollan las Recomendaciones OIML, deben decidir qué información se incluirá en los Reportes de Ensayo y en los Certificados de Conformidad OIML. Por ejemplo: el nombre, la versión y el checksum del archivo ejecutable del siguiente ejemplo, deben incluirse en el Certificado de Ensayo.

Reporte de Ensayo no XYZ122344

Validación del Software del medidor de flujo Tournesol Metering **modelo** TT100

El software del instrumento de medición se validó, para mostrar la conformidad con los requerimientos de la Recomendación OIML R-xyz.

La validación se basó en el reporte del Documento Internacional de OIML D 31:2008, en la que se interpretan y explican los requerimientos esenciales del software. Este reporte describe el examen del software, necesario para declarar la conformidad con la R-xyz.

Fabricante Tournesol Metering P.O.
Box 1120333
100 Klow
Syldavie
Referencia: Mr. Tryphon Tournesol

Solicitante
New Company
Nova Street 123
1000 Las Dopicos
San Theodorod
Referencia: Archibald Haddock

Objeto del Ensayo

El medidor Tournesol Metering TT100 es un instrumento de medición destinado a medir el flujo en líquidos. El rango previsto va de 1 L/s hasta 2000 L/s. Las funciones básicas del instrumento son:

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

El medidor de flujo se describe como un instrumento de medición construido a medida (un sistema embebido) con dispositivo de almacenamiento que contiene lo datos legalmente relevantes.

El medidor de flujo TT100 es un instrumento independiente con un transductor conectado. El transductor incorpora una compensación de temperatura. El ajuste del caudal es posible gracias a parámetros de calibración, almacenados en una memoria no volátil del transductor. Está fija al instrumento y no puede desconectarse. El volumen medido se indica en una pantalla. No es posible la comunicación con otros dispositivos.

El software embebido del instrumento de medición fue desarrollado por

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

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

La versión validada del software es **V1.2c**. La versión del software se presenta en la pantalla al encender el dispositivo y al presionar la tecla "nivel" durante 4 segundos.

El código fuente comprende los siguientes archivos legalmente relevantes:

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

El archivo ejecutable **"tt100_12.exe"** está protegido de modificaciones por medio de un checksum. El valor del checksum por el algoritmo **XYZ** es **1A2B3C**.

La validación fue respaldada por los siguientes documentos del fabricante:

- TT 100, Manual de Usuario Versión 1.6;
- TT 100 Manual de Mantenimiento Versión 1.1;
- Descripción del Software TT100 (documento de diseño interno, fechado 22 Nov 2003);
- Diagrama del circuito electrónico TT100 (plano nro. 222-31, fechado 15 Oct 2003).

La versión final del objeto de ensayo se envió al Laboratorio Nacional de Ensayo y Medición, el 25 de noviembre de 2003.

Desempeño de la validación

La validación se llevó a cabo de acuerdo con el Documento de la OIML D 31:2008. La validación fue realizada entre el 1ro de noviembre y el 23 de diciembre de 2003. Se efectuó una revisión del diseño el 3 de diciembre, por parte del Dr. K. Fehler, en la sede central de Tournesol Metering en Klow. Se realizó otro trabajo de validación en el Laboratorio Nacional de Ensayo y Medición por parte del Dr. K. Fehler y del Sr. S. Problème.

Se validaron los siguientes requerimientos:

- identificación del software;
- corrección de los algoritmos y de las funciones;
- protección del software;
- prevención contra mal uso accidental;
- protección contra fraude;
- soporte de las características del hardware;
- almacenamiento de datos, transmisión por medio de 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;
- guía (tutorial), inspección de código;
- ensayo de módulo de software, del módulo calculate.c con SDK XXX.

Resultado

Se validaron los siguientes requerimientos de OIML D 31:2008 sin que se encontraran fallas:

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 estaban descriptos inicialmente en el manual del operador. Se incluyeron los dos comandos en el manual del operador fechado el 10 de diciembre de 2003.

Se encontró una falla de software, en el paquete de software V1.2b, que limitaba el mes de febrero a 28 días, incluso en un año bisiesto. La falla se corrigió en V1.2c.

El resultado aplica solamente, al item ensayado con el Nro. de serie 1188093-B-2004.

Conclusión

The software del **Tournesol Metering TT100 V1.2c** cumple con los requerimientos de la OIML R-xyz.

Laboratorio Nacional de Ensayo y Medición
Departamento de Software
Dr. K.E.I.N. Fehler Sr. S.A.N.S. Problème
Gerente Técnico Oficial Técnico

Lista de verificación

Cláusula	Requerimiento	Aprobado	Falló	Observaciones
5.1 **5.1.1**	**Requerimientos generales** **Identificación del Software** El software legalmente relevante debe ser claramente identificado.			
5.1.2	**Corrección de los algoritmos y de las funciones** Los algoritmos de medición y las funciones de un dispositivo de medición deben ser correctos.			
5.1.3 **5.1.3.1**	**Protección del software** **Prevención de mal uso** Un instrumento de medición- especialmente el software-deberá construirse de tal manera que las posibilidades de un mal uso accidental (no intencional), sean mínimas.			
5.1.3.2 **a)** **b)** **c)** **d)**	**Protección contra fraude** El software legalmente relevante deberá asegurarse contra: modificaciones no autorizadas, descarga o cambios por remplazo del dispositivo de memoria. Adicionalmente a los sellos mecánicos, pueden ser necesarios medios técnicos, para asegurar los instrumentos de medición que tengan un sistema operativo o una opción para cargar software. Solo funciones claramente documentadas (ver 6.1), pueden ser activadas por la inferfaz de usuario. La interfaz de usuario debe ser tal, que no facilite el uso fraudulento. La presentación de la información debe cumplir con 5.2.2. Los parámetros que fijan las características legalmente relevantes del instrumento de medición, deberán ser protegidos contra modificación no autorizada. Si es necesario para los fines de la verificación, la configuración actual de los parámetros debe poder mostrarse en pantalla o imprimirse. La protección del software comprende el sellado apropiado usando medios mecánicos, electrónicos y/o criptográficos, que hagan que una intervención no autorizada sea imposible o evidente.			
5.1.4 **5.1.4.1**	**Soporte de las características del hardware** **Soporte de detección de fallas** Se le podrá solicitar al fabricante del instrumento, el diseño de unidades funcionales de verificación en las partes del software o del hardware o que provea medios mediante los cuales las partes del hardware puedan ser soportadas por las partes del software del instrumento.			
5.1.4.2	**Soporte de protección de durabilidad** Es elección del fabricante diseñar herramientas de protección de durabilidad en el software o en el hardware o permitir que las herramientas del hardware sean respaldadas por software.			
5.2 **5.2.1**	**Requerimientos específicos** **Especificando y separando las partes relevantes y especificando las interfaces de las partes** Las partes metrológicamente críticas de un sistema de medición no serán influenciadas inadmisiblemente, por otras partes del sistema de medición.			
5.2.1.1 **a)** **b)**	**Separación de dispositivos y subconjuntos** Los subconjuntos o dispositivos electrónicos de un sistema de medición, que realizan funciones legalmente relevantes, deben ser identificados, claramente definidos y documentados. Durante los ensayos de aprobación de modelo, se debe demostrar que las funciones relevantes y los datos de los subconjuntos y dispositivos electrónicos no pueden ser influenciados inadmisiblemente, por comandos recibidos a través de la interfaz.			
5.2.1.2 **a)** **b)**	**Separación de partes del software** El requerimiento de conformidad aplica a la parte del software legalmente relevante de un instrumento de medición (ver 5.2.5) y debe ser identificables como se describe en 5.1.1. Si la parte legalmente relevante del software, se comunica con otras partes del software, se debe definir una interfaz de software. Toda comunicación se debe realizar exclusivamente utilizando esta interfaz. La parte del software legalmente relevante y la interfaz deben ser claramente documentadas. Todas las funciones legalmente relevantes y dominios de datos del software, deben ser descriptos para permitir a la autoridad de aprobación de modelo, decidir si la separación del software es correcta.			

Cláusula	Requerimiento	Aprobado	Falló	Observaciones
c) **d)**	Debe haber una asignación no ambigua de cada comando, para todas las funciones invocadas o para los cambios de datos, en la parte del software legalmente relevante. Los comandos que se envían a través de la interfaz de software, deben ser declarados y documentados. Solo se pueden activar a través de la interfaz del software, los comandos que hayan sido documentados. El fabricante debe declarar la totalidad de la documentación de comandos En los casos en que el software legalmente relevante haya sido separado del software no relevante, el software legalmente relevante debe tener prioridad en el uso de recursos sobre el software no relevante.			
5.2.2	**Indicaciones compartidas** Si la indicación se realiza utilizando una interfaz de usuario de ventanas múltiples, aplican los siguientes requerimientos: -el software que ejecuta la indicación de los valores de medición y otra información legalmente relevante, pertenece a la parte legalmente relevante. La ventana que contiene estos datos debe tener la más alta prioridad.			
5.2.3 **5.2.3.1**	**Almacenamiento de datos, transmisión por medio de sistemas de comunicación** El valor de medición almacenado o transmitido debe estar acompañado por toda la información relevante necesaria para uso futuro legalmente relevante.			
5.2.3.2	Los datos estarán protegidos por recursos de software para garantizar la autenticidad, integridad y si es necesario la veracidad de la información concerniente al momento (tiempo) en que se hizo la medición. El software que muestra en pantalla o que además procesa los valores de medición y los datos que los acompañan, deberá verificar el momento en que se realizó la medición, la autenticidad y la integridad de los datos, luego de haberlos leído del lugar de almacenamiento no seguro o después de haberlos recibido de una canal de transmisión no seguro. Si se detecta una irregularidad, se deben descartar los datos o se los debe marcar como datos no utilizables.			
5.2.3.3	Para un nivel de protección más alto es necesario aplicar métodos criptográficos.			
5.2.3.4 **a)** **b)** **c)**	**Almacenamiento automático** Los datos de medición deben ser almacenados automáticamente cuando se concluye la medición. El dispositivo de almacenamiento debe tener la suficiente inalterabilidad, para asegurar que los datos no se corrompan en condiciones normales de almacenamiento. Debe haber suficiente memoria de almacenamiento para cualquier aplicación particular. Cuando el valor final utilizado con propósitos legales es el resultado de un cálculo, todos los datos que son necesarios para el cálculo deben ser almacenados automáticamente con el valor final. Los datos almacenados pueden borrarse si: • la transacción ya ha sido liquidada; o bien • estos datos son imprimidos por un dispositivo impresor sujeto a control legal. Luego que se hayan cumplido los requerimientos de la sección 5.2.3.4.b y cuando la memoria está llena, se permite el borrado de los datos memorizados cuando se cumplen las dos condiciones que siguen: • los datos se borran en el mismo orden en que fueron grabados y se respetan las reglas establecidas para la aplicación en cuestión; • el borrado se realiza o automáticamente o al realizar una operación manual especial.			
5.2.3.5	**Retardo de la transmisión** La medición no debe ser inadmisiblemente influenciada por un retardo de la transmisión.			
5.2.3.6	**Interrupción de la transmisión** Si los servicios de la red no están disponibles, no se deben perder datos de medición. El proceso de medición se podría detener para evitar la pérdida de datos de medición.			
5.2.3.7	**Sello de tiempo** El sello de tiempo debe leerse del reloj del dispositivo. Se deben tomar medidas de protección apropiadas de acuerdo con el nivel de severidad que se va a aplicar (ver 5.1.3.2.c). Si la información concerniente a los datos de tiempo (momento) en que se realiza la medición es necesaria, se debe aumentar la confiabilidad del reloj interno del instrumento de medición utilizando medios específicos.			

Cláusula	Requerimiento	Aprobado	Falló	Observaciones
5.2.4 **5.2.4.1**	**Compatibilidad de los sistemas operativos y el hardware, portabilidad** El fabricante definirá el entorno adecuado de software y de hardware. Los recursos mínimos y una configuración adecuada necesaria para un correcto funcionamiento, deben ser declarados por el fabricante.			
5.2.4.2	Se deben proveer recursos técnicos para evitar la operación, cuando no se alcanzan los requerimientos mínimos de configuración.			
5.2.6 **5.2.6.1**	**Mantenimiento y reconfiguración** Solo se permite el uso de versiones del software legalmente relevante, que sean conformes al modelo aprobado.			
5.2.6.2	**Actualización verificada** Luego de la actualización del software legalmente relevante de un instrumento de medición (intercambio con otra versión aprobada o reinstalación) el instrumento de medición no puede ser empleado para propósitos legales antes de que se le realice una verificación y se hayan renovado los medios de protección.			
5.2.6.3 **a)** **b)** **c)** **d)** **e)** **f)** **g)**	**Actualización trazable** La Actualización Trazable del software debe ser automática. Al completar el procedimiento de actualización, el entorno de protección del software debe estar al mismo nivel que el requerido por la aprobación de modelo. El instrumento de medición de objetivo debe tener un software legalmente relevante fijo. Se deben emplear medios técnicos para garantizar la autenticidad del software cargado. Si el software cargado falla en la verificación de autenticidad, el instrumento debe descartarlo y utilizar la versión previa del software o cambiar su modo de operación a no utilizable. Se deben utilizar medios técnicos para asegurar la integridad del software a cargar, es decir que antes de ser cargado, no ha sido inadmisiblemente cambiado. Se deben utilizar medios técnicos apropiados, para asegurar que las Actualizaciones Trazables sean adecuadamente trazables en el instrumento. El instrumento de medición deberá tener un subconjunto/dispositivo electrónico para que el usuario o propietario exprese su consentimiento. Debe ser posible habilitar y deshabilitar este subconjunto/dispositivo electrónico, por ejemplo: por medio de un interruptor que pueda ser sellado o por medio de un parámetro. Si el subconjunto/dispositivo electrónico está habilitado, cada descarga debe ser iniciada por el usuario o el propietario. Si está deshabilitado el usuario o el propietario no necesitan realizar ninguna acción para llevar a cabo la descarga. Si no se pueden cumplir los requerimientos de 5.2.6.3.a á 5.2.6.3.f, igual es posible actualizar la parte del software no legalmente relevante. En este caso se deben cumplir los siguientes requerimientos: • hay una separación inconfundible entre el software legalmente relevante y el no legalmente relevante de acuerdo con 5.2.1; • la parte legalmente relevante del software (en su totalidad) no puede ser actualizada sin romper un sello; • está establecido en el certificado de aprobación de modelo, que es aceptable la actualización de las partes no legalmente relevantes.			
5.2.6.4	El instrumento de medición debe poseer una función, que registre de forma automática e imborrable, cualquier ajuste del parámetro específico del dispositivo, por ejemplo: un registro de auditoría. El instrumento debe ser capaz de mostrar los datos registrados.			
5.2.6.5	Los medios de trazabilidad y los registros son parte del software legalmente relevante y deben ser protegidos como tales.			

Anexo C
Índice