WELMEC

Cooperación europea en metrología legal

Guía del software

(Directiva 2004/22/EC relativa a Instrumentos de Medida)

Mayo 2009

WELMEC

Cooperación europea en metrología legal

WELMEC es una cooperación entre las autoridades de metrología legal de los Estados miembros de la Unión Europea y la Asociación Europea de Libre Comercio. Este documento es una de las distintas guías publicadas por WELMEC para orientar a los fabricantes de instrumentos de medida y a los organismos notificados responsables de la evaluación de conformidad de sus productos. Las guías son puramente orientativas y no imponen ninguna restricción o requisito técnico adicional más allá de aquellas que se incluyen en las Directivas CE pertinentes. Aunque se pueden admitir propuestas alternativas, la orientación que se proporciona en este documento representa lo expuesto por WELMEC como la mejor práctica a seguir.

Nota: todas las referencias a la Directiva 2004/22/EC relativa a los instrumentos de medida contenidas en este documento se realizarán mediante el acrónimo “MID”

Publicación CEM edición digital 1
Traducción al español de la 4ª edición del original publicado por WELMEC

NIPO: 706-09-004-7

Índice

Prefacio

Esta guía se basa en la versión 1.00 de la "*Software Requirements and Validation Guide"*, 29 de octubre de 2004, desarrollada y emitida por la Red de Crecimiento Europeo "MID software". Desde enero de 2002 hasta diciembre de 2004 la comisión de la UE respaldó dicha red mediante el contrato G7RT-CT-2001-05064.

La guía es puramente orientativa y no impone ninguna restricción o requisito técnico adicional más allá de aquellos que se incluyen en la MID. Se pueden admitir propuestas alternativas, aunque la orientación que se proporciona en este documento se presenta lo considerado por WELMEC como la mejor práctica a seguir.

Aunque la guía está orientada a los instrumentos incluidos en las regulaciones de la MID, los resultados son de carácter general y pueden aplicarse en otros ámbitos.

Esta última edición aprovecha la experiencia adquirida en la aplicación de esta guía.

1. Introducción

Este documento proporciona una orientación a todos aquellos relacionados con la aplicación de la MID, especialmente para los instrumentos de medida equipados con software.
Va dirigido tanto a los fabricantes de instrumentos de medida como a los organismos notificados responsables de la evaluación de la conformidad de los mismos.

Aplicando esta guía puede asumirse la conformidad con los requisitos de la MID relativos al software.

Además, puede asumirse también que todos los organismos notificados aceptan la presente guía como una interpretación fiel de la MID respecto al software.

Para demostrar cómo se relacionan los requisitos de la presente guía con los requisitos respectivos en la MID, se ha incluido una referencia cruzada en la presente guía como anexo (capítulo 13).

La guía anterior era la guía 7.1, elaborada por el grupo de trabajo 7 de WELMEC. Ambas guías se basan en los mismos principios y derivan de los requisitos de la MID. Se ha revisado la guía 7.1 y sigue existiendo (edición 2) pero ahora es de carácter meramente informativo, mientras que la guía 7.2 es la única que recomienda WELMEC para la creación, examen y validación del software de los instrumentos de medida controlados por software sometidos a la MID.

En la página Web: http://www.welmecwg7.ptb.de se encuentra disponible información actualizada sobre las guías y la actividad del grupo de trabajo 7 de WELMEC.

2. Términos y definiciones

Los términos y definiciones contenidos en este apartado describen el vocabulario tal y como se usa en esta guía. Cuando una definición se ha tomado total o parcialmente de una norma u otra fuente se proporcionan referencias a la misma.

Almacenamiento a largo plazo de los datos de medida: almacenamiento utilizado para conservar los datos de medida disponibles una vez finalizada la misma para fines posteriores legalmente relevantes (p. ej., la conclusión de una transacción comercial).

Almacenamiento integrado: almacenamiento no extraíble que forma parte del instrumento de medida (p. ej., RAM, EEPROM, disco duro).

Autenticación: verificación de la identidad declarada o alegada de un usuario, proceso, o dispositivo.

Clases de riesgo: clases que engloban tipos de instrumentos de medida con evaluaciones de riesgo comparables.

Configuración básica: diseño de un *instrumento de medida* respecto a su arquitectura básica. Existen dos configuraciones básicas diferentes: instrumentos de medida desarrollados específicamente e instrumentos de medida que usan un ordenador universal. Estos términos son aplicables del mismo modo a los subconjuntos.

Configuración TI (Tecnologías de la Información): diseño de un instrumento de medida respecto de las funciones TI y elementos característicos que son —de acuerdo a los requisitos— independientes de la función de medición. En esta guía se consideran cuatro configuraciones TI: almacenamiento a largo plazo de los datos de medida, transmisión de los datos de medida, descarga de software y separación de software (consulte también «configuración básica»). Estos términos son aplicables del mismo modo a los subconjuntos.

Descarga de software: proceso de transferencia automática del software a un instrumento de medida o unidad de hardware de destino mediante cualquier medio técnico, desde una fuente local o remota (p.

ej., medios de almacenamiento intercambiables, ordenador portátil, ordenador remoto), a través de conexiones arbitrarias (p. ej., enlace directo, redes).

Identificación del software: secuencia de caracteres legibles ligada indefectiblemente al software (p. ej., número de versión, suma de comprobación –*checksum*-).

Instrumento de medida: cualquier dispositivo o sistema con funciones de medición. El calificativo "de medida" se omite siempre que de lugar a confusión [Artículo 4, MID].

Instrumento de medida desarrollado específicamente (tipo P): instrumento de medida diseñado y construido específicamente para una tarea concreta. Por consiguiente, toda la aplicación software se desarrolla para realizar la medida. Para una definición más detallada, véase el apartado 4.1.

Instrumento de medida que utilizan un ordenador universal (tipo U): instrumento de medida que consta de un ordenador de propósito general, que suele ser un sistema basado en PC, para realizar funciones legalmente relevantes. Se asume que un sistema de medida es de tipo U si no se cumplen las condiciones de un instrumento de medida desarrollado específicamente (tipo P).

Integridad de los datos y del software: garantía de que los datos y el software no han sufrido cambios no autorizados durante su uso, transferencia o almacenamiento.

Interfaz de comunicación: interfaz electrónica, óptica, de radiofrecuencia o por cualquier otro sistema que permite que la información pase automáticamente entre los componentes de los instrumentos de medida, subconjuntos o dispositivos externos.

Interfaz de usuario: interfaz que constituye la parte del instrumento o sistema de medida que permite transmitir información entre un usuario humano y el instrumento de medida o sus componentes de hardware o software, como por ejemplo un interruptor, un teclado, un ratón, una pantalla, un monitor, una impresora o una pantalla táctil.

Parámetro específico del dispositivo: parámetro legalmente relevante con un valor que depende de cada instrumento. Los parámetros específicos del dispositivo están compuestos por los parámetros de calibración (p. ej., ajuste del intervalo u otros ajustes o correcciones) y los parámetros de configuración (p. ej., valor máximo, valor mínimo, unidades de medida, etc.). Solamente se pueden ajustar o seleccionar en un modo operativo especial del instrumento. Los parámetros específicos del dispositivo pueden clasificarse como aquellos que deberían estar protegidos (inalterables) y aquellos a los que puede acceder una persona autorizada, p. ej., el propietario del instrumento o el proveedor del producto (parámetros configurables).

Parámetro específico del modelo: parámetro legalmente relevante cuyo valor depende únicamente del modelo de instrumento. Los parámetros específicos del modelo forman parte del software legalmente relevante. Se fijan en el examen de modelo del instrumento.

Parámetro legalmente relevante: parámetro de un instrumento de medida o un subconjunto sometido a control legal. Se pueden distinguir los siguientes tipos de parámetros legalmente relevantes: parámetros específicos del modelo y parámetros específicos del dispositivo.

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

Red cerrada: red de un número fijo de participantes con una identidad, funcionalidad y ubicación conocidas (véase también «red abierta»).

Registro de actividades: contador software (p. ej., *contador de sucesos*) y/o un registro de información (p. ej., *registro de sucesos*) de los cambios realizados en los parámetros o el software legalmente relevantes.

Separación del software: separación inequívoca del software entre el legalmente relevante y el legalmente no relevante. Si no hay separación de software, todo el software en conjunto se considera legalmente relevante.

Software legalmente relevante: programas, datos y parámetros específicos del modelo pertenecientes a un instrumento de medida o subconjunto, que definen o satisfacen funciones que están sujetas a control legal.

Software fijo: parte del software definido como fijo en el examen de modelo, es decir *modificable únicamente con la aprobación del organismo notificado*. Esta parte fija es idéntica en cada instrumento individual.

Solución aceptable: diseño o base de un módulo de software o de una unidad de hardware, o de un elemento que se considera que cumple un requisito determinado. Una solución aceptable constituye un ejemplo de cómo se puede cumplir un requisito específico, sin prejuicio de otras soluciones que también satisfagan ese requisito.

Subconjunto: dispositivo hardware (unidad de hardware) que funciona independientemente y que junto con otros subconjuntos (o instrumentos de medida), con los cuales es compatible, constituyen un instrumento de medida [Artículo 4, MID].

TEC: type examination certificate (Certificado de examen de modelo).

Transmisión de datos de medida: transmisión de datos de medida a través de redes de comunicación u otros medios a un dispositivo remoto donde se procesan o utilizan posteriormente con fines legalmente regulados.

Validación: confirmación del cumplimiento de los requisitos particulares para el uso previsto mediante el examen y la aportación de evidencias objetivas (p. ej., información que puede demostrarse verdadera basada en datos obtenidos de observaciones, mediciones, *ensayos*, etc.). En el presente caso dichos requisitos son los de la MID.

Las siguientes definiciones son bastante específicas. Se usan tan solo en algunos casos y para las clases de riesgo D o superiores.

Algoritmo *hash*: algoritmo que comprime el contenido de un bloque de datos en un número de longitud determinada (código *hash*), de modo que el cambio de cualquier bit del bloque de datos conlleve, en la práctica, a otro código *hash*. Los algoritmos *hash* se seleccionan de tal manera que la probabilidad teórica de que dos bloques de datos diferentes tengan el mismo código *hash* sea muy baja.

Algoritmo de firma: algoritmo criptográfico que cifra (codifica) texto normal en texto cifrado (texto codificado o secreto) mediante una clave de firma y que permite descodificar el texto cifrado si se dispone de la correspondiente clave de descifrado.

Autoridad certificadora: asociación que genera, guarda y emite información sobre la autenticidad de las claves públicas de personas u otras entidades (p. ej., instrumentos de medida) de manera confiable.

Certificación de claves: proceso por el que se asocia un valor de clave pública con un individuo, organización u otra entidad.

Clave de firma: cualquier número o secuencia de caracteres utilizada para codificar y descodificar información. Hay dos clases diferentes de claves de firma: sistemas de clave simétrica y sistemas de clave asimétrica. La clave simétrica indica que el emisor y el receptor de la información utilizan la misma clave. El sistema de claves se denomina asimétrico si las claves del emisor y del receptor son diferentes, pero compatibles. Por lo general, la clave del emisor la conoce el emisor y la clave del receptor es pública en un entorno definido.

Infraestructura PKI: organización que garantiza la confiabilidad del sistema de claves públicas. Incluye la concesión y distribución de certificados digitales a todos los miembros que forman parte del intercambio de información.

Firma electrónica: código abreviado (firma) que se asigna unívocamente a un texto, bloque de datos o archivo de software binario para demostrar la integridad y autenticidad de los datos almacenados o transmitidos. La firma se crea mediante un algoritmo de firma y una clave de firma secreta. Por lo general, la generación de una firma electrónica consta de dos pasos: (1) primero, un algoritmo *hash* comprime el contenido de la información que va a firmarse en un valor abreviado, y (2) a continuación, el algoritmo de firma combina este número con la clave secreta para generar la firma.

Sistema de clave pública – Public Key Systems (PKS): par de claves de firma diferentes, una llamada clave secreta y la otra clave pública. Para verificar la integridad y autenticidad de la información, el valor *hash* de esta información generado por un algoritmo *hash* se codifica con la clave secreta del emisor para crear la firma, descifrada más tarde por el receptor que usa la clave pública del emisor.

3. Cómo usar esta guía

Este capítulo describe la organización de la guía y explica como utilizarla.

3.1 Estructura general

La guía se organiza como una serie estructurada de bloques de requisitos. La estructura general de la guía sigue la clasificación de los instrumentos de medida en las configuraciones básicas y la clasificación de las denominadas configuraciones TI. Cada serie de requisitos se complementa con los requisitos específicos de cada instrumento.

Por lo tanto, existen tres tipos de series de requisitos:

1. requisitos para las dos configuraciones básicas de los instrumentos de medida (denominadas tipo P y U),

2. requisitos para las cuatro configuraciones TI (denominadas extensiones L, T, S y D)

3. requisitos específicos del instrumento (denominados extensiones I.1, I.2, etc.).

El primer tipo de requisitos es aplicable a todos los instrumentos. El segundo tipo de requisitos atañe a las siguientes funciones TI: almacenamiento a largo plazo de los datos de medida (L), transmisión de los datos de medida (T), descarga de software (D) y separación de software (S). Cada serie de estos requisitos solo se aplica si existe la función correspondiente. El último tipo es una colección de requisitos específicos del instrumento. La numeración se corresponde con la de los anexos específicos de los instrumentos en la MID. La serie de bloques de requisitos que puede aplicarse a un instrumento de medida determinado se muestra esquemáticamente en la figura 3-1.

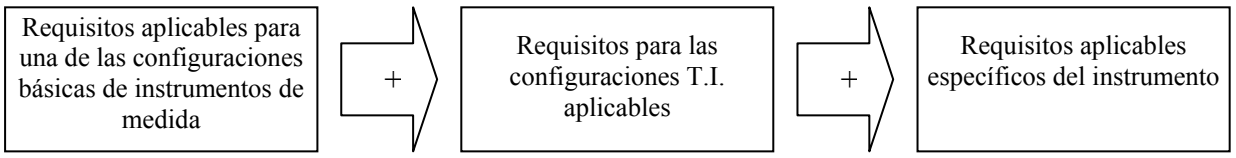

Figura 3-1: Tipo de series de requisitos que deberían aplicarse a un instrumento.

Los esquemas de la figura 3-2 muestran las series de requisitos que existen.

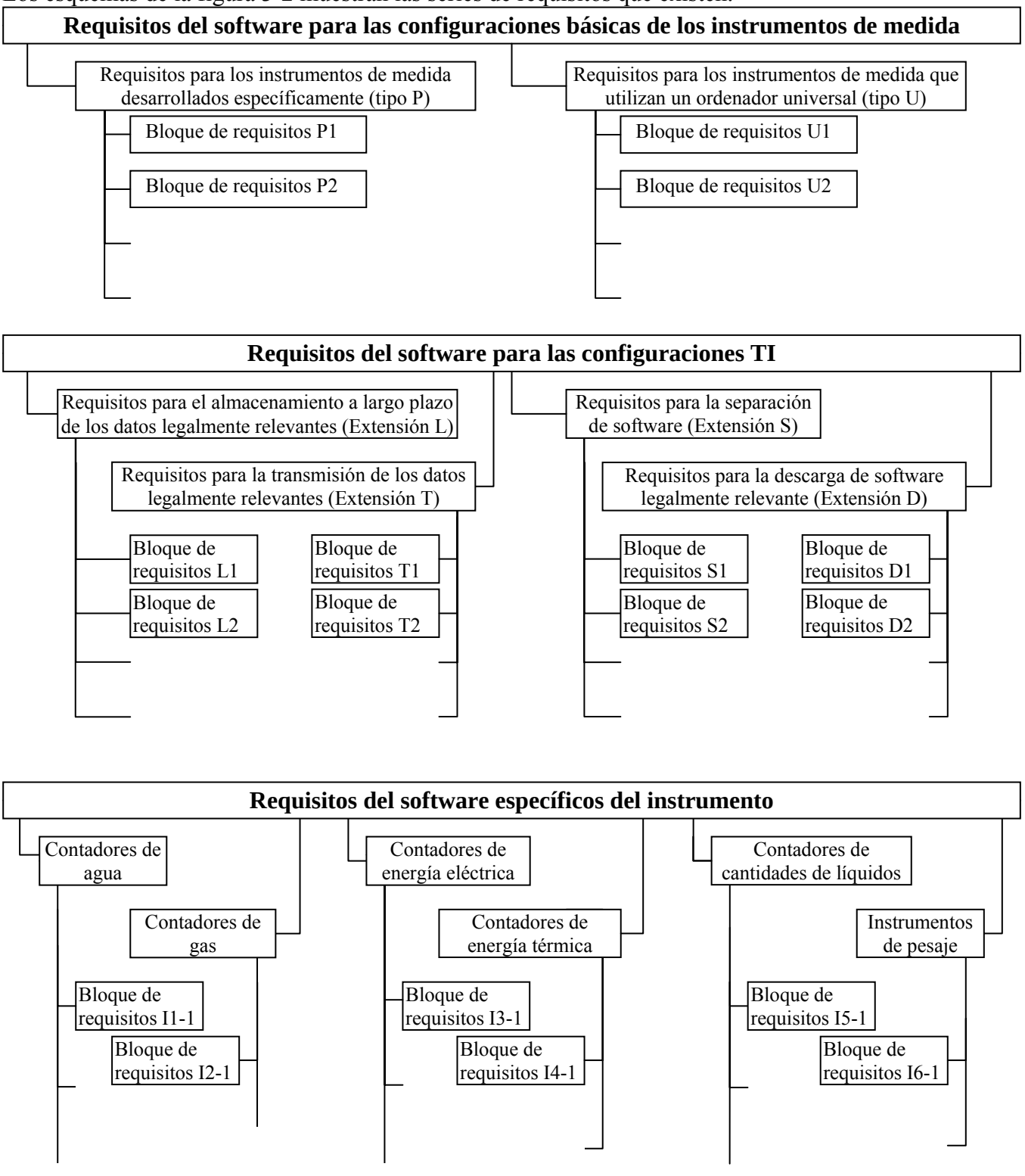

Figura 3-2: Descripción general de las series de requisitos.

Además de la estructura descrita, los requisitos de esta guía se diferencian según las clases de riesgo. Se presentan seis clases de riesgo enumeradas de la A a la F en orden creciente de nivel riesgo. La clase de menor riesgo (A) y la clase de mayor riesgo (F) no se utilizan en la actualidad. Se reservan para el caso eventual de que lleguen a ser necesarias en el futuro. Las clases restantes de riesgo que van de la B a la E abarcan todas las clases de instrumentos regulados por la MID. Proporcionan además un rango suficiente para el caso de variar las evaluaciones de riesgo. Las clases se definen en el capítulo 11 de esta guía, el cual es solo de carácter informativo.

Cada instrumento de medida debe asignarse a una clase de riesgo, ya que los requisitos particulares del software que deben aplicarse quedan determinados por la clase de riesgo a la que pertenece el instrumento.

3.2 Cómo seleccionar los apartados adecuados

Esta guía de software es de aplicación a una gran variedad de instrumentos. La guía tiene estructura modular. Las series de requisitos adecuadas pueden seleccionarse fácilmente mediante el siguiente procedimiento:

Paso 1: Selección de la configuración básica (P o U)

Solo será necesario aplicar una de las dos series de requisitos para las configuraciones básicas. Se decidirá si la configuración básica del instrumento se ajusta a: un instrumento desarrollado específicamente con software integrado (tipo P, véase el apartado 4.1) o un instrumento que utilice un ordenador universal (tipo U, véase el apartado 5.1). Si no se trata de un instrumento completo, sino de uno de sus componentes, la decisión se tomará según dicho componente. Se aplicará la serie completa de requisitos de la correspondiente configuración básica.

Paso 2: Selección de las configuraciones TI aplicables (extensiones L, T, S y D)

Las configuraciones TI comprenden: almacenamiento a largo plazo de datos legalmente relevantes (L), transmisión de datos legalmente relevantes (T), separación de software (S) y descarga de software legalmente relevante (D). Las series de requisitos correspondientes, denominadas extensiones modulares, son independientes entre sí. Las extensiones seleccionadas dependen solo de la configuración TI. Si se selecciona un conjunto de extensiones, deberá aplicarse por completo las series de requisitos de cada extensión. Se decidirá cuales de las extensiones modulares, si la hay, son aplicables y se aplicarán convenientemente (figura 3-2).

Paso 3: Selección de los requisitos específicos del instrumento (extensión I)

Se seleccionarán, según la extensión específica del instrumento I.x, los requisitos aplicables específicos del instrumento, si los hay, y se aplicarán convenientemente (figura 3-2).

Paso 4: Selección de la clase de riesgo aplicable (extensión I)

Se seleccionará la clase de riesgo definida en el subapartado I.x.6 correspondiente a la extensión I.x específica del instrumento. En este, las clases de riego pueden definirse de manera uniforme para una clase de instrumentos de medida o de forma diferenciada por categorías, campos de aplicación, etc. Una vez que se haya seleccionado la clase de riesgo aplicable, tan solo será necesario considerar los requisitos y la guía de validación respectivos.

3.3 Cómo trabajar con bloques de requisitos

Cada bloque de requisitos contiene un requisito bien definido. Consta de una definición, especificaciones aclaratorias, documentación que debe proporcionarse, guía de validación y ejemplos de soluciones aceptables (si están disponibles). El contenido de un bloque de requisitos puede

subdividirse según las clases de riesgo. En la figura 3-3 se muestra el esquema de un bloque de requisitos.

Título del requisito		
Enunciado del requisito (posible diferenciación según las clases de riesgo)		
Especificaciones (ámbito de aplicación, explicaciones adicionales, casos excepcionales, etc.)		
Documentación que debe proporcionarse (posible diferenciación según las clases de riesgo)		
Guía de validación para una clase de riesgo	**Guía de validación** para otra clase de riesgo	…
Ejemplo de solución aceptable para una clase de riesgo	**Ejemplo de solución aceptable** para otra clase de riesgo	…

Figura 3-3: Estructura de un bloque de requisitos

El bloque de requisitos representa el contenido técnico del requisito incluida la guía de validación. Se dirige tanto a los fabricantes como a los organismos notificados, en dos sentidos: (1) considerar el requisito como una condición mínima y (2) no realizar exigencias adicionales al requisito.

Notas para el fabricante:

- Debe cumplirse el enunciado y las especificaciones adicionales.
- Debe proporcionarse la documentación tal y como se requiere.
- Las soluciones aceptables son ejemplos que cumplen con el requisito. No existe la obligación de seguirlas.
- La guía de validación tiene carácter informativo.

Notas para los organismos notificados:

- Debe cumplirse el enunciado y las especificaciones adicionales.
- Debe seguirse la guía de validación.
- Debe confirmarse que la documentación proporcionada es completa.

3.4 Cómo trabajar con las listas de comprobación

Las *listas de comprobación* son un medio que permite, tanto al fabricante como al examinador, asegurase de que se han cubierto todos los requisitos de un capítulo. Forman parte del modelo del informe de ensayos. Hay que tener en cuenta que las *listas de comprobación* solo son un resumen y no distinguen entre clases de riesgo. Las *listas de comprobación* no sustituyen a las definiciones del requisito. Debe consultarse los bloques de requisitos para las descripciones completas.

Procedimiento:

- Se recopilarán las *listas de comprobación* necesarias según la selección descrita en los pasos 1, 2 y 3 del apartado 3.2.
- Se repasarán las *listas de comprobación* verificando que se han cumplido todos los requisitos.
- Se rellenarán adecuadamente las *listas de comprobación*.

4 Requisitos básicos del software integrado en un instrumento de medida desarrollado específicamente (tipo P)

La serie de requisitos de este capítulo es válida tanto para instrumentos como para componentes de instrumentos desarrollados específicamente. También es válida para los subconjuntos aunque no se mencione de forma explícita en el texto. Si el instrumento de medida utiliza un ordenador universal (PC de propósito general), deberá referirse a la serie de requisitos del siguiente capítulo (instrumento

tipo U). También se aplicarán los requisitos para instrumentos tipo U si el instrumento no se ajusta con la siguiente descripción técnica.

4.1 Descripción técnica

Un instrumento de tipo P es un instrumento de medida con un sistema TI integrado (generalmente es un sistema basado en un microprocesador o microcontrolador), con las siguientes características:

- Toda la aplicación software ha sido desarrollada para la medición. Esta aplicación incluye tanto las funciones que están sometidas a control legal como otras funciones.
- La interfaz de usuario es específica para la medición (es decir, está normalmente en un modo operativo sometido a control legal). Es posible cambiar a un modo operativo que no esté sometido a control legal.
- Si existe un sistema operativo, este no tiene un intérprete de comandos accesible al usuario (para cargar o modificar programas, enviar comandos al sistema operativo, cambiar el entorno de la aplicación,...).

El instrumento de tipo P puede tener propiedades y características adicionales que se tratan en las siguientes extensiones de requisitos:

- El software se diseña y se trata como un todo, a menos que se haya aplicado una separación de software según la extensión S.
- El software es invariable y no hay modo de programar o cambiar el software legalmente relevante. Solo se permite la descarga de software si se cumple la extensión D.
- Se permiten las interfaces de transmisión de los datos de medida a través de redes de comunicación abiertas o cerradas (debe cumplirse la extensión T).
- Se permite el almacenamiento de datos de medida, ya sea en un almacenamiento integrado, en uno remoto o en uno extraíble (debe cumplirse la extensión L).

4.2 Requisitos específicos para el tipo P

Clases de riesgo de la B a la E
P1: Documentación *Además de la documentación específica requerida en cada uno de los siguientes requisitos, la documentación incluirá básicamente*: a) *Descripción del software legalmente relevante*, b) *Descripción de la exactitud de los algoritmos de medida (p. ej., algoritmos de redondeo y cálculo de precios)*, c) *Descripción de la interfaz de usuario, los menús y los diálogos*, d) *Identificación inequívoca del software*, e) *Si no está descrita en el manual de funcionamiento, descripción general del hardware del sistema (p. ej., diagrama topológico de bloques, tipo de ordenador(es), tipo de red, etc.)*, f) *Manual de funcionamiento*.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">P2: Identificación del software:
El software legalmente relevante deberá estar claramente identificado. La identificación del software estará inequívocamente ligada al mismo. Deberá presentarse mediante un comando o durante el funcionamiento.</td></tr>
<tr><td>Especificaciones:
1. Las modificaciones del software metrológicamente relevante requieren información del organismo notificado. El organismo notificado decide si es necesaria o no una nueva identificación del software. Solo se requiere una nueva identificación del software si las modificaciones de este conducen a cambios de las funciones o características aprobadas.</td><td colspan="2">Especificaciones
1. Además de la especificación 1B: cada modificación del software legalmente relevante definido como fijo en el examen de modelo requiere una nueva identificación del software.</td></tr>
<tr><td colspan="3">2. La identificación del software será fácilmente visualizable para verificación e inspección (fácilmente significa mediante la interfaz de usuario habitual, sin herramientas adicionales).
3. La identificación del software tendrá una estructura que identifique claramente las versiones que requieran examen de modelo y las que no.
4. Si los parámetros específicos del modelo pueden modificar las funciones del software , cada función o variante puede identificarse independientemente o bien puede identificarse el paquete entero en su conjunto.</td></tr>
<tr><td colspan="2">Documentación requerida:
La documentación contendrá la identificación del software y describirá cómo se genera dicha identificación, cómo está inequívocamente ligada al propio software, cómo puede visualizarse y cómo se estructura para diferenciar entre cambios de versión que necesiten o no examen de modelo.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
La documentación mostrará las medidas tomadas para proteger la identificación del software frente a la falsificación.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se examinará la descripción de la generación y visualización de la identificación del software.
• Se comprobará si todos los programas que realizan funciones legalmente relevantes están claramente identificados y descritos de modo que quede claro tanto para el organismo notificado como para el fabricante, qué funciones de software están cubiertas por la identificación del software y cuáles no.
• Se comprobará si el fabricante proporciona un valor nominal de la identificación (número de versión o suma de comprobación funcional). Este deberá indicarse en el certificado de ensayos.
Comprobaciones funcionales:
• Se comprobará que la identificación del software puede visualizarse tal y como se describe en la documentación.
• Se comprobará que la identificación presentada es correcta.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si son adecuadas las medidas de protección tomadas frente a la falsificación.</td></tr>
</table>

Ejemplo de solución aceptable:

- La identificación del software legalmente relevante se compone de dos partes. La parte (A) debe modificarse si los cambios del software requieren un nuevo examen. La parte (B) tan solo indica cambios menores del software (p. ej., correcciones de errores) que no requieren un nuevo examen.
- La identificación se genera y visualiza a través de un comando.

• La parte (A) de la identificación consiste en un número de versión o el número del certificado de examen de modelo.	• La parte (A) de la identificación consiste en una suma de comprobación generada automáticamente sobre el software legalmente relevante que se ha declarado fijo en el examen de modelo. Para el otro software legalmente relevante, la parte (A) es un número de versión o el número del certificado de examen de modelo. • Un ejemplo de solución aceptable para generar la suma de comprobación es el algoritmo CRC-16.

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente que contiene la generación de la identificación.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará si todas las partes relevantes del software están cubiertas por el algoritmo que genera la identificación. • Se comprobará la correcta implementación del algoritmo.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">P3: Influencia sobre el software a través de la interfaz de usuario
Los comandos introducidos a través de la interfaz de usuario no influirán en el software legalmente relevante ni en los datos de medida de forma inadmisible.</td></tr>
<tr><td colspan="3">Especificaciones:
1. Los comandos pueden ser una actuación o secuencia de actuaciones a través de teclas o interruptores llevadas a cabo manualmente.
2. Esto implica que hay una asignación inequívoca de cada comando a una función o cambio de datos.
3. Esto implica que las actuaciones a través de teclas o interruptores que no estén declaradas ni documentadas como comandos no tienen ningún efecto en las funciones y datos de medida del instrumento.</td></tr>
<tr><td colspan="2">Documentación requerida:
Si el instrumento tiene la capacidad de recibir comandos, la documentación incluirá:
• Una lista completa de todos los comandos (p. ej., elementos de menú) junto con una declaración de que no existen otros comandos distintos de los relacionados.
• Una breve descripción de su significado y su efecto en las funciones y datos del instrumento de medida.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
• La documentación mostrará las medidas tomadas para validar que la documentación de los comandos es completa.
• La documentación contendrá un protocolo que muestre las pruebas de todos los comandos.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se evaluará si todos los comandos documentados son admisibles; es decir, si tienen o no un efecto permitido en las funciones de medida (y datos relevantes).
• Se comprobará si el fabricante ha suministrado una declaración explícita de que la documentación de comandos es completa.
Comprobaciones funcionales:
Se realizarán pruebas (aleatorias) tanto con los comandos documentados como con los no documentados. Se comprobarán todos los elementos de menú, si existen.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si las medidas tomadas y los protocolos de prueba son adecuados para el nivel de protección alto.</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
Existe un módulo de software que recibe e interpreta comandos de la interfaz de usuario. Este módulo pertenece al software legalmente relevante. Solo transmite comandos permitidos a los otros módulos de software legalmente relevantes. Todas las secuencias de actuaciones a través de teclas o interruptores desconocidas o no permitidas se rechazan y carecen de efecto alguno en el software o en los datos de medida legalmente relevantes.</td></tr>
</table>

<table>
<tr><th>Consideraciones adicionales para la clase de riesgo E</th></tr>
<tr><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
El código fuente del instrumento.</td></tr>
<tr><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en el código fuente:
• Se comprobará en el diseño del software si el flujo de datos relativo a los comandos del software legalmente relevante está definido de manera inequívoca y puede verificarse.
• Se buscarán flujos de datos inadmisibles desde la interfaz de usuario hasta los dominios que deban protegerse.
• Se comprobará manualmente o mediante herramientas que los comandos se descodifican correctamente y que no existen comandos no documentados.</td></tr>
</table>

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">P4: Influencia sobre el software a través de interfaces de comunicación
Los comandos introducidos a través de interfaces de comunicación del instrumento no influirán en el software legalmente relevante ni en los datos de medida de forma inadmisible.</td></tr>
<tr><td colspan="3">Especificaciones:
1. Esto implica que hay una asignación inequívoca de cada comando a una función o cambio de datos
2. Esto implica que las señales o códigos que no están declarados ni documentados como comandos no tienen ningún efecto en las funciones y datos de medida del instrumento.
3. Los comandos pueden ser una secuencia de señales eléctricas (ópticas, electromagnéticas, etc.) sobre los canales de entrada o códigos en los protocolos de transmisión de datos.
4. No son aplicables las restricciones de este requisito cuando se realiza una descarga de software según la extensión D.
5. Este requisito se aplica solo a interfaces que no estén selladas.</td></tr>
<tr><td colspan="2">Documentación requerida:
Si el instrumento dispone de una interfaz, la documentación incluirá:
• Una lista completa de todos los comandos junto con una declaración de que no existen otros comandos distintos de los relacionados.
• Una breve descripción de su significado y su efecto en las funciones y datos del instrumento de medida.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
• La documentación mostrará las medidas tomadas para validar que la documentación de los comandos es completa.
• La documentación contendrá un protocolo que muestre las pruebas de todos los comandos o cualquier otra medida adecuada para probar que son correctos.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se evaluará si todos los comandos documentados son admisibles, es decir, si tienen un efecto permitido o ningún tipo de efecto en las funciones de medida (y datos relevantes).
• Se comprobará si el fabricante ha suministrado una declaración explícita de que la documentación de comandos es completa.
Comprobaciones funcionales:
Se realizarán pruebas (aleatorias) , mediante equipos periféricos, si existen.
Nota: Si no es posible excluir efectos inadmisibles en las funciones de medición (o datos relevantes) a través de la interfaz y si el software no se puede corregir como correspondería, el certificado de ensayos deberá indicar que la interfaz no es protectora y describirá los medios necesarios de seguridad/sellado. Esto también es de aplicación a las interfaces no descritas en la documentación.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará que las medidas tomadas y los protocolos de prueba son adecuados para el nivel de protección alto.</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
Existe un módulo de software que recibe e interpreta datos de la interfaz. Este módulo pertenece al software legalmente relevante. Solo transmite comandos permitidos a los otros módulos del software legalmente relevante. Todas las secuencias de señales o código desconocidas o no permitidas se rechazan y carecen de efecto alguno en el software o en los datos de medida legalmente relevantes.</td></tr>
</table>

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del instrumento.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará en el diseño del software si el flujo de datos relativo a comandos del software legalmente relevante está definido de manera inequívoca y puede verificarse. • Se buscarán flujos de datos inadmisibles desde la interfaz usuario hasta los dominios que deban protegerse. • Se comprobará manualmente o mediante herramientas que los comandos se descodifican correctamente y que no existen comandos no documentados.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
P5: Protección frente a cambios accidentales o no intencionados *El software legalmente relevante y los datos de medida estarán protegidos frente a modificaciones involuntarias.*		
Especificaciones: Las posibles causas de fallos y modificaciones accidentales son: influencias físicas impredecibles, efectos causados por las funciones de usuario y defectos residuales del software, incluso aunque se hayan aplicado las técnicas de desarrollo actuales. Este requisito incluye: a) Influencias físicas: los datos de medida almacenados deberán estar protegidos frente a la corrupción o borrado cuando ocurre un fallo o, de forma alternativa, se detectará el fallo. b) Funciones de usuario: Antes de modificar o borrar datos, se solicitará confirmación. c) Defectos del software: Deberán tomarse las medidas apropiadas para proteger los datos frente a los modificaciones no intencionados que pudieran producirse por un diseño incorrecto del programa o errores de programación (p. ej., comprobaciones de fiabilidad).		
Documentación requerida: La documentación deberá mostrar las medidas tomadas para proteger el software y los datos frente a modificaciones involuntarias.		
Guía de validación: *Comprobaciones basadas en la documentación:* • Se comprobará que se genera y verifica de forma automática una *suma de comprobación* del código del programa y de los parámetros relevantes. • Se comprobará que no pueden sobrescribirse los datos antes de que finalice el periodo de tiempo previsto y documentado por el fabricante para el almacenamiento de estos. • Se comprobará que aparece un mensaje de advertencia en caso de que el usuario esté a punto de eliminar archivos que contengan datos de medida. *Comprobaciones funcionales:* Si existe la posibilidad de eliminar totalmente los datos de medida, se verificará mediante comprobaciones aleatorias que aparece un mensaje de advertencia antes de realizar esta acción.		
Ejemplo de solución aceptable: • La modificación accidental del software y de los datos de medida puede comprobarse mediante el cálculo de una suma de comprobación de las partes relevantes, comparándola con el valor nominal y, en caso de variación, deteniendo la modificación. • Los datos de medida no se borran sin una autorización previa; p. ej., un cuadro de diálogo o una ventana que pide confirmación para su borrado. • Para la detección de fallos consúltese también la extensión I.		

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del instrumento.
Guía de validación (además de la guía para las clases de riesgo B, C y D): *Comprobaciones basadas en el código fuente:* • Se comprobará si las medidas tomadas para la detección de modificaciones (fallos) son adecuadas. • Si se aplica una suma de comprobación, se deberá comprobar si esta incluye todas las partes del software legalmente relevante.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">P6: Protección frente a las modificaciones intencionadas
El software legalmente relevante estará protegido frente a modificaciones, cargas o intercambios (swapping) inadmisibles de la memoria hardware.</td></tr>
<tr><td colspan="3">Especificaciones:
1. Instrumento sin interfaces: La manipulación del código de programa podría ser posible mediante la manipulación de la memoria física, es decir, la memoria se extrae físicamente y se reemplaza por una que contenga software o datos fraudulentos. Para prevenir que esto suceda, la carcasa del instrumento debería protegerse o la memoria física se protegerá frente a la extracción no autorizada.
2. Instrumento con interfaces: Las interfaces no incluirán más funciones que las examinadas. Todas las funciones de las interfaces se someterán a examen (véase P4). Cuando las interfaces se utilicen para la descarga de software, deberá cumplirse la extensión D.
3. Se considerará que los datos están suficientemente protegidos solo si los procesa el software legalmente relevante. Si se pretende modificar el software legalmente no relevante después del examen de modelo, deberán cumplirse los requisitos de la extensión S.</td></tr>
<tr><td colspan="2">Documentación requerida:
La documentación garantizará que el software legalmente relevante no pueda modificarse de forma inadmisible.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
Se describirán las medidas tomadas para proteger frente a los cambios intencionados.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se examinará si son suficientes los medios documentados de seguridad frente a intercambios no autorizados de la memoria que contiene el software.
• Si la memoria puede programarse en circuito (sin desmontarla), se comprobará si el modo de programación puede deshabilitarse eléctricamente y si pueden protegerse/precintarse los medios para deshabilitarlo. (Para la comprobación de los medios de descarga, véase la extensión D)
Comprobaciones funcionales:
Se comprobará de forma práctica el modo de programación y se comprobará si funciona la deshabilitación.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
El instrumento está precintado y las interfaces cumplen los requisitos P3 y P4.</td></tr>
</table>

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del instrumento.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará en el código fuente si las medidas tomadas para la detección de cambios intencionados son adecuadas.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">P7: Protección de parámetros
Los parámetros que fijan las características legalmente relevantes del instrumento de medida estarán protegidos frente a modificaciones no autorizadas.</td></tr>
<tr><td colspan="3">Especificaciones:
1. Los parámetros específicos del modelo son idénticos para cada ejemplar del mismo y, generalmente, forman parte del código del programa. Por lo tanto, se les aplica el requisito P6.
2. Los parámetros específicos del dispositivo considerados protegidos pueden modificarse mediante el uso de un teclado integrado o interruptores o a través de interfaces, pero únicamente antes de que se hayan protegido.
3. Los parámetros específicos del dispositivo considerados configurables pueden modificarse después de protegerse.</td></tr>
<tr><td colspan="2">Documentación requerida:
La documentación debería describir todos los parámetros legalmente relevantes, sus rangos y valores nominales, dónde están almacenados, cómo pueden visualizarse, cómo y cuándo han sido protegidos, es decir, antes o después de la verificación.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
Se describirán las medidas tomadas para la protección de los parámetros.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se comprobará que es imposible cambiar o ajustar los parámetros específicos del dispositivo protegidos después de protegerlos.
• Se comprobará si todos los parámetros relevantes según las listas (proporcionadas en la extensión I, si existen) se han clasificado como protegidos.
Comprobaciones funcionales:
• Se comprobará el modo de ajuste (configuración) y se comprobará si funciona la deshabilitación tras la protección.
• Se examinará la clasificación y el estado de los parámetros (protegido/configurable) en la pantalla del instrumento, si existe una opción de menú para ello.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto .</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
a) los parámetros se protegen precintando el instrumento o la carcasa de la memoria y deshabilitando la entrada que habilita/deshabilita la escritura del circuito de memoria mediante un puente de conexión o interruptor asociados que también se han protegido.</td></tr>
<tr><td colspan="2">Registros de actividades:
b) Un contador de sucesos registra cada modificación del valor de los parámetros. Puede mostrarse el recuento actual y compararse con el valor inicial del contador registrado en la última verificación oficial y está etiquetado de forma indeleble en el instrumento.
c) Las modificaciones de los parámetros se registran en un registro de sucesos. Es un registro de información almacenado en una memoria no volátil. Cada entrada es generada automáticamente por el software legalmente relevante y contiene:
• la identificación del parámetro (p. ej., el nombre)
• el valor del parámetro (el actual o el valor anterior)
• el registro de fecha y hora del cambio.
El registro de sucesos no puede eliminarse ni modificarse sin destruir un precinto.</td><td>÷</td></tr>
</table>

Clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente que muestra la forma de proteger y visualizar los parámetros legalmente relevantes.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará en el código fuente si son adecuadas las medidas tomadas para proteger los parámetros (p. ej., modo de ajuste deshabilitado después de la protección).

5 Requisitos básicos del software de los instrumentos de medida que utilizan un ordenador universal (tipo U)

5.1 Descripción técnica

La serie de requisitos del software de esta sección se aplica a un instrumento basado en un ordenador de propósito general. La descripción técnica del sistema de medida tipo U se resume a continuación. Básicamente se debe asumir un sistema de tipo U si no se cumplen las condiciones de un instrumento de tipo P (véase el capítulo 4.1).

Configuración hardware

a) Sistema modular basado en un ordenador de propósito general. El ordenador puede ser autónomo, formar parte de una red cerrada (p. ej., Ethernet, LAN *token ring*) o parte de una red abierta (p. ej., Internet).
b) Puesto que el sistema es de propósito general, la unidad del sensor (módulo de medida) normalmente será externo al ordenador y estará conectado a él mediante un enlace de comunicación cerrado. No obstante, el enlace de comunicación también podría ser abierto (p. ej., red), de manera que podrían conectarse varios sensores.
c) La interfaz de usuario puede cambiarse de un modo operativo, que no esté sometido a control legal, a uno que sí lo esté, y viceversa.
d) El almacenamiento puede ser fijo (p. ej., disco duro) o extraíble (p. ej., disquetes, CD-RW).

Configuración software

e) Puede utilizarse cualquier sistema operativo. Además de la aplicación del instrumento de medida, pueden encontrarse a la vez otras aplicaciones de software en el sistema. Parte del software (p. ej., la aplicación del instrumento de medida) está sometido a control legal y no puede modificarse de forma inadmisible después de la aprobación. Las partes que no estén sometidas a control legal pueden modificarse.
f) El sistema operativo y los *drivers* de bajo nivel (p. ej., los *drivers* de vídeo, de la impresora, del disco, etc.) son legalmente no relevantes a menos que estén programados especialmente para una tarea de medida específica

5.2 Requisitos específicos del software para el tipo U

Clases de riesgo de la B a la E
U1: Documentación *Además de la documentación específica requerida en cada uno de los requisitos que figuran a continuación, la documentación incluirá básicamente*: a. *Una descripción de las funciones de software legalmente relevantes, el significado de los datos, etc*. b. *Descripción de la exactitud de los algoritmos de medida (p. ej., algoritmos de redondeo y cálculo de precios)* c. *Descripción de la interfaz de usuario, los menús y los diálogos*. d. *Una identificación del software legal*. e. *Descripción general del hardware del sistema (p. ej., diagrama topológico de bloques, tipo de ordenador(es), tipo de red, etc.), si no está descrita en el manual de funcionamiento*. f. *Descripción general de los aspectos de seguridad del sistema operativo (p. ej., protección, cuentas de usuario, privilegios, etc.)*. g. *Manual de funcionamiento*.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">U2: Identificación del software:
El software legalmente relevante deberá estar claramente identificado. La identificación del software estará inequívocamente ligada al mismo. Deberá determinarse y presentarse mediante un comando o durante el funcionamiento.</td></tr>
<tr><td>Especificaciones:
1. La identificación excluye al sistema operativo y a los drivers de bajo nivel (p. ej., los drivers de vídeo, de la impresora, del disco, etc.), pero debe incluir los drivers programados especialmente para una tarea específica legalmente relevante.
2. Las modificaciones del software metrológicamente relevante requieren información del organismo notificado. El organismo notificado decide si es necesaria o no una nueva identificación del software. Solo se requiere una nueva identificación del software si las modificaciones de este conducen a cambios de las funciones o características aprobadas.</td><td colspan="2">Especificaciones:
1. Restricción de 1B: se identificarán los drivers (de bajo nivel) definidos como relevantes en el examen de modelo.
2. Además de 2B: Cada modificación del código del programa legalmente relevante definido como fijo en el examen de modelo o modificaciones de los parámetros específicos del modelo requieren una nueva identificación del software.</td></tr>
<tr><td colspan="3">3. La identificación del software será fácilmente visualizable para verificación e inspección (fácilmente significa mediante la interfaz de usuario habitual, sin herramientas adicionales).
4. La identificación del software tendrá una estructura que identifique claramente las versiones que requieran examen de modelo y las que no.
5. La identificación puede aplicarse a diferentes niveles, p. ej., para programas completos, módulos, funciones, etc.
6. Si las funciones del software pueden modificarse mediante parámetros, cada función o variante puede identificarse independientemente o bien puede identificarse el paquete entero en su conjunto.</td></tr>
<tr><td colspan="2">Documentación requerida:
La documentación contendrá la identificación del software y describirá cómo se genera dicha identificación, cómo está inequívocamente ligada al propio software, cómo puede visualizarse y cómo se estructura para diferenciar entre cambios de versión que necesiten o no examen de modelo.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
La documentación mostrará las medidas tomadas para proteger la identificación del software frente a la falsificación.</td></tr>
</table>

Guía de validación: *Comprobaciones basadas en la documentación:* • Se examinará la descripción de la generación y visualización de la identificación del software. • Se comprobará si todo el software legalmente relevante está claramente identificado y descrito de modo que quede claro tanto para el organismo notificado como para el fabricante, qué funciones de software están cubiertas por la identificación del software y cuáles no. • Se comprobará si el fabricante proporciona un valor nominal de la identificación (número de versión o suma de comprobación funcional). Este deberá indicarse en el certificado de ensayos. *Comprobaciones funcionales:* • Se comprobará que la identificación del software puede visualizarse tal y como se describe en la documentación. • Se comprobará que la identificación presentada es correcta.	**Guía de validación** (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en la documentación:* Se comprobará si son adecuadas las medidas de protección tomadas frente a la falsificación.

Ejemplo de solución aceptable:

- La identificación del software legalmente relevante se compone de de dos partes. La parte (A) debe modificarse si los cambios del software requieren un nuevo examen. La parte (B) tan solo indica cambios menores del software (p. ej., correcciones de errores) que no requieren un nuevo examen.
- La parte (B) de la identificación se genera y visualiza a través de un comando.

• La parte (A) de la identificación consiste en un número de versión o el número del certificado de examen de modelo. Para evitar que se modifique con herramientas de software simples, se almacena en el archivo del programa ejecutable en formato binario.	• La parte (A) de la identificación consiste en una suma de comprobación generada automáticamente sobre el software legalmente relevante que se ha declarado fijo en el examen de modelo. Para el otro software legalmente relevante, la parte (A) es un número de versión o el número del certificado de examen de modelo. Para evitar que se modifique con herramientas de software simples, se almacena en formato binario en el archivo del programa ejecutable.	
	• Una solución aceptable para realizar la suma de comprobación es el CRC-16.	• Los algoritmos aceptables para la suma de comprobación son CRC-32 o los algoritmos hash (como SHA-1, MD5, RipeMD160, etc.).

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente que contiene la generación de la identificación.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará si todas las partes relevantes del software están cubiertas por el algoritmo que genera la identificación. • Se comprobará la correcta implementación del algoritmo.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">U3: Influencia sobre el software a través de la interfaz de usuario
Los comandos introducidos a través de la interfaz de usuario no influirán en el software legalmente relevante ni en los datos de medida de forma inadmisible.</td></tr>
<tr><td colspan="3">Especificaciones:
1. Esto implica que hay una asignación inequívoca de cada comando a una función o cambio de datos.
2. Esto implica que las actuaciones a través de teclas o interruptores que no están declaradas ni documentadas como comandos no tienen ningún efecto en las funciones y datos de medida del instrumento.
3. Los comandos pueden ser una sola actuación o secuencia de actuaciones llevadas a cabo por el operador. Se proporcionará información al usuario sobre qué comandos están permitidos.</td></tr>
<tr><td colspan="2">÷</td><td>4. El intérprete de comandos del usuario estará cerrado, es decir, el usuario no podrá cargar ni escribir programas, ni ejecutar comandos en el sistema operativo.</td></tr>
<tr><td colspan="2">Documentación requerida:
La documentación incluirá:
• Una lista completa de todos los comandos junto con una declaración de que no existen otros comandos distintos de los relacionados.
• Una breve descripción de su significado y su efecto en las funciones y datos del instrumento de medida.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
• La documentación mostrará las medidas tomadas para validar que la documentación de los comandos es completa.
• La documentación contendrá un protocolo que muestre las pruebas de todos los comandos.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se evaluará que todos los comandos documentados son admisibles; es decir, si tienen o no un efecto permitido en las funciones de medida (y datos relevantes).
• Se comprobará que el fabricante ha suministrado una declaración explícita de que la documentación de comandos es completa.
Comprobaciones funcionales:
Se realizarán pruebas (aleatorias) tanto con los comandos documentados como con los no documentados. Se comprobarán todos los elementos de menú, si existen.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si las medidas tomadas y los protocolos de prueba son adecuados para el nivel de protección alto.</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
• Un módulo en el software legalmente relevante filtra comandos inadmisibles. Solo este módulo recibe comandos y no hay forma de eludirlo. Se bloqueará cualquier entrada falsa. Mediante un módulo de software especial, se controla y orienta al usuario en la introducción de comandos. Este módulo de orientación está ligado inequívocamente al módulo que bloquea los comandos inadmisibles.</td></tr>
<tr><td colspan="2">÷</td><td>• Se bloquea el acceso al sistema operativo.</td></tr>
</table>

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del software legalmente relevante.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará en el diseño del software si el flujo de datos relativo a los comandos del software legalmente relevante está definido de manera inequívoca y puede verificarse. • Se buscarán flujos de datos inadmisibles desde la interfaz de usuario hasta los dominios que deban protegerse. • Se comprobará manualmente o mediante herramientas que los comandos se descodifican correctamente y que no existen comandos no documentados.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
U4: Influencia a través de la interfaz de comunicación *Los comandos introducidos a través de interfaces de comunicación no protegidas del dispositivo no influirán de forma inadmisible en el software legalmente relevante ni en los datos de medida*.		
Especificaciones: 1. Esto implica que hay una asignación inequívoca de cada comando a una función o cambio de datos 2. Esto implica que las señales o códigos que no están declarados ni documentados como comandos no tienen ningún efecto en las funciones y datos del instrumento. 3. Los comandos pueden ser una secuencia de señales eléctricas (ópticas, electromagnéticas, etc.) sobre los canales de entrada o códigos en los protocolos de transmisión de datos. 4. No son aplicables las restricciones de este requisito cuando se realiza una descarga de software según la extensión D.		
5. Aquellas partes del sistema operativo que interpreten comandos legalmente relevantes se considerarán software legalmente relevante. 6. Otras partes del software pueden utilizar la interfaz siempre que no perturben o falsifiquen la recepción o transmisión de los comandos o datos legalmente relevantes		5. Todos los programas y partes del programa involucrados en la transmisión y recepción de comandos o datos legalmente relevantes estarán bajo la supervisión del software legalmente relevante. 6. La interfaz que recibe o transmite comandos o datos legalmente relevantes será específica para esta función y únicamente podrá utilizarla el software legalmente relevante. Sin embargo, no se excluye el uso de interfaces estándar, si se implementan medidas de protección de software de acuerdo con la extensión T.
Documentación requerida: La documentación incluirá: • Una lista completa de todos los comandos junto con una declaración de que no existen otros comandos distintos de los relacionados. • Una breve descripción de su significado y su efecto en las funciones y datos del instrumento de medida.		**Documentación requerida** (además de la documentación requerida para las clases de riesgo B y C): • La documentación mostrará las medidas tomadas para validar que la documentación de los comandos es completa. • La documentación contendrá un protocolo que muestre las pruebas de todos los comandos o cualquier otra medida adecuada para probar que son correctos.

Guía de validación: *Comprobaciones basadas en la documentación:* • Se evaluará si todos los comandos documentados son admisibles, es decir, si tienen un efecto permitido o ningún tipo de efecto en el software (y los datos de medida) legalmente relevantes. • Se comprobará si el fabricante ha suministrado una declaración explícita de que la documentación de comandos es completa. *Comprobaciones funcionales:* Se realizarán pruebas (aleatorias), mediante equipos periféricos, si existen.	**Guía de validación** (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en la documentación:* Se comprobará que las medidas tomadas y los protocolos de prueba son adecuados para el nivel de protección alto.
Ejemplo de solución aceptable: Existe un módulo de software que recibe e interpreta comandos de la interfaz. Este módulo pertenece al software legalmente relevante. Solo reenvía comandos permitidos a los otros módulos del software legalmente relevante. Todos los comandos desconocidos o no permitidos se rechazan y carecen de efecto alguno en el software o en los datos de medida legalmente relevantes.	

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del instrumento.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará en el diseño del software si el flujo de datos relativo a los comandos del software legalmente relevante está definido de manera inequívoca y puede verificarse. • Se buscarán flujos de datos inadmisibles desde la interfaz de usuario hasta los dominios que deban protegerse. • Se comprobará manualmente o mediante herramientas que los comandos se descodifican correctamente y que no existen comandos no documentados.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">U5: Protección frente a cambios accidentales o no intencionados
El software legalmente relevante y los datos de medida estarán protegidos frente a modificaciones no intencionadas.</td></tr>
<tr><td colspan="3">Especificaciones:
1. Los cambios no intencionados pueden deberse a:
a. Un diseño de programa incorrecto, p. ej., funcionamiento en bucle incorrecto, modificación de variables globales en una función, etc.
b. Un uso incorrecto del sistema operativo
c. La sobrescritura o eliminación accidental de los datos y programas almacenados (véase también la extensión L).
d. Asignación incorrecta de los datos de una transacción de una medición. Las medidas y los datos pertenecientes a una transacción de una medición no deben mezclarse con aquellos de una transacción diferente debido a la programación o almacenamiento incorrectos.
e. Efectos físicos (perturbación electromagnética, temperatura, vibración, etc.).</td></tr>
<tr><td colspan="2">Documentación requerida:
La documentación debería mostrar las medidas tomadas para proteger el software y los datos frente a modificaciones involuntarias.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
La documentación mostrará las medidas tomadas para validar la efectividad de los medios de protección.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se comprobará que se genere y se verifique de forma automática una suma de comprobación del código del programa y de los parámetros relevantes.
• Se comprobará que no pueden sobrescribirse los datos antes de que finalice el periodo de tiempo previsto y documentado por el fabricante para el almacenamiento de estos.
• Se comprobará que aparece un mensaje de advertencia en caso de que el usuario esté a punto de eliminar archivos que contengan datos de medida.
Comprobaciones funcionales:
Si existe la posibilidad de eliminar totalmente los datos de medida, se verificará mediante comprobaciones aleatorias que aparece un mensaje de advertencia antes de realizar esta acción.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
• Se comprobará que las medidas tomadas son adecuadas para un nivel de protección alto.</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
• Prevención del diseño incorrecto del programa – esto queda fuera del alcance de estas clases de riesgo.
• Uso incorrecto del sistema operativo, sobrescritura o eliminación de los datos y programas almacenados - el fabricante debería hacer un uso total de los derechos de protección o privacidad proporcionados por el sistema operativo o por el lenguaje de programación.
• La modificación accidental de los programas y archivos de datos puede comprobarse mediante el cálculo de una suma de comprobación del código relevante, comparándolo con el valor nominal y deteniéndolo si se ha modificado el código, o reaccionando de manera adecuada si se han visto afectados parámetros o datos.
• Cuando el sistema operativo lo permita, se recomienda que se eliminen todos los derechos de usuario para la eliminación, movimiento o modificación del software legalmente relevante y que el acceso se controle mediante otros programas de utilidad. Se recomienda el acceso a los programas y datos mediante contraseñas, así como el uso de modos de solo lectura. El supervisor del sistema debería restaurar los derechos solo cuando sea necesario.</td></tr>
</table>

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del instrumento.
Guía de validación (además de la guía para las clases de riesgo B, C y D): *Comprobaciones basadas en el código fuente:* • Se comprobará si las medidas tomadas para la detección de modificaciones (fallos) son adecuadas. • Si se aplica una suma de comprobación, se deberá comprobar si esta incluye todas las partes del software legalmente relevante.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
U6: Protección frente a los cambios intencionados *El software y datos de medida legalmente relevantes se protegerán frente a modificaciones inadmisibles.*		
Especificaciones: 1. Pueden considerarse intentos de modificación con fines fraudulentos: a. Modificación del código del programa incluidos los datos integrados - si el código del programa está en formato ejecutable (.exe), estará suficientemente protegido para las clases de riesgo B y C. b. Modificación de los datos de medida - véase la extensión L. 2. La sustitución del software aprobado no deberá ser posible utilizando simplemente el sistema operativo, p. ej., cargar y utilizar software no aprobado (véase, p. ej., U3). Para descarga de software, véase la extensión D. 3. Cuando sea necesario, se tomarán medidas para proteger el software legalmente relevante frente a la modificación llevada a cabo mediante herramientas simples (p. ej., editores de texto).		**Especificaciones:** 1. El nivel de protección debería ser equivalente al del pago electrónico. En general, un ordenador universal solo es adecuado para esta clase de riesgo si dispone de hardware adicional para la protección.
Documentación requerida: La documentación debería garantizar que el software y los datos de medida almacenados no pueden modificarse de forma inadmisible.		**Documentación requerida** (además de la documentación requerida para las clases de riesgo B y C): Se deben describir las medidas de protección tomadas.
Guía de validación: **Caso 1**: Intérprete de comandos cerrado del software sometido a control legal. *Comprobaciones basadas en la documentación:* • Los módulos de software se inician automáticamente. • El usuario no tiene acceso al sistema operativo del PC. • El usuario no tiene acceso a ningún otro software que no sea el aprobado. • Se proporciona una declaración escrita que indica que no hay funciones ocultas para eludir el intérprete de comandos cerrado. **Caso 2**: Sistema operativo y/o software accesible al usuario. *Comprobaciones basadas en la documentación:* Con el código máquina de los módulos de software se genera una suma de comprobación El software legalmente relevante no puede iniciarse si el código está falsificado.		**Guía de validación** (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en la documentación:* Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.

Ejemplo de solución aceptable: • El código del programa y los datos pueden protegerse mediante sumas de comprobación. El programa calcula su propia suma de comprobación y la compara con un valor de referencia que está oculto en el código ejecutable. Si la autocomprobación falla, el programa se bloquea. • Cualquier algoritmo de firma debería tener una longitud de clave de al menos 2 bytes; sería suficiente una suma de comprobación según el algoritmo CRC-16 con un vector inicial secreto (oculto en el código ejecutable) (véanse también las extensiones L y T). • La manipulación no autorizada del software legalmente relevante puede controlarse mediante el control de acceso o los atributos de protección de privacidad del sistema operativo. El nivel de administración de estos sistemas se asegurará mediante el cierre del software o medios equivalentes.	**Ejemplo de solución aceptable**: El código de programa puede protegerse almacenando el software legalmente relevante en una unidad conectable y especializada que está precintada. Dicha unidad puede incluir, por ejemplo, una memoria de solo lectura y un microcontrolador.

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del instrumento.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará la comunicación con el hardware de protección adicional. • Se comprobará que las modificaciones de programas o datos se detectan y que en dicho caso la ejecución del programa se detiene.

Clase de riesgo B	**Clase de riesgo C**	**Clase de riesgo D**
U7: Protección de parámetros *Los parámetros legalmente relevantes estarán protegidos frente a modificaciones no autorizadas.*		
Especificaciones: 1. Los parámetros específicos del modelo son idénticos para cada ejemplar del mismo y generalmente forman parte del código del programa, es decir, del software legalmente relevante. Por lo tanto, se les aplica el requisito U6. 2. Parámetros específicos del dispositivo: • Los parámetros considerados protegidos pueden modificarse mediante el uso de un teclado integrado o interruptores o a través de interfaces, pero únicamente *antes* de que hayan protegido. Puesto que en un *ordenador universal* los parámetros específicos del dispositivo podrían manipularse mediante herramientas simples*, estos no se almacenarán en el almacenamiento estándar de un ordenador universal*. El almacenamiento de estos parámetros solo es aceptable en hardware adicional. • Los parámetros específicos del dispositivo considerados configurables pueden modificarse después de protegerse.		
Documentación requerida: La documentación deberá describir todos los parámetros legalmente relevantes, sus rangos y valores nominales, dónde están almacenados, cómo pueden visualizarse, cómo y cuándo han sido protegidos, es decir, antes o después de la verificación.		**Documentación requerida** (además de la documentación requerida para las clases de riesgo B y C): Se describirán las medidas tomadas para la protección de los parámetros.

Guía de validación: *Comprobaciones basadas en la documentación:* • Se comprobará que es adecuado el método de protección de los parámetros específicos del modelo. • Se comprobará que los parámetros específicos del dispositivo no se guardan en almacenamiento estándar del ordenador universal, sino en hardware independiente que pueda precintarse e inhabilitarse para la escritura. *Comprobaciones funcionales:* • Se comprobará el modo de ajuste (configuración) y se comprobará si funciona la deshabilitación tras la protección. • Se examinará la clasificación y el estado de los parámetros (protegido/configurable) en la pantalla del instrumento, si existe una opción de menú para ello. En el certificado de examen de modelo debería figurar una lista de aquellos parámetros que son configurables y su ubicación.	**Guía de validación** (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en la documentación:* Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.
Ejemplo de solución aceptable: • Los parámetros específicos del dispositivo se guardan en un almacenamiento conectable que está protegido frente a su posible extracción, o directamente en la unidad del sensor (módulo de medida). Se impide la escritura de los parámetros precintando en el estado deshabilitado el interruptor que permite habilitar y deshabilitar la escritura. Se pueden combinar los registros de actividades con el hardware de protección (véase P7). • Los parámetros configurables se guardan en un almacenamiento estándar del ordenador universal.	

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del instrumento.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* Se comprobará si son adecuadas las medidas tomadas para proteger los parámetros.

Clase de riesgo B	**Clase de riesgo C**	**Clase de riesgo D**
U8: Autenticidad del software y presentación de los resultados. *Se utilizarán medios para garantizar la autenticidad del software legalmente relevante. Se garantizará la autenticidad de los resultados presentados.*		
Especificaciones: 1. Se impedirá la simulación fraudulenta (*spoof*) mediante herramientas de software simples, del software legalmente relevante aprobado. 2. Los resultados presentados pueden considerarse auténticos si la presentación procede del software legalmente relevante.		**Especificaciones:** 1. Restricción de 1BC, 2BC: Son necesarios medios, basados en hardware adicional, para la protección contra el mal uso intencionado, incluyendo la simulación.
3. Los valores de medida presentados incluirán toda la información necesaria para evitar cualquier confusión con otra información (que no sea legalmente relevante). 4. Se garantizará por medios técnicos que en el ordenador universal solo pueda ejecutar funciones legalmente relevantes el software aprobado para tal fin (p. ej., la unidad del sensor o módulo de medida trabajará solo con el programa aprobado).		

<table>
<tr><td>Documentación requerida:
La documentación debería describir cómo se garantiza la autenticidad del software.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
Se describirán las medidas de protección tomadas.</td></tr>
<tr><td>Guía de validación:
Comprobaciones basadas en la documentación:
• Es necesario determinar en el examen que las presentaciones están generadas por el software legalmente relevante así como la manera de evitar las técnicas de suplantación mediante programas que no sean legalmente relevantes.
• Se comprobará que las tareas legalmente relevantes solo puedan realizarse mediante el software legalmente relevante aprobado.
Comprobaciones funcionales:
• Se comprobará a través de controles visuales si la presentación de los resultados se distingue fácilmente de otra información que también pueda presentarse.
• Se comprobará, de acuerdo con la documentación, si la información presentada es completa.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.</td></tr>
<tr><td colspan="2">Ejemplo de solución aceptable:
Medios formales:
1. La parte (B) de identificación del software (suma de comprobación, número de versión o número del certificado de examen de modelo, véase U2) indicada por el software se compara con el valor presente en el certificado de examen de modelo.
Medios técnicos:
1. El software legalmente relevante genera una ventana para la aplicación de medida. Las medidas técnicas necesarias de la ventana son:
• Los programas legalmente no relevantes no tendrán acceso alguno a los valores de medición hasta que estos hayan sido mostrados.
• La ventana se refrescará periódicamente. El programa asociado comprobará que esté siempre visible.
• El procesamiento de los valores de medida se detiene siempre que esta ventana se cierre o no esté completamente visible.
El manual de funcionamiento (y el certificado de examen de modelo) debería contener una copia de la ventana como referencia.
2a. La unidad del sensor (módulo de medida) cifra los valores de medición con una clave conocida para el software aprobado que funciona en el ordenador universal (p. ej., su número de versión). Solo el software aprobado puede descifrar y utilizar los valores de medida, los programas no aprobados en el ordenador universal no podrán hacerlo ya que desconocen la clave. Para el tratamiento de claves, véase la extensión T.
2b. Antes de enviar los valores de medida, la unidad del sensor inicia una secuencia de protocolo (handshake) con el software legalmente relevante en el ordenador universal basada en claves secretas. La unidad del sensor enviará sus valores de medida, solo si el programa del ordenador universal se comunica correctamente. Para el tratamiento de claves, véase la extensión T.</td></tr>
<tr><td>3. La clave utilizada en 2a/2b puede elegirse e introducirse en la unidad del sensor y en el software del ordenador universal sin destruir ningún precinto.</td><td>3. La clave utilizada en 2a/2b es el código hash del programa del ordenador universal. Cada vez que se modifique el software en el PC, la nueva clave se introducirá en la unidad del sensor y se precintará.</td></tr>
</table>

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del software legalmente relevante.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará que el software legalmente relevante genera los resultados de medición presentados. • Se comprobará si todas las medidas tomadas son adecuadas y correctas para garantizar la autenticidad del software (p. ej., que las tareas legalmente relevantes solo pueden realizarse mediante el software legalmente relevante aprobado).

Clases de riesgo de la B a la E
U9: Influencia de otro software *El software legalmente relevante se diseñará de tal manera que ningún otro software influya en él de modo inadmisible.*
Especificaciones: Este requisito implica la separación del software entre el software legalmente relevante y el que no lo es. Se cumplirá la extensión S. Este es el caso estándar para ordenadores universales.
Documentación requerida: Véase la extensión S.
Guía de validación: Véase la extensión S.
Ejemplo de solución aceptable: Véase la extensión S.

6 Extensión L: Almacenamiento a largo plazo de los datos de medida

Es una extensión a los requisitos específicos del software integrado en instrumentos de medida desarrollados específicamente (requisitos para tipo P) y del software para instrumentos de medida que utilizan un ordenador universal (requisitos para tipo U). Describe los requisitos para el almacenamiento de los datos de medida desde el momento en que se haya completado físicamente una medición hasta que han finalizado todos los procesos que deba realizar *el software legalmente relevante*. Esto también se aplica al almacenamiento posterior de los datos.

6.1 Descripción técnica

La serie de requisitos de esta extensión solo se aplica si incluye almacenamiento a largo plazo de los datos de medida. Se refiere solo a aquellos datos de medida legalmente relevantes. En la siguiente tabla se presentan tres configuraciones técnicas distintas para el almacenamiento a largo plazo. En el caso de un dispositivo de medida desarrollado específicamente es típica la opción de un almacenamiento integrado: el almacenamiento forma parte del hardware y del software metrológicamente necesarios. En el caso de instrumentos que usan un ordenador universal, es típica otra opción: el uso de recursos ya existentes, p. ej., discos duros. La tercera opción es la del almacenamiento extraíble: el almacenamiento puede extraerse del dispositivo, que puede ser o un dispositivo desarrollado específicamente o un ordenador universal, y puede llevarse a cualquier parte. Cuando se recuperan datos de un almacenamiento extraíble para fines legales, p. ej., visualización, impresión de recibos, etc., el dispositivo de recuperación estará sometido a control legal.

Almacenamiento integrado Instrumento simple, desarrollado específicamente, sin herramientas externas o medios que permitan editar o cambiar datos, almacenamiento integrado de datos o parámetros de medida, p. ej., memoria RAM, memoria flash o disco duro.
Almacenamiento para ordenador universal Ordenador universal, interfaz gráfica de usuario, sistema operativo multitarea, las tareas sometidas a control legal y las que no lo están coexisten paralelamente, se puede extraer el almacenamiento del dispositivo o se pueden copiar los contenidos ya sea dentro o fuera del ordenador.
Almacenamiento extraíble o remoto (externo) Instrumento básico (instrumento desarrollado específicamente o que utiliza un ordenador universal), el almacenamiento se puede extraer del instrumento. Estos pueden ser, por ejemplo, disquetes, tarjetas flash o bases de datos remotas conectadas a través de la red.

Tabla 6-1: Descripción técnica de almacenamientos a largo plazo

6.2 Requisitos específicos del software para almacenamiento a largo plazo

Los requisitos que se muestran en esta sección se deben aplicar junto con una serie de requisitos, ya sea para los instrumentos básicos desarrollados específicamente o para aquellos que utilizan un ordenador universal.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
L1 Completitud de los datos de medida almacenados *Los datos de medida almacenados deben contener toda la información relevante que sea necesaria para reproducir mediciones anteriores*.		
Especificaciones: Los datos de medida almacenados pueden ser necesarios como referencia en una fecha posterior; p. ej., para comprobar facturas. Todos los datos necesarios, tanto por razones legales como por razones metrológicas, se almacenarán junto con los valores de medida.		
Documentación requerida: Descripción de todos los campos de los conjuntos de datos.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si se incluye en el conjunto de datos toda la información necesaria para fines legal y metrológicamente relevantes .		
Ejemplo de solución aceptable: El conjunto de datos legal y metrológicamente completo consta de los siguientes campos: • valores de medida con la resolución correcta; • unidades de medida legalmente correctas; • precio unitario o precio que hay que pagar (si es aplicable); • momento y lugar de la medición (si es aplicable); • identificación del instrumento (si es aplicable) (almacenamiento externo). Los datos se almacenan con la misma resolución, valores, unidades, etc., que indica o imprime el instrumento.		

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B, C y D): El código fuente que genera los conjuntos de datos para su almacenamiento.
Guía de validación (además de la guía para las clases de riesgo B, C y D): *Comprobaciones basadas en el código fuente:* Se comprobará que los conjuntos de datos se crean correctamente.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">L2 Protección frente a cambios accidentales o no intencionados
Los datos almacenados estarán protegidos frente a cambios accidentales o no intencionados.</td></tr>
<tr><td colspan="3">Especificaciones:
1. Los cambios de datos accidentales pueden deberse a efectos físicos.
2. Los cambios no intencionados pueden deberse al usuario del dispositivo. Las tareas de mantenimiento de los datos pueden requerir que se elimine de cuando en cuando la información relativa a facturas pagadas o vencidas. Deberían utilizarse medios automáticos o semiautomáticos para garantizar que solamente se eliminen los datos especificados y se evite la eliminación accidental de datos "vivos". Esto es particularmente importante en sistemas conectados en red y en el caso de almacenamiento remoto o extraíble, donde los usuarios podrían no darse cuenta de la importancia de los datos.
3. El receptor calculará una suma de comprobación y la comparará con el valor de referencia asociado. Si los valores coinciden, el conjunto de datos es válido y se puede utilizar; si no se deben eliminar o marcar como inválidos.</td></tr>
<tr><td colspan="2">Documentación requerida:
Descripción de las medidas de protección (p. ej., el algoritmo de la suma de comprobación, incluyendo la longitud del polinomio generador).</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
La documentación describirá las medidas tomadas para validar la efectividad de los medios de protección.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se comprobará que se genere una suma de comprobación de los datos.
• Se comprobará que el software legalmente relevante que lee los datos y calcula la suma de comprobación, compara verdaderamente el valor calculado con el de referencia.
• Se comprobará que los datos no se pueden sobrescribir antes de que se acabe el periodo de almacenamiento previsto y documentado por el fabricante.
• Se comprobará que aparece un mensaje de advertencia en caso de que el usuario esté a punto de eliminar archivos que contengan datos de medida.
Comprobaciones funcionales:
Si existe la posibilidad de eliminar los datos de medida, se verificará mediante comprobaciones aleatorias que aparece un mensaje de advertencia antes de realizar esta acción.</td><td>Guía de validación (además de la guía para las clases de riesgo B, y C):
Comprobaciones basadas en la documentación:
Se comprobará que las medidas tomadas sean adecuadas para un nivel de protección alto.</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
• Para detectar cambios en los datos debido a efectos físicos, se calcula una suma de comprobación con el algoritmo CRC-16 de todo el conjunto de datos y se inserta en el mismo conjunto para su almacenamiento.
<u>Nota:</u> El algoritmo no es secreto y, al contrario que en el requisito L3, tampoco lo son el vector inicial del registro CRC ni el polinomio generador, es decir, el divisor en el algoritmo. El vector inicial y el polinomio generador son conocidos tanto por el programa que crea como por el que verifica las sumas de comprobación.
• Los datos de medida y los archivos de facturas pueden protegerse asociando un registro automático con la fecha y hora de su creación o con una bandera o etiqueta que indica si las facturas están pagadas o no. Un programa de utilidad podría mover o eliminar los archivos solo si las facturas están cobradas o vencidas.
• Los datos de medida no se eliminan sin una autorización previa; p. ej., un cuadro de diálogo o una ventana que pide confirmación para la eliminación.</td></tr>
</table>

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B, C y D): El código fuente que realiza la protección de los datos almacenados.
Guía de validación (además de la guía para las clases de riesgo B, C y D): *Comprobaciones basadas en el código fuente:* Se comprobará que las medidas tomadas para proteger los datos almacenados son adecuadas y se han implementado correctamente.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
L3 Integridad de los datos *Los datos de medida almacenados deben estar protegidos frente a cambios intencionados*.		
Especificaciones: 1. Este requisito se aplica a todos los tipos de almacenamiento, excepto a los integrados. 2. La protección debe ser efectiva contra cambios intencionados llevados a cabo mediante herramientas comunes de software. 3. Se entiende por herramientas comunes de software, aquellas que están fácilmente disponibles y su uso es sencillo; p. ej., los paquetes de ofimática.		**Especificaciones:** 1. Este requisito se aplica a todos los tipos de almacenamiento, excepto a los integrados. 2. La protección debe ser efectiva contra cambios intencionados realizados mediante herramientas sofisticadas de software. 3. Las «herramientas sofisticadas de software» son, p. ej., depuradores, recompiladores, herramientas de desarrollo de software, etc. 4. El nivel de protección deberá ser equivalente al que se requiere para el pago electrónico. 5. La protección se aplica mediante una firma electrónica con un algoritmo que garantiza que no existen firmas idénticas para conjuntos de datos diferentes. *Nota:* Incluso si el algoritmo y la clave cumplen el nivel alto de protección, una solución técnica con un PC estándar **no** alcanzaría este nivel de protección si no hay medios de protección para los programas que firman o verifican los conjuntos de datos (véase la guía básica **U** para ordenadores universales en el comentario del requisito U6 - D).
Documentación requerida: El método para realizar la protección deberá estar documentado.		**Documentación requerida** (además de la documentación requerida para las clases de riesgo B y C): Se describirán las medidas de protección tomadas.

Guía de validación:
Comprobaciones basadas en la documentación:
• Si se usa una suma de comprobación o una firma:
  • Se comprobará si esta se genera sobre todo el conjunto de datos.
  • Se comprobará que el software legalmente relevante, que lee los datos y calcula la suma de comprobación o descifra la firma, verdaderamente compara el valor calculado con el de referencia.
• Se comprobará que los datos secretos (p. ej., el valor inicial de la clave, si se utiliza) se mantienen secretos contra el espionaje con herramientas simples.
Comprobaciones funcionales:
Se comprobará que el programa de recuperación rechaza un conjunto de datos falsificados.
	Guía de validación (además de la guía para las clases de riesgo B y C):
	Comprobaciones basadas en la documentación:
	Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.

Ejemplo de solución aceptable: Justo antes de reutilizar los datos, se recalcula el valor de la suma de comprobación y se compara con el valor de referencia almacenado. Si los valores coinciden, el conjunto de datos es válido y se puede utilizar; si no, debe eliminarse o marcarse como inválido. Una solución aceptable es el algoritmo **CRC-16**. *Nota:* El algoritmo no es secreto pero, al contrario que en el requisito **L2**, debe serlo el vector inicial del registro CRC o el polinomio generador (es decir, el divisor en el algoritmo). El vector inicial y el polinomio generador solo los conocen los programas que generan y verifican las sumas de comprobación. Deben tratarse como *claves* (véase **L5**).	**Ejemplo de solución aceptable:** En lugar de CRC, se calcula una firma. Un algoritmo de firma adecuado podría ser uno de los algoritmos hash (p. ej., SHA-1 o RipeMD160), combinado con un algoritmo de cifrado como RSA o de curvas elípticas. La longitud mínima de la clave es de 768 bits (RSA) o 128-160 bits (curvas elípticas).

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente que lleva a cabo la integridad de los datos almacenados.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* Se comprobará que las medidas tomadas para garantizar la integridad de los datos almacenados son adecuadas y están correctamente implementadas.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">L4 Autenticidad de los datos de medida almacenados
Deben poder rastrearse fielmente los datos de medida almacenados hasta la medición que los generó.</td></tr>
<tr><td colspan="3">Especificaciones:
1. La autenticidad de los datos de medida puede ser necesaria como referencia en una fecha posterior; p. ej., para comprobar facturas.
2. La autenticidad requiere la correcta asignación (vinculación) de los datos de medida a la medición que los generó.
3. La autenticidad presupone la identificación de los conjuntos de datos.
4. Para garantizar la autenticidad, no se requiere necesariamente cifrar los datos.</td></tr>
<tr><td colspan="2">Documentación requerida:
Descripción del método utilizado para garantizar la autenticidad.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
Se describirán las medidas de protección tomadas.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se comprobará que existe un enlace correcto entre cada valor de medida y la medición correspondiente.
• Si se usa una suma de comprobación o una firma, se comprobará si esta se genera sobre el todo el conjunto de datos.
• Se comprobará que los datos secretos (p. ej., el valor inicial de la clave, si se utiliza) se mantienen secretos contra el espionaje con herramientas simples.
Comprobaciones funcionales:
Se comprobará que tanto los datos almacenados como los datos que aparecen en el recibo o factura son idénticos.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
Un conjunto de datos almacenados contiene los siguientes campos de datos (además de los campos definidos en L3):
• Un único número de identificación (actual). El número de identificación también se copia en la nota generada por el instrumento (tique).
• La fecha/hora a la que se ha realizado la medida (registro de fecha y hora). El registro de fecha y hora también se copia en el tique.
• Una identificación del instrumento de medida que ha generado el valor.
• La firma que se usa para garantizar la integridad de los datos puede utilizarse simultáneamente para garantizar la autenticidad. La firma cubre todos los campos del conjunto de datos. Consúltense los requisitos L2, L3.
• En el tique se puede reflejar que los valores de medida pueden compararse con los datos de referencia que están almacenados en un medio sometido a control legal. Esta correspondencia se demuestra comparando el número de identificación o el registro de fecha y hora impreso en el tique con aquella del conjunto de datos almacenados.</td></tr>
<tr><th colspan="3">Consideraciones adicionales para la clase de riesgo E</th></tr>
<tr><td colspan="3">Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
El código fuente que genera los conjuntos de datos para almacenarlos y realiza la autenticación.</td></tr>
<tr><td colspan="3">Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en el código fuente:
Se comprobará que los conjuntos de datos se crean correctamente y se autentican de manera fidedigna.</td></tr>
</table>

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">L5: Confidencialidad de las claves
Las claves y los datos que las acompañan deben tratarse como datos legalmente relevantes y mantenerse ocultos y protegidos frente a posibles riesgos originados por herramientas software.</td></tr>
<tr><td colspan="2">Especificaciones:
1. Este requisito solo se aplica si se utiliza una clave secreta.
2. Este requisito se aplica al almacenamiento de datos de medida que se lleva a cabo en un dispositivo externo al instrumento de medida o mediante ordenadores universales.
3. La protección se debe aplicar frente a cambios intencionados realizados mediante herramientas comunes de software.
4. Si el acceso a las claves secretas está restringido, p. ej., mediante el precintado de la carcasa de un dispositivo desarrollado específicamente, no se necesitará ningún medio de protección software adicional.</td><td>Especificaciones:
1. Este requisito se aplica al almacenamiento en ordenadores universales y en dispositivos externos.
2. La protección se debe aplicar frente a cambios intencionados realizados mediante herramientas sofisticadas de software.
3. Se deben utilizar métodos adecuados equivalentes a los del pago electrónico. El usuario debe ser capaz de verificar la autenticidad de la clave pública.</td></tr>
<tr><td colspan="2">Documentación requerida:
Descripción de la gestión de las claves y de los medios para mantener las claves y la información asociada en secreto.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
Se describirán las medidas de protección tomadas.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
Se comprobará que la información secreta no pueda verse comprometida.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.</td></tr>
<tr><td colspan="2">Ejemplo de solución aceptable:
La clave secreta y los datos que la acompañan están almacenados en formato binario en el código ejecutable del software legalmente relevante. Por tanto no es obvia la dirección en la que se almacenan estos datos. El software del sistema no ofrece ninguna opción para editar o ver estos datos. Si el algoritmo CRC se utiliza como firma, el vector inicial o polinomio generador desempeña la función de clave.</td><td>Ejemplo de solución aceptable:
La clave secreta se almacena en una parte del hardware que puede precintarse físicamente. El software no ofrece ninguna opción para ver o editar estos datos.
Nota: Una solución técnica con un PC estándar podría no ser suficiente para garantizar el alto nivel de protección si no existen medios hardware de protección adecuados para la clave y otros datos secretos (véase la guía básica para ordenador universal U6).
1) Infraestructura PKI: la clave pública del almacenamiento sometido a control legal ha sido certificada por una Autoridad certificadora.
2) Confianza directa: no es necesario implicar a una Autoridad certificadora si, por un acuerdo anterior, ambas partes son capaces de leer la clave pública del instrumento de medida directamente en un dispositivo sometido a control legal que muestra el conjunto de datos relevantes.</td></tr>
</table>

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente que realiza la gestión de las claves.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* Se comprobará que las medidas tomadas para la gestión de claves son adecuadas.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">L6: Recuperación de los datos almacenados
El software utilizado para verificar los conjuntos de datos de medida almacenados mostrará o imprimirá los mismos, comprobará si han sido modificados y avisará si ha encontrado cambios. Los datos detectados como corruptos no deben utilizarse.</td></tr>
<tr><td colspan="3">Especificaciones:
1. Los datos de medida almacenados podrían ser necesarios como referencia en una fecha posterior; p. ej., si se cuestiona alguna transacción. Si existe alguna duda en la corrección de un tique o recibo, deberá ser posible identificar sin ambigüedad los datos de medida almacenados de la medición puesta en duda (véase también L1, L3, L4 y L5).
2. El número de identificación (véase L1) debe estar impreso en el tique o recibo del cliente, junto con una explicación y una referencia al almacenamiento sometido a control legal.
3. La verificación consiste en comprobar la integridad, autenticidad y correcta asignación de los datos de medida almacenados.
4. El software de verificación utilizado para mostrar o imprimir los datos almacenados estará sometido a control legal.
5. Para los requisitos específicos de un instrumento, consulte la extensión I.</td></tr>
<tr><td colspan="2">Documentación requerida:
• Descripción de las funciones del programa de recuperación.
• Descripción de la detección de datos corruptos.
• Manual de funcionamiento de este programa.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
Se describirán las medidas de protección tomadas.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se comprobará que el software de recuperación verdaderamente compara el valor calculado con los valores de referencia.
• Se comprobará que el software de recuperación forme parte del software legalmente relevante.
Comprobaciones funcionales:
• Se comprobará si el programa detecta conjuntos de datos corruptos.
• Se realizarán comprobaciones aleatorias para verificar que la recuperación proporciona toda la información necesaria.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
El programa de verificación lee el conjunto de datos almacenado, recalcula la firma sobre todos los campos de datos y la compara con el valor de referencia almacenado. Si ambos valores coinciden, el conjunto de datos es correcto; de lo contrario, los datos no se utilizan y el programa los elimina o marca como inválidos.</td></tr>
</table>

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del programa de recuperación.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* Se comprobará si las medidas tomadas para recuperación, verificación de firmas, etc. son adecuadas y están correctamente implementadas.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
L7: Almacenamiento automático. *Los datos de medida deberán almacenarse automáticamente cuando concluya la medición.*		
Especificaciones: 1. Este requisito se aplica a todos los tipos de almacenamiento. 2. Este requisito significa que la función de almacenamiento no dependerá de la decisión del operador. Sin embargo, algunos tipos de instrumentos, p. ej. instrumentos de pesaje, solicitan al operador la aceptación o no del resultado. En otras palabras, podrían existir algunas medidas intermedias que no se almacenen (por ejemplo durante la carga o antes de que la cantidad de productos solicitados se encuentre en el receptor de carga). No obstante, incluso en este caso, el resultado se almacenará automáticamente cuando el operador lo acepte. 3. En caso de que se realice un almacenamiento completo, véase el requisito L8.		
Documentación requerida: Confirmación de que el almacenamiento se realiza de forma automática. Descripción de la interfaz gráfica de usuario.		
Guía de validación: *Comprobaciones funcionales:* Se examinará mediante comprobaciones aleatorias que los valores de medida se almacenan automáticamente después de terminar o aceptar la medición. Se comprobará que no existen botones ni opciones de menú que interrumpan o deshabiliten el almacenamiento automático.		
Ejemplo de solución aceptable: No existen opciones de menú ni botones en la interfaz gráfica de usuario que permitan iniciar manualmente el almacenamiento de los resultados de medida. Los valores de medida se combinan en un conjunto de datos junto con información adicional, tal como un registro de fecha y hora o una firma y se almacenan inmediatamente después de realizar o aceptar la medición, respectivamente.		

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B, C y D): El código fuente del instrumento.
Guía de validación (además de la guía para las clases de riesgo B, C y D): *Comprobaciones basadas en el código fuente:* Se comprobará si las medidas tomadas para el almacenamiento automático son adecuadas y se implementan correctamente.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D

L8: Capacidad de almacenamiento y continuidad

El almacenamiento a largo plazo debe tener la capacidad suficiente para el uso previsto.

Especificaciones:

1. Cuando un medio de almacenamiento está lleno o se extrae/desconecta del instrumento, el operador recibirá una advertencia. No será necesaria esta advertencia si se asegura en la construcción que solo los datos fuera de fecha se pueden sobrescribir. Para otras acciones necesarias, consulte los requisitos específicos del instrumento de medida (extensión I).
2. La regulación relativa al período mínimo de almacenamiento de los datos de medida está fuera del alcance de este requisito y es competencia de las regulaciones nacionales. Es responsabilidad del propietario tener un instrumento con suficiente capacidad de almacenamiento para cumplir los requisitos aplicables a su actividad. El organismo notificado para el examen «CE» de modelo solo comprobará que los datos se almacenan y se recuperan correctamente y si se impiden nuevas transacciones cuando el almacenamiento está lleno.
3. La exigencia de ciertas inscripciones en el dispositivo, tales como las relativas a la capacidad de almacenamiento o a otra información incluida que permite calcular la capacidad, también está fuera del alcance de este requisito. No obstante, el fabricante facilitará la información sobre la capacidad.

Documentación requerida:

Descripción de la gestión de casos excepcionales cuando se almacenan valores de medida.

Guía de validación:

Comprobaciones basadas en la documentación:

- Se comprobará que el fabricante proporciona la capacidad de almacenamiento o una fórmula para calcularla.
- Se comprobará que no puedan sobrescribirse los datos antes de que finalice el periodo de tiempo para el almacenamiento de estos, previsto y documentado por el fabricante.

Comprobaciones funcionales:

- Se comprobará que aparece un mensaje de advertencia en caso de que el usuario esté a punto de eliminar archivos que contengan datos de medida (si existe posibilidad de eliminarlos).
- Se comprobará que aparece un mensaje de advertencia si el almacenamiento está lleno o se ha extraído.

Ejemplo de solución aceptable:

- Para mediciones que se pueden interrumpir, que de manera rápida y sencilla se pueden detener (p. ej., pesaje, medición de combustible, etc.), la medición se puede completar incluso si el almacenamiento deja de estar disponible. El instrumento o dispositivo de medida debería tener un *buffer* (memoria intermedia) que tenga la capacidad suficiente para almacenar la transacción en curso. Después de esto, no se podrá comenzar ninguna otra transacción y los datos almacenados en el *buffer* se guardarán para que puedan transmitirse más adelante a un almacenamiento nuevo.
- Las mediciones que no se pueden interrumpir (p. ej., las mediciones de energía, volumen, etc.) no necesitarán un *buffer* especial intermedio porque estas mediciones siempre son acumulativas. El registro acumulativo podrá leerse y transferirse al medio de almacenamiento más tarde, cuando este vuelva a estar disponible.
- Los datos de medida podrán sobrescribirse automáticamente mediante un programa de utilidad que compruebe si el plazo establecido de dichos datos está vencido (consulte los reglamentos nacionales relativos a los periodos de tiempo establecido legalmente) o si se ha pagado la factura. El programa de utilidad mostrará un mensaje de confirmación al usuario para eliminar los datos que se borrarán en orden desde el más antiguo.

Consideraciones adicionales para la clase de riesgo E

Documentación requerida (además de la documentación requerida para las clases de riesgo B, C y D):

El código fuente que realiza el almacenamiento de datos.

Guía de validación (además de la guía para las clases de riesgo B, C y D):

Comprobaciones basadas en el código fuente:

Se comprobará si las medidas tomadas para el almacenamiento son adecuadas y se implementan correctamente.

7 Extensión T: Transmisión de datos de medida a través de redes de comunicación

Esta es una extensión de los requisitos del software de las guías básicas P y U. Solo debe utilizarse si los datos de medida se transmiten a través de redes de comunicación a un dispositivo remoto donde se terminen de procesar y/o se utilicen para fines regulados legalmente. Esta extensión no se aplica a menos que haya algún procesamiento posterior de datos legalmente relevantes. Si el software se descarga en un dispositivo sometido a control legal, se aplican los requisitos de la extensión D.

7.1 Descripción técnica

La serie de requisitos de esta extensión se aplica únicamente si el dispositivo en cuestión está conectado a una red y transmite o recibe datos de medida legalmente relevantes. En la siguiente tabla, se identifican tres configuraciones de red. La más simple es un conjunto de dispositivos que están todos sometidos a control legal. Los participantes se fijan en la verificación legal. Una variante de esto (red cerrada, parcialmente sometida a control legal) es una red con participantes que no están sometidos a control legal pero todos son conocidos y no cambian durante la operación. Una red abierta no tiene limitaciones en cuanto a la identidad, funcionalidad, presencia y ubicación de los participantes.

Descripción de las configuraciones
Red cerrada, completamente sometida a control legal Solo hay un número fijo de participantes conectados, con una identidad, funcionalidad y ubicación claras. Todos los dispositivos están sometidos a control legal. No existen dispositivos en la red que no estén sometidos a control legal.
Red cerrada, parcialmente sometida a control legal Hay un número fijo de participantes con una identidad y ubicación claras conectados a la red. No todos los dispositivos están sometidos a control legal y, por tanto, se desconoce su funcionalidad.
Red abierta A la red se pueden conectar participantes arbitrarios (dispositivos con funciones arbitrarias). La identidad y funcionalidad de un dispositivo participante y su ubicación pueden ser desconocidas para otros participantes. Cualquier red que contenga dispositivos sometidos a control legal con receptor de infrarrojos o interfaces de comunicación entre redes inalámbricas se considerará red abierta.

Tabla 7-1: Descripción técnica a través de redes de comunicación.

7.2 Requisitos específicos del software para transmisión de datos

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
T1: Completitud de los datos transmitidos *Los datos transmitidos deberán contener toda la información relevante necesaria para presentar o procesar posteriormente los resultados de medida en la unidad receptora.*		
Especificaciones: La parte metrológica de un conjunto de datos transmitidos se compone de uno o varios valores de medida con la resolución correcta, la unidad de medida correcta legalmente, y según la aplicación, el precio unitario o el precio a pagar y el lugar de la medición.		
Documentación requerida: Se documentarán todos los campos del conjunto de datos.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si se incluye en el conjunto de datos toda la información para el procesamiento posterior de los valores de medida en la unidad receptora .		
Ejemplo de solución aceptable: El conjunto de datos contiene los siguientes campos: • valores de medida con la resolución correcta; • unidades de medida legalmente correctas; • precio unitario o precio que hay que pagar (si es aplicable); • hora y fecha de la medición (si es aplicable); • identificación del instrumento (si es aplicable) (transmisión de datos); • El lugar de la medición (si es aplicable).		

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B, C y D): El código fuente que genera los conjuntos de datos para su transmisión.
Guía de validación (además de la guía para las clases de riesgo B, C y D): *Comprobaciones basadas en el código fuente:* Se comprobará que los conjuntos de datos se crean correctamente.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
T2: Protección frente a los cambios accidentales o no intencionados *Los datos transmitidos estarán protegidos frente a cambios accidentales o no intencionados*.		
Especificaciones: 1. Los cambios de datos accidentales pueden deberse a efectos físicos. 2. Los cambios no intencionados pueden deberse al usuario del dispositivo. 3. Se proporcionarán medios para detectar errores de transmisión.		
Documentación requerida: • Descripción del algoritmo de la suma de comprobación, si se usa, incluida la longitud del polinomio generador. • Descripción de un método alternativo en caso de que se utilice.		**Documentación requerida** (además de la documentación requerida para las clases de riesgo B y C): La documentación describirá las medidas tomadas para validar la efectividad de los medios de protección.
Guía de validación: *Comprobaciones basadas en la documentación:* • Se comprobará que se genere una suma de comprobación de los datos. • Se comprobará que el software legalmente relevante que recibe los datos recalcula la suma de comprobación y la compara con el valor de referencia incluido en el conjunto de datos.		**Guía de validación** (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en la documentación:* Se comprobará que las medidas tomadas sean adecuadas para un nivel de protección alto.

Ejemplo de solución aceptable:

1) Para detectar cambios en los datos, se calcula una suma de comprobación con el algoritmo **CRC-16** de todos los bytes del conjunto de datos y se inserta en dicho conjunto para su transmisión. Justo antes de reutilizar los datos, el receptor recalcula el valor de la suma de comprobación y lo compara con el valor de referencia adjunto. Si los valores coinciden, el conjunto de datos es válido y se puede utilizar; si no, habrá que eliminarlo o marcarlo como inválido.

   Nota: El algoritmo no es secreto y, al contrario que en el requisito T3, tampoco lo son el vector inicial del registro CRC ni el polinomio generador, es decir, el divisor en el algoritmo. El vector inicial y el polinomio generador son conocidos tanto por el programa que crea como por el que verifica las sumas de comprobación.

2) Usar los medios proporcionados por los protocolos de transmisión, p. ej., TCP/IP o IFSF.

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B, C y D): El código fuente que realiza la protección de los datos transmitidos.
Guía de validación (además de la guía para las clases de riesgo B, C y D): *Comprobaciones basadas en el código fuente:* Se comprobará que las medidas tomadas para proteger los datos transmitidos son adecuadas.

Clase de riesgo B	**Clase de riesgo C**	**Clase de riesgo D**
T3·: Integridad de los datos *Los datos transmitidos legalmente relevantes deben estar protegidos frente a cambios intencionados realizados con herramientas software.*		
Especificaciones: 1. Este requisito solo se aplica a redes abiertas o parcialmente sometidas a control legal, y no a redes cerradas. 2. La protección debe ser efectiva contra cambios intencionados llevados a cabo mediante herramientas comunes de software. 3. Se entiende por herramientas comunes de software aquellas que están fácilmente disponibles y su uso es sencillo; p. ej., los paquetes de ofimática.		**Especificaciones:** 1. Este requisito se aplica a redes abiertas y a redes cerradas parcialmente sometidas a control legal. 2. La protección se aplica mediante una firma electrónica con un algoritmo que garantiza que no existen firmas idénticas para conjuntos de datos diferentes 3. La protección debe ser efectiva contra cambios intencionados realizados mediante herramientas sofisticadas de software. 4. Las «herramientas sofisticadas de software» son, p. ej., depuradores, recompiladores, herramientas de desarrollo de software, etc. 5. El nivel de protección deberá ser equivalente al que se requiere para el pago electrónico. *Nota:* Incluso si el algoritmo y la clave cumplen el nivel alto de protección, una solución técnica con un PC estándar **no** alcanzaría este nivel de protección si no hay medios de protección para los programas que firman o verifican los conjuntos de datos (véase la guía básica **U** para ordenadores universales en comentario del requisito U6-D).
Documentación requerida: Descripción del método de protección		**Documentación requerida** (además de la documentación requerida para las clases de riesgo B y C): Se describirán las medidas de protección tomadas.

Guía de validación:
Comprobaciones basadas en la documentación:
• Si se usa una suma de comprobación o una firma:
  • Se comprobará si esta se genera sobre todo el conjunto de datos.
  • Se comprobará que el software legalmente relevante, que recibe los datos y recalcula la suma de comprobación o descifra la firma, verdaderamente compara el valor calculado con el de referencia.
• Se comprobará que los datos secretos (p. ej., el valor inicial de la clave, si se utiliza) se mantienen ocultos ante el espionaje con herramientas simples.
	Guía de validación (además de la guía para las clases de riesgo B y C):
	Comprobaciones basadas en la documentación:
	Se comprobará si las medidas tomadas son adecuadas respecto a la tecnología actual para garantizar un nivel de protección alto.

Ejemplo de solución aceptable: Se genera una suma de comprobación de los datos a transmitir. Justo antes de reutilizar los datos, se recalcula el valor de la suma de comprobación y se compara con el valor de referencia incluido en el conjunto de datos recibido. Si los valores coinciden, el conjunto de datos es válido y se puede utilizar; si no, debe eliminarse o marcarse como inválido. Una solución aceptable es el algoritmo **CRC-16**. *Nota:* El algoritmo no es secreto pero, al contrario que en el requisito T2, sí debe serlo el vector inicial del registro CRC o el polinomio generador (es decir, el divisor en el algoritmo). El vector inicial y el polinomio generador solo los conocen los programas que generan y verifican las sumas de comprobación. Deben tratarse como *claves* (véase **T5**).	**Ejemplo de solución aceptable:** • En lugar del CRC, se calcula una firma. Un algoritmo de firma adecuado podría ser uno de los algoritmos *hash* (p. ej., SHA-1 o RipeMD160), combinado con un algoritmo de cifrado como el RSA o el de curvas elípticas. La longitud mínima de la clave es de 768 bits (RSA) o 128-160 bits (curvas elípticas). • Algunos protocolos de transmisión proporcionan protección (p. ej., HTTPS).

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente que lleva a cabo la integridad de los datos transmitidos.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* Se comprobará que las medidas tomadas para garantizar la integridad de los datos transmitidos son adecuadas.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">T4: Autenticidad de los datos transmitidos
El programa que reciba los datos relevantes transmitidos, deberá poder verificar la autenticidad y la asignación de los valores de medida a una medición determinada.</td></tr>
<tr><td colspan="3">Especificaciones:
1a. En una red de participantes desconocidos, es necesario identificar sin ambigüedad el origen de los datos de medida transmitidos. (La autenticidad se basa en el número de identificación del conjunto de datos y la dirección de la red).
1b. En una red cerrada, todos los participantes son conocidos. No se necesitan medios de TI adicionales, pero la topología de la red (el número de participantes) estará fijado mediante precintado.
2. Es posible que haya retrasos imprevistos durante la transmisión. Para asignar correctamente un valor de medida recibido a una medición determinada, se debe registrar el momento de la medición.
3. Para garantizar la autenticidad, no se requiere necesariamente el cifrado de los datos de medida.</td></tr>
<tr><td colspan="2">Documentación requerida:
Red de participantes desconocidos: Descripción de los medios de TI para asignar correctamente el valor de medida a la medición.
Red cerrada: Descripción de los medios hardware que preservan el número de participantes de la red. Descripción de la identificación inicial de los participantes.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
Se describirán las medidas de protección tomadas.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se comprobará que existe un vínculo correcto entre cada valor de medida y la medición correspondiente.
• Se comprobará que los datos están firmados digitalmente para garantizar su correcta identificación y autenticación.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
• Cada conjunto de datos tiene un único número de identificación (actual), que puede contener el momento en que se ha realizado la medición (registro de fecha y hora).
• Cada conjunto de datos contiene información acerca del origen de los datos de medida, es decir, el número de serie o la identidad del instrumento de medida que generó el valor.
• En una red de participantes desconocidos, se garantiza la autenticidad si el conjunto de datos contiene una firma que no sea ambigua. La firma cubre todos estos campos del conjunto de datos.
• El receptor del conjunto de datos comprueba la fiabilidad de todos los datos.</td></tr>
</table>

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del dispositivo de envío y recepción.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* Se comprobará que las medidas tomadas para garantizar la autenticidad de los datos transmitidos son adecuadas.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">T5: Confidencialidad de las claves
Las claves y los datos que las acompañan deben tratarse como datos legalmente relevantes y mantenerse ocultos y protegidos frente a posibles riesgos originados por herramientas software.</td></tr>
<tr><td colspan="2">Especificaciones:
1. Este requisito solo se aplica si hay una clave secreta en el sistema (normalmente no en redes cerradas).
2. La protección se debe aplicar frente a cambios intencionados realizados mediante herramientas comunes de software.
3. Si el acceso a las claves secretas está restringido, p. ej., mediante el precintado de la carcasa de un dispositivo desarrollado específicamente, no se necesitará ningún medio de protección software adicional.</td><td>Especificaciones:
1. Este requisito solo se aplica si hay una clave secreta en el sistema (normalmente no en redes cerradas).
2. La protección se debe aplicar frente a cambios intencionados realizados mediante herramientas sofisticadas de software.
3. Los valores de medida recibidos se leen del conjunto de datos y se comprueba su firma mediante la clave pública del instrumento de medida emisor (o del dispositivo que generó el conjunto de datos relevante). Con esta comprobación el receptor puede probar que el valor y la firma se corresponden.
4. Se deben utilizar métodos adecuados equivalentes a los del pago electrónico..</td></tr>
<tr><td colspan="2">Documentación requerida:
Descripción de la gestión de las claves y de los medios para mantener las claves y la información asociada en secreto.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
Se describirán las medidas de protección tomadas.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
Se comprobará que la información secreta no pueda verse comprometida.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si las medidas tomadas son adecuadas respecto a la tecnología actual para garantizar un nivel de protección alto.</td></tr>
<tr><td colspan="2">Ejemplo de solución aceptable:
La clave secreta y los datos que la acompañan están almacenados en formato binario en el código ejecutable del software legalmente relevante. Por tanto, no es obvia la dirección en la que se almacenan estos datos. El software del sistema no ofrece ninguna opción para editar o ver estos datos. Si el algoritmo CRC se utiliza como firma, el vector inicial o polinomio generador desempeña la función de clave.</td><td>Ejemplo de solución aceptable:
La clave secreta se almacena en una parte del hardware que pueda precintarse físicamente. El software no ofrece ninguna opción para ver o editar estos datos.
<u>Nota:</u> Una solución técnica con un PC estándar podría no ser suficiente para garantizar el alto nivel de protección si no existen medios hardware de protección adecuados para la clave y otros datos secretos (véase la guía básica para ordenador universal U6).
1) Infraestructura PKI: la clave pública del almacenamiento sometido a control legal ha sido certificada por una Autoridad certificadora.
2) Confianza directa: no es necesario implicar a una Autoridad certificadora si, por un acuerdo anterior, ambas partes son capaces de leer la clave pública del instrumento de medida directamente en un dispositivo sometido a control legal que muestra el conjunto de datos relevantes.</td></tr>
</table>

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente que realiza la gestión de las claves.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* Se comprobará que las medidas tomadas para la gestión de claves son adecuadas.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
T6: Tratamiento de datos corruptos *Si se detectan datos corruptos, estos no deben utilizarse.*		
Especificaciones: Aunque los protocolos de comunicación normalmente repiten una transmisión hasta que es correcta, es posible que se reciba algún conjunto de datos corrupto.		
Documentación requerida: Descripción de los mecanismos de detección de fallos de transmisión o de cambios intencionados.		**Documentación requerida** (además de la documentación requerida para las clases de riesgo B y C): Se deben describir las medidas tomadas para el correcto tratamiento de los datos corruptos.
Guía de validación: *Comprobaciones basadas en la documentación y comprobaciones funcionales:* Se comprobará que los datos corruptos no se utilizan para el fin previsto.		**Guía de validación** (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en la documentación:* Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.
Ejemplo de solución aceptable: Cuando el programa que recibe los conjuntos de datos detecta una discrepancia entre el conjunto de datos y el valor de referencia de la firma, primero intenta reconstruir el valor original si hay información redundante disponible. Si falla la reconstrucción, genera una advertencia para el usuario, no proporciona el valor de medición y: • Activa una bandera en un campo especial del conjunto de datos (campo de estado) con el significado «no válido», o • Elimina el conjunto de datos corrupto.		

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del dispositivo receptor.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* Se comprobará que las medidas tomadas para el tratamiento de los datos corruptos son adecuadas.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
T7: Retraso en la transmisión *Los retrasos en la transmisión no influirán de modo inadmisible en la medición.*		
Especificaciones: El fabricante investigará la duración de la transmisión de los datos y garantizará que, en el peor de los casos, la medición no se vea influida de modo inadmisible.		
Documentación requerida: Descripción de cómo se protege la medición frente a un retraso en la transmisión.		
Guía de validación: Se comprobará que un retraso en la transmisión no influye en la medición.		
Ejemplo de solución aceptable: Implementación de los protocolos de transmisión para los buses de campo.		

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B, C y D): El código fuente que realiza la transmisión de los datos.
Guía de validación (además de la guía para las clases de riesgo B, C y D): *Comprobaciones basadas en el código fuente:* Se comprobará que las medidas tomadas para el tratamiento de las demoras en las transmisiones son adecuadas.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
T8: Disponibilidad de los servicios de transmisión *Si los servicios de red dejan de estar disponibles, no se debe perder ningún dato de medida.*		
Especificaciones: 1. El usuario del sistema de medida no podrá corromper los datos de medida interrumpiendo la transmisión. 2. Las perturbaciones de la transmisión se producen accidentalmente y no se pueden excluir. El dispositivo de envío debe ser capaz de manejar esta situación. 3. Si los servicios de transmisión dejan de estar disponibles, la reacción del instrumento dependerá del principio de medida (véase la extensión I).		
Documentación requerida: Descripción de las medidas de protección frente a la interrupción de la transmisión u otros fallos.		
Guía de validación: *Comprobaciones basadas en la documentación:* • Se comprobará qué medidas se han implementado para la protección frente a las pérdidas de datos. • Se comprobará cuáles son las medidas previstas en caso de fallos de transmisión. *Comprobaciones funcionales:* Las comprobaciones aleatorias deben mostrar que no se pierde ningún dato relevante por causa de una interrupción de la transmisión.		
Ejemplo de solución aceptable: 1) Para mediciones que se pueden interrumpir, que se pueden detener de manera rápida y sencilla (p. ej., pesaje, medición de combustible, etc.), la medición se puede completar incluso si falla la transmisión. Sin embargo, el instrumento de medida o dispositivo que esté transmitiendo los datos legalmente relevantes deberá contar con un *buffer* que tenga la capacidad suficiente para almacenar la transacción en curso. Después de esto, no se podrá iniciar ninguna otra transacción y los datos almacenados en el *buffer* se guardarán para que puedan transmitirse más adelante. Para consultar otros ejemplos véase la extensión I. 2) Las mediciones que no se pueden interrumpir (p. ej., las mediciones de energía, volumen, etc.) no necesitarán un *buffer* especial intermedio porque estas mediciones siempre son acumulativas. El registro acumulativo podrá leerse y transmitirse más tarde, cuando se restablezca la conexión.		

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B, C y D): El código fuente que realiza la transmisión de los datos.
Guía de validación (además de la guía para las clases de riesgo B, C y D): *Comprobaciones basadas en el código fuente:* Se comprobará que son adecuadas las medidas tomadas para reactivar un servicio de transmisión interrumpido.

8 Extensión S: Separación de software

La separación de software es una metodología de diseño opcional que permite al fabricante modificar fácilmente el software legalmente no relevante. Si se implementa la separación de software, se considerará esta extensión además de los requisitos básicos de los tipos P y U.

8.1 Descripción técnica

En general, los instrumentos de medida o sistemas controlados por software disponen de una funcionalidad compleja y contienen módulos legalmente relevantes y módulos que no lo son. Es una ventaja para el fabricante y para el examinador —aunque no es obligatorio— separar estos módulos de software del sistema de medida.
En la siguiente tabla se describen dos variantes de separación de software (las series de requisitos contemplan ambas opciones).

Descripción
La separación de software se implementa independientemente del sistema operativo dentro de un dominio de aplicación; es decir, a nivel de lenguaje de programación (***separación de software de bajo nivel***). *Nota*: Esta característica se aplica tanto a los dispositivos de medida diseñados específicamente como a los ordenadores universales.
Los módulos de software que se van a separar se implementan como objetos independientes a nivel de sistema operativo (***separación de software de alto nivel***). *Nota*: Este tipo de separación normalmente solo es posible con ordenadores universales. Son ejemplos de solución programas ejecutables de forma independiente, bibliotecas dinámicas, etc.

Tabla 8-1: Descripción técnica de la separación de software.

La protección frente a cambios inadmisibles de los valores y parámetros de medida se aborda solo de forma indirecta, ya que el programador de los componentes de software que no estén sometidos a control legal no debe proporcionar al usuario del sistema de medida la posibilidad de corromperlo. Sin embargo, el programador debe considerar la protección en cualquier caso (con o sin separación) y los requisitos adecuados proporcionados en las configuraciones básicas P y U (capítulos 4 y 5) de la guía.

8.2 Requisitos específicos para separación de software

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
S1: Realización de la separación de software *Habrá una parte del software que contenga todo el software y los parámetros legalmente relevantes que estará claramente separada de las demás partes del software.*		
Especificaciones: 1. En caso de *separación de bajo nivel*, todas las *unidades de programa* (subrutinas, procedimientos, funciones, clases, etc.) y, en caso de *separación de alto nivel*, pertenecen al software legalmente relevante[1] todos los *programas* y *bibliotecas:* • que contribuyan al cálculo de los valores de medida o que afecten a este; • que contribuyan a funciones auxiliares, tales como la visualización de datos, seguridad de datos, almacenamiento de datos, identificación de software, descarga de software, transmisión o almacenamiento de datos, verificación de datos recibidos o almacenados, etc. 2. Todas las *variables*, *parámetros* y *archivos temporales* que afecten a los valores de medición o a las funciones o datos legalmente relevantes pertenecen al software legalmente relevante. 3. Los componentes de la interfaz de software protectora (véase S3) forman parte del software legalmente relevante. 4. El software que legalmente no es relevante incluye las unidades de programa, datos o parámetros restantes que no están incluidos en los puntos anteriores. Se pueden realizar modificaciones en esta parte sin necesidad de informar de ello al organismo notificado siempre que se tengan en cuenta los siguientes requisitos para la separación de software.		
Documentación requerida: Descripción de todos los componentes mencionados en las especificaciones anteriores que pertenezcan al software legalmente relevante.		**Documentación requerida** (además de la documentación requerida para las clases de riesgo B y C): La documentación describirá la correcta implementación de la separación de software.
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará que todos los componentes legalmente relevantes mencionados en las especificaciones 1–3 se incluyen en el software legalmente relevante.		**Guía de validación** (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en la documentación:* Se comprobará si la separación de software se ha realizado correctamente.
Ejemplo de solución aceptable: Como se describe en el propio requisito.		

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del software legalmente relevante.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará el diseño del software para ver si el flujo de datos relativo a la información legalmente relevante está definido inequívocamente en el software legalmente relevante y puede verificarse. • Se comprobará (p. ej., analizando el flujo de datos con herramientas o de forma manual) que todas las unidades de programa, bibliotecas y programas involucrados en el procesamiento de los valores de medida están registrados en el software legalmente relevante. • Se realizarán búsquedas de flujos de datos inadmisibles desde las partes no sujetas a control legal hasta los dominios que deban protegerse.

[1] Nota:
Separación de bajo nivel : La combinación de componentes a nivel del lenguaje de programación o la combinación de partes de un programa (es decir, subrutinas, procedimientos, funciones, clases) para formar la parte legalmente relevante del programa. El resto del programa es la parte legalmente no relevante.
Separación de alto nivel: Combinación de todas las partes del software en un objeto que es identificable por el sistema operativo (un programa, una DLL, etc.). El resto del programa es la parte legalmente no relevante.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">S2: Indicación mixta
La información adicional generada por el software, que no es legalmente relevante, solo podrá mostrarse en pantalla o impresa, en caso de que no haya posibilidad de confusión con la información originada en la parte legalmente relevante.</td></tr>
<tr><td colspan="3">Especificaciones:
Ya que es posible que el programador del software legalmente no relevante desconozca si son admisibles las indicaciones, es responsabilidad del fabricante garantizar que toda la información indicada cumpla el requisito.</td></tr>
<tr><td colspan="2">Documentación requerida:
Descripción del software que realiza la indicación.
Descripción de cómo se protege la indicación de información legalmente relevante contra indicaciones engañosas generadas por el software legalmente no relevante.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
La documentación describirá como se realiza la indicación mixta.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones funcionales:
Se comprobará de forma visual que no haya posibilidad alguna de que la información adicional generada por el software legalmente no relevante y presentada en pantalla o impresa se confunda con la información originada por el software legalmente relevante.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si la indicación mixta se ha implementado correctamente.</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
• La información que va a mostrar el software legalmente no relevante se transfiere a través de la interfaz protectora (véase S3) al software legalmente relevante. En la interfaz pasa a través de un filtro que detecta la información inadmisible. A continuación, la información admisible se inserta en la indicación controlada por el software legalmente relevante.
• En una pantalla con ventanas (ordenador universal) el software legalmente relevante comprueba a intervalos breves si la ventana con la información legalmente relevante está siempre visible y en la parte superior del grupo de ventanas. Si está oculta, minimizada o fuera del borde, el software genera una advertencia o detiene la salida y procesamiento de los valores de medida. Puede cerrarse la ventana con información legalmente relevante cuando termina la medición.</td></tr>
</table>

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del software legalmente relevante.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará que el software legalmente relevante genera la indicación de los valores de medida. • Se comprobará que los programas legalmente no relevantes no pueden cambiar o suprimir esta indicación.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">S3: Interfaz de software protectora
El intercambio de datos entre el software legalmente relevante y el software que no lo sea debe realizarse mediante una interfaz de software protectora, que incluya las interacciones y el flujo de datos.</td></tr>
<tr><td colspan="3">Especificaciones:
1. Ninguna interacción ni flujo de datos debe influir de forma inadmisible en el software legalmente relevante incluyendo el comportamiento dinámico del proceso de medición.
2. Existirá una asignación inequívoca de cada comando enviado mediante la interfaz software a una función o modificación de datos iniciado en el software legalmente relevante.
3. Los códigos y datos que no estén declarados y documentados como comandos no deben tener efecto sobre el software legalmente relevante.
4. La interfaz estará completamente documentada y ni el programador del software legalmente relevante ni los programadores del software que no lo sea implementarán ningún otro flujo de datos o interacción que no estén documentados (elusión de la interfaz).
<u>Nota</u>: Los programadores son responsables del cumplimiento de estas restricciones. No es posible aplicar medios técnicos que les impidan eludir la interfaz software. Se debería instruir al programador de la interfaz protectora sobre este requisito.</td></tr>
<tr><td colspan="2">Documentación requerida:
• Descripción de la interfaz software, especialmente qué dominios de datos implementa la interfaz.
• Una lista completa de todos los comandos junto con una declaración de que no hay comandos adicionales.
• Una breve descripción de su significado y su efecto sobre las funciones y datos del instrumento de medida.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
La documentación describirá la implementación de la interfaz software.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se comprobará que se han definido y descrito las funciones del software legalmente relevante que pueden activarse a través de la interfaz protectora.
• Se comprobará que se han definido y descrito los parámetros que pueden intercambiarse a través de la interfaz.
• Se comprobará que la descripción de las funciones y de los parámetros es concluyente y completa.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si la interfaz de software se ha implementado correctamente.</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
• Los dominios de datos de la parte de software legalmente relevante se encapsulan declarando únicamente variables locales en la parte legalmente relevante.
• La interfaz se implementa como una subrutina perteneciente al software legalmente relevante que se llama desde el software legalmente no relevante. Los datos se transfieren al software legalmente relevante como parámetros de la subrutina.
• El software legalmente relevante filtra los comandos inadmisibles de la interfaz.</td></tr>
</table>

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente del software legalmente relevante.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará el diseño del software para ver si el flujo de datos está definido de modo inequívoco en el software legalmente relevante y puede verificarse. • Se comprobará el flujo de datos a través de la interfaz de software con herramientas o de forma manual. Se comprobará si se ha documentado todo el flujo de datos entre las partes (no se elude la interfaz de software declarada). • Se realizarán búsquedas de flujos de datos inadmisibles desde las partes no sujetas a control legal hasta los dominios que deban protegerse. • Se comprobará que los comandos, si existen, se decodifican correctamente y que no existen comandos no documentados.

9 Extensión D: Descarga de software legalmente relevante

Esta extensión es de aplicación a la descarga de software legalmente relevante mientras las características metrológicas permanezcan inalteradas y la declaración de la conformidad sea válida; p. ej., correcciones de fallos. Además de estos requisitos se considerarán los requisitos básicos de los tipos P y U que se describen en los capítulos 4 y 5 de la guía.

9.1 Descripción técnica

El software solo puede descargarse a instrumentos de medida con las siguientes propiedades:

Configuración hardware El dispositivo de destino está sometido a control legal. Puede ser un instrumento de medida desarrollado específicamente (tipo P) o uno basado en un ordenador universal (tipo U). Las conexiones de comunicación para la descarga pueden ser directas p. ej., RS232, USB, a través de una red cerrada parcial o totalmente bajo control legal p. ej., Ethernet, red de área local tipo *token ring* o a través de una red abierta p. ej., Internet.
Configuración software El software del dispositivo de destino puede estar completamente bajo control legal o puede existir separación de software. La descarga del software legalmente relevante debe cumplir los requisitos que se indican a continuación. Si no hay separación de software en el instrumento de medida, todos los requisitos siguientes serán de aplicación para todas las descargas.

Tabla 9-1: Descripción técnica de las configuraciones para la descarga de software.

9.2 Requisitos específicos del software

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">D1: Mecanismo de descarga
La descarga y la instalación posterior del software será automática y garantizará que al finalizar el proceso el entorno de protección del software se encuentre en el nivel aprobado.</td></tr>
<tr><td colspan="3">Especificaciones:
1. La descarga será automática para garantizar que el nivel de protección existente no se ve comprometido.
2. El dispositivo de destino tiene un software legalmente relevante fijo que contiene todas las funciones de comprobación necesarias para cumplir los requisitos D2–D4.
3. El instrumento debería ser capaz de detectar si la descarga o la instalación fallan. Se mostrará una advertencia. Si la descarga o instalación falla o se interrumpe, el estado original del instrumento de medida no se verá afectado. De modo alternativo, el instrumento mostrará un mensaje de error permanente y su funcionamiento metrológico se inhibirá hasta que se corrija la causa del error.
4. Tras finalizar la instalación correctamente, se deberían restaurar todos los medios de protección a su estado original a menos que el software descargado tenga autorización del organismo notificado en el certificado de examen de modelo para corregirlos.
5. Durante la descarga y la instalación posterior del software descargado, se inhibirá la función de medición del instrumento o se garantizará la medición correcta.
6. Si se producen fallos durante la descarga deben implementarse los requisitos de control de fallos descritos en la extensión I. El número de intentos de reinstalación será limitado.
7. Si no pueden cumplirse los requisitos D2–D4, aún podrá descargarse la parte del software que no sea legalmente relevante. En este caso, deberán cumplirse los requisitos siguientes:
- Existe una separación clara entre el software legalmente relevante y el software que no lo es, según la extensión S.
- Toda la parte del software legalmente relevante es fija, es decir, no puede descargarse ni modificarse sin romper ninguna protección.
- En el certificado de examen de modelo, se establece que se acepta la descarga de la parte legalmente no relevante.</td></tr>
<tr><td colspan="2">Documentación requerida:
La documentación debería describir brevemente la naturaleza automática de la descarga, la comprobación y la instalación, cómo se garantiza el nivel de protección al finalizar el proceso y qué sucede si se produce un fallo.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
La documentación describirá la implementación del mecanismo de descarga.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación:
• Se comprobará la documentación para ver cómo se gestiona el procedimiento de descarga.
• Se comprobará que la descarga e instalación se controlan automáticamente, que el instrumento de medida está bloqueado (si procede) y que la protección del software no se ve comprometida tras una descarga.
• Se comprobará que existe un software legalmente relevante fijo que no se puede descargar para comprobaciones de autenticidad e integridad.
• Se comprobará que durante la descarga de software no es posible realizar ninguna medición ó se garantiza que las que se realicen sean correctas.
Comprobaciones funcionales:
Se realizará, al menos, una descarga de software para comprobar que esta función se realiza correctamente.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si la implementación del mecanismo de descarga es correcta.</td></tr>
</table>

Ejemplo de solución aceptable:
Un programa de utilidad residente en la parte fija del software que:

- **a.** Negocia con el remitente (*handshake*) y comprueba la existencia de permisos.
- **b.** Inhibe automáticamente la medición a menos que se pueda garantizar una medición correcta.
- **c.** Descarga automáticamente el software legalmente relevante a un área de almacenamiento segura.
- **d.** Realiza automáticamente las comprobaciones requeridas en D2–D4.
- **e.** Instala automáticamente el software en la ubicación correcta.
- **f.** Se ocupa de la gestión interna; p. ej., eliminación de archivos redundantes, etc.
- **g.** Garantiza que cualquier protección eliminada para facilitar la descarga e instalación se repone automáticamente al nivel aprobado al finalizar el proceso.
- **h.** Inicia los procedimientos adecuados de control de fallos si se produce uno.

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente de la parte de software fija responsable de la gestión del proceso de descarga.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* Se comprobará si las medidas tomadas para gestionar el proceso de descarga son adecuadas.

<table>
<tr><th>Clase de riesgo B</th><th>Clase de riesgo C</th><th>Clase de riesgo D</th></tr>
<tr><td colspan="3">D2: Autenticación del software descargado
Se emplearán medios para garantizar que el software descargado es auténtico, y para indicar que ha sido aprobado por un organismo notificado.</td></tr>
<tr><td colspan="3">Especificaciones:
1. Antes de que el software descargado se utilice por primera vez, el instrumento de medida comprobará automáticamente que:
a. El software es auténtico (no una simulación fraudulenta);
b. El software está aprobado para ese modelo de instrumento de medida.
2. Los medios por los que el software identifica su condición de aprobado por el organismo notificado serán seguros para evitar la falsificación.
3. Si el software descargado no cumple alguna de las comprobaciones anteriores, véase D1.
4. Si el fabricante tiene intención de cambiar o actualizar el software legalmente relevante deberá comunicar los cambios al organismo notificado responsable. El organismo notificado decide si es o no necesario una adicional al certificado de examen de modelo. Para la descarga del software es indispensable que exista una identificación del software asignada de forma inequívoca a la versión aprobada del software.</td></tr>
<tr><td colspan="2">Documentación requerida:
La documentación debería describir:
• Cómo se garantiza la autenticidad de la identificación del software.
• Cómo se garantiza la autenticidad de la aprobación del organismo notificado.
• Cómo se garantiza que el software descargado está aprobado para el modelo de instrumento de medida para el que ha sido descargado.</td><td>Documentación requerida (además de la documentación requerida para las clases de riesgo B y C):
La documentación describirá la implementación de la autenticación.</td></tr>
<tr><td colspan="2">Guía de validación:
Comprobaciones basadas en la documentación y comprobaciones funcionales:
• Se comprobará en la documentación cómo se evitan las descargas de software fraudulento.
• Se comprobará, a través de comprobaciones funcionales, que se evitan las descargas de software fraudulento.
• Se asegurará la comprobación de autenticidad del software según la documentación y a través de comprobaciones funcionales.</td><td>Guía de validación (además de la guía para las clases de riesgo B y C):
Comprobaciones basadas en la documentación:
Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.</td></tr>
<tr><td colspan="3">Ejemplo de solución aceptable:
1. Autenticidad: por razones de integridad (véase D3), se genera una firma electrónica sobre la parte del software que se va a descargar. La autenticidad se garantiza si una clave almacenada en la parte fija del software del instrumento confirma que la firma procede del fabricante. La correspondencia de las claves se realizará automáticamente.
2. Organismo notificado: la clave se almacena en la parte fija del software antes de la verificación inicial.
3. Modelo correcto del instrumento de medida: la comprobación del modelo de instrumento requiere la correspondencia automática de una identificación del modelo de instrumento que se almacena en la parte fija del software del mismo con una lista de compatibilidad asociada al software.</td></tr>
</table>

4. **Aprobación por el organismo notificado** Si se garantiza la autenticidad mediante el uso de la clave del fabricante, puede asumirse la aprobación por el organismo notificado.	4. **Aprobación por el organismo notificado** Para comprobar que ese software ha sido aprobado realmente, una posibilidad es que todo el software aprobado que se haya descargado contenga la firma de la autoridad responsable. La clave pública de la autoridad responsable se almacena en el instrumento de medida y se utiliza para comprobar automáticamente la firma asociada al software. Esta se puede visualizar en el instrumento para compararla con la clave publicada por la autoridad responsable.

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente de la parte de software fija responsable de la comprobación de la autenticidad del software descargado.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* Se comprobará si las medidas tomadas para la comprobación de la autenticidad son adecuadas.

Clase de riesgo B	**Clase de riesgo C**	**Clase de riesgo D**
D3: Integridad del software descargado *Se emplearán medios para garantizar que durante la descarga el software descargado no haya sido modificado de forma inadmisible.*		
Especificaciones: 1. Antes de utilizar por primera vez el software descargado, el instrumento de medida comprobará automáticamente que dicho software no se haya modificado de forma inadmisible. 2. Si el software descargado no supera esta comprobación, véase D1.		
Documentación requerida: La documentación describirá cómo se garantiza la integridad del software.		**Documentación requerida** (además de la documentación requerida para las clases de riesgo B y C): La documentación describirá las medidas que garantizan la integridad.
Guía de validación: Se garantizará la comprobación de la integridad del software después de la descarga según la documentación y a través de comprobaciones funcionales.		**Guía de validación** (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en la documentación:* Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.
• Ejemplo de solución aceptable: • La integridad puede demostrarse realizando una suma de comprobación del software legalmente relevante y comparándola con la suma de comprobación asociada al software (véase también U2 para un ejemplo de solución aceptable). • Algoritmo aceptable: CRC, vector inicial secreto, 32 bits de longitud. El vector inicial se almacena en la parte de software fija.		• Ejemplo de solución aceptable: • Generar un valor hash del software a descargar (p. ej.: algoritmos SHA-1, Ripe MD 160) y cifrarlo (RSA, curvas elípticas) con una longitud de clave adecuada. • La clave para descifrar se almacena en la parte de software fija. •

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): El código fuente de la parte de software fija responsable de la comprobación de la integridad del software descargado.
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* Se comprobará si son adecuadas las medidas tomadas para la comprobación de la integridad.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
D4: Trazabilidad de la descarga del software legalmente relevante *Se garantizará mediante los medios técnicos adecuados que las descargas del software legalmente relevante puedan rastrearse dentro del instrumento para realizar controles posteriores.*		
Especificaciones: 1. Este requisito permite que las autoridades de inspección, responsables de la supervisión metrológica de los instrumentos sometidos a control metrológico, rastreen las descargas del software legalmente relevante durante un período de tiempo adecuado (que dependerá de la legislación nacional). 2. Los medios y registros de trazabilidad forman parte del software legalmente relevante y deberían protegerse como tales.		
Documentación requerida: La documentación deberá: • Describir brevemente cómo se implementan y protegen los medios para la trazabilidad. • Establecer cómo puede rastrearse el software descargado.		**Documentación requerida** (además de la documentación requerida para las clases de riesgo B y C): La documentación describirá las medidas que garantizan la trazabilidad.
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará que se implementan y protegen los medios para la trazabilidad. *Comprobaciones funcionales:* Se comprobará la funcionalidad de los medios a través de comprobaciones aleatorias.		**Guía de validación** (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en la documentación:* Se comprobará si las medidas tomadas son adecuadas con respecto a la tecnología actual para garantizar un nivel de protección alto.
Ejemplo de solución aceptable: • Registro de actividades. El instrumento de medida puede estar equipado con un registro de sucesos que registra automáticamente al menos la fecha y la hora de la descarga, la identificación del software legalmente relevante que se ha descargado, la identificación de la parte descargada, y una anotación del éxito de la operación. Se genera una entrada por cada intento de descarga, independientemente de si ha tenido éxito. • Después de haber alcanzado el límite del registro de sucesos, se garantizará por medios técnicos que no es posible realizar más descargas. Los registros de sucesos solo se podrán borrar rompiendo un precinto físico o electrónico y solo podrán volver a precintarlos las autoridades de inspección.		

Consideraciones adicionales para la clase de riesgo E
Documentación requerida (además de la documentación requerida para las clases de riesgo B y C): *El código fuente de la parte fija del software responsable de rastrear los procesos de descarga y de gestionar el registro de sucesos.*
Guía de validación (además de la guía para las clases de riesgo B y C): *Comprobaciones basadas en el código fuente:* • Se comprobará si las medidas tomadas para rastrear los procesos de descarga son adecuadas. • Se comprobará si las medidas tomadas para proteger el registro de sucesos son adecuadas.

Consentimiento para la descarga

Se asume que el fabricante del instrumento de medida mantiene a su cliente bien informado sobre las actualizaciones del software, en especial sobre la parte legalmente relevante, y que el cliente no se negará a su actualización. Además se asume que el fabricante y el cliente, usuario o propietario del instrumento acordarán un procedimiento adecuado para la realización de la descarga en función del uso y ubicación del instrumento.

10 Extensión I: Requisitos del software específicos del instrumento.

Esta extensión complementa los requisitos generales del software de los capítulos anteriores y no puede considerarse de forma independiente de las partes P o U ni de otras extensiones (véase el capítulo 3). Refleja la existencia de anexos de la MID específicos para cada instrumento (MI-x) y contiene aspectos y requisitos específicos de los instrumentos o sistemas de medida (o subconjuntos). Sin embargo, estos requisitos no van más allá de los requisitos de la MID. Sólo se hace referencia a las recomendaciones de la OIML o a las normas ISO/IEC, cuando estas pueden considerarse documentos normativos en el sentido de la MID, y si respaldan una interpretación armonizada de los requisitos de esta Directiva.

Además de los aspectos y requisitos del software específicos del instrumento, la extensión I contiene la asignación específica de clases de riesgos para el instrumento (o categoría) que garantiza un nivel armonizado de examen, protección y conformidad del software.

Por ahora, la extensión I está pensada como un borrador inicial a completar por el respectivo grupo de trabajo de WELMEC con los conocimientos específicos correspondientes. Por lo tanto, la extensión I tiene una "estructura abierta", es decir, que proporciona un esqueleto que —además de la asignación inicial de las clases de riesgo— está cumplimentado solo parcialmente (p. ej., para los contadores de servicio público e instrumentos de pesaje de funcionamiento automático). También puede utilizarse para otros instrumentos (incluidos o no en la MID), según las experiencias adquiridas y las decisiones tomadas por los grupos de trabajo WELMEC responsables. La numeración x de los subapartados 10.x se corresponde con la numeración de los anexos específicos de la MID. Los instrumentos no incluidos en la MID podrían añadirse comenzando en el 10.11.

Para un determinado tipo x de instrumento de medida, pueden existir diferentes aspectos del software específicos a tener en cuenta. Estos aspectos deberían tratarse de un modo sistemático como se indica a continuación: cada subapartado 10.x debería dividirse en secciones 10.x.y, donde «y» trata los siguientes aspectos:

10.x.1 Reglamentos específicos, normas y otros documentos normativos

Aquí deben mencionarse los reglamentos específicos de instrumentos (o categorías), las normas y demás documentos normativos (p. ej., las recomendaciones de la OIML) o las guías WELMEC que pueden ayudar a desarrollar los requisitos del software específicos del instrumento (o categoría) como una interpretación de los requisitos del anexo I y de los anexos específicos MI-x de la MID.
Normalmente, los requisitos del software específicos del instrumento se aplican junto con los requisitos generales de los capítulos anteriores. De otro modo, se debería exponer claramente si un requisito del software específico sustituye a uno (o a varios) de los requisitos generales del software o si uno (o varios) de los requisitos generales del software no es (son) aplicable(s) y el motivo.

10.x.2 Descripción técnica

Aquí pueden proporcionarse:

- ejemplos de las configuraciones técnicas específicas más comunes,
- la aplicación de las partes P, U y extensiones para estos ejemplos y
- listas de comprobación (específicas de los instrumentos) útiles para el fabricante y el examinador.

La descripción debería incluir:

- el principio de medida (medición acumulativa o independiente, medición repetible o no repetible y medición estática o dinámica) y
- detección de fallos y la reacción ante ellos. Existen dos casos posibles:

  a) que la presencia de un error sea obvia o que pueda comprobarse de forma sencilla o existan medios hardware para detectar el fallo,
  b) que no resulte obvia la presencia de un error y no pueda comprobarse fácilmente y no haya medios hardware para la detectar el fallo.

  En el último caso (b), la detección de fallos y la reacción ante estos requiere medios de software adecuados y, por tanto, requisitos de software adecuados

- la configuración hardware; al menos, deberían incluirse los siguientes aspectos:

  a) ¿Se trata de un sistema modular basado en un ordenador de propósito general o se trata de un instrumento dedicado con un sistema integrado sometido a control legal?
  b) ¿El sistema informático es autónomo o forma parte de una red cerrada (p. ej., Ethernet, LAN *token ring*), o forma parte de una red abierta (p. ej., Internet)?
  c) ¿La unidad del sensor (módulo de medida) está separado (ubicación y suministro de energía separados) del sistema de tipo U o está integrado en él completa o parcialmente?
  d) ¿La interfaz de usuario se encuentra siempre sometida a control legal (tanto para los instrumentos de tipo P y U) o puede cambiarse a un modo operativo que no esté sometido a control legal?
  e) ¿Se prevé el almacenamiento de datos a largo plazo? Si es así, ¿entonces el almacenamiento es local (p. ej., disco duro) o remoto (p. ej., servidor de ficheros)?
  f) ¿El medio de almacenamiento es fijo (p. ej., ROM interna) o extraíble (p. ej., disquete, CD-RW, tarjeta inteligente o *memory stick*)?

- la configuración software y el entorno; al menos, deberían incluirse los siguientes aspectos:

  a) ¿Qué sistema operativo se utiliza o puede utilizarse?
  b) ¿Hay otras aplicaciones de software en el sistema además del software legalmente relevante?
  c) ¿Existe software que no esté sometido a control legal pensado para poder modificarse libremente tras la aprobación?

10.x.3 Requisitos del software específicos

Aquí deberían relacionarse y describirse, de un modo parecido al de los capítulos anteriores, los requisitos del software específicos.

10.x.4 Ejemplos de funciones y datos legalmente relevantes

Aquí pueden proporcionarse ejemplos de:

- parámetros específicos del dispositivo (p. ej., parámetros individuales de configuración y calibración de un instrumento de medida específico),
- parámetros específicos del modelo (p. ej., los parámetros específicos que se fijan en el examen de modelo) o
- funciones específicas legalmente relevantes.

10.x.5 Otros aspectos

Aquí pueden mencionarse otros aspectos como por ejemplo la documentación específica necesaria para el examen (software) del modelo, descripciones específicas e instrucciones que deben proporcionarse en los certificados de examen de modelo. También pueden mencionarse otros aspectos (p. ej., los requisitos relativos a la realización de ensayos).

10.x.6 Asignación de la clase de riesgo

Aquí debería definirse la clase de riesgo adecuada para los instrumentos de tipo x. Esto puede hacerse:

- de forma general (para todas las categorías del tipo respectivo) o
- según el campo de aplicación o categoría u otros aspectos, si existen.

10.1 Contadores de agua

10.1.1 Reglamentos específicos, normas y otros documentos normativos

Los Estados miembros pueden —según el artículo 2 de la MID— prescribir el uso de contadores de agua sometidos a la regulación de la MID en el uso residencial, comercial y de industria ligera.
Los requisitos específicos de este capítulo se basan exclusivamente en el anexo MI-001.
No se han tenido en cuenta las recomendaciones y normas de la OIML.

10.1.2 Descripción técnica

10.1.2.1 Configuración hardware

Los contadores de agua suelen construirse como dispositivos desarrollados específicamente (tipo P en esta guía).

10.1.2.2 Configuración software

Es específica de cada fabricante, pero normalmente debería esperarse que siguiera las recomendaciones proporcionadas en el cuerpo principal de esta guía.

10.1.2.3 Principio de medida

Los contadores de agua acumulan de forma continua el volumen consumido. El volumen acumulado se visualiza en el instrumento. Se emplean varios principios.

La medición de volumen es no repetible.

10.1.2.4 Detección de fallos y reacción ante ellos

El requisito MI-001, 7.1.2 trata las perturbaciones electromagnéticas. Es necesario interpretar este requisito para los instrumentos controlados por software porque solo se puede detectar una perturbación y recuperarse de la misma mediante acción combinada de determinadas partes del hardware y del software específico. Desde el punto de vista del software no importa cuál sea el motivo de una perturbación (electromagnético, eléctrico, mecánico, etc.): los procedimientos de recuperación son los mismos.

10.1.3 Requisitos de software específicos (contadores de agua)

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I1-1: Recuperación ante fallos *El software se recuperará de una perturbación y pasará al funcionamiento normal.*		
Especificaciones: Deberán activarse indicadores con la fecha para facilitar el registro de periodos de mal funcionamiento.		
Documentación requerida: Una breve descripción del mecanismo de recuperación ante fallos y cuándo se activa.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si la implementación de la recuperación ante fallos es adecuada. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: Una subrutina microprocesada reinicia periódicamente un "temporizador de control hardware" (hardware *watchdog*) evitando su disparo. Si alguna función no se ha procesado o – en el peor de los casos – el microprocesador se cuelga en un bucle infinito, este reinicio no tiene lugar y el temporizador de control se dispara al cabo del tiempo establecido.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I1-2: Funcionalidades para la generación de copias de seguridad *Existirá una funcionalidad que, en caso de que se produzca alguna perturbación, proporcione copias de seguridad periódicas de los datos legalmente relevantes como los valores de medición y el estado actual del proceso. Estos datos se guardarán en un almacenamiento no volátil.*		
Especificaciones: Los intervalos de almacenamiento deben ser suficientemente breves como para que la discrepancia entre los valores actuales y los acumulativos sea pequeña.		
Documentación requerida: Una breve descripción de sobre qué datos se ha realizado copia de seguridad y de cuándo se realizó dicha copia. Un cálculo del error máximo que puede producirse para los valores acumulativos.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará que todos los datos legalmente relevantes se guardan en un almacenamiento no volátil y que se pueden recuperar. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: Se realizan copias de seguridad de los datos legalmente relevantes según se requiera (p. ej., cada 60 minutos).		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I1-3: Anexo I, 8.5 de la MID (Evitar la puesta a cero de los valores de medida acumulativos) *En el caso de los instrumentos de medida de empresas de servicio público el indicador de la cantidad total suministrada o los indicadores de los que puede extraerse la cantidad total suministrada, que sirvan de referencia total o parcial para el pago, no podrán ponerse a cero durante su utilización.*		
Especificaciones: Los registros acumulativos de un instrumento de medida pueden ponerse a cero antes de su puesta en servicio.		
Documentación requerida: Documentación de los medios de protección frente a la puesta a cero de los registros de volumen.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará que los valores de medida legalmente relevantes y acumulativos no puedan ponerse a cero sin dejar rastro. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: Los registros de volumen están protegidos frente a los cambios y la puesta a cero del mismo modo que los parámetros (véase P7).		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I1-4: Comportamiento dinámico *El software legalmente no relevante no deberá influir de forma negativa en el comportamiento dinámico de un proceso de medida.*		
Especificaciones: • Este requisito se aplica junto con S-1, S-2 y S-3 si se ha realizado separación de software conforme a la extensión S. • Este requisito adicional garantiza que, para aplicaciones en tiempo real de los contadores, el comportamiento dinámico del software legalmente relevante no se ve influenciado de forma inadmisible por el software legalmente no relevante, es decir, que los recursos del software legalmente relevante no se vean reducidos por la parte no legal de forma inadmisible.		
Documentación requerida: • Descripción de la jerarquía de interrupción. • Diagrama de tiempos de las tareas de software. Límites del ejecutable proporcionado para tareas legalmente no relevantes.		
Guía de validación: *Comprobaciones basadas en la documentación:* La documentación de los límites del ejecutable proporcionado para tareas legalmente no relevantes estará disponible para el programador de la parte del software legalmente no relevante. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: La jerarquía de interrupción está diseñada de manera que impida influencias adversas.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I1-5: Identificación impresa del software *La identificación del software suele presentarse en un dispositivo indicador. Como excepción para los contadores de agua, será una solución aceptable una impresión que identifique el software en la placa de características del instrumento siempre que se cumplan las siguientes condiciones:* *A. La interfaz de usuario no tiene capacidad de control para activar la indicación de la identificación del software en el dispositivo indicador o este técnicamente no permite mostrar la identificación del software (contador mecánico).* *B. El instrumento no tiene ninguna interfaz para comunicar la identificación del software.* *C. No es posible cambiar el software del contador después de su fabricación o solo es posible si se cambia también el hardware o un componente hardware.*		
Especificaciones: • El fabricante del hardware o del componente hardware pertinente es responsable de que la identificación del software esté correctamente marcado en dicho hardware. • Se aplican todas las demás especificaciones de P2/U2.		
Documentación requerida: La misma que en P2/U2.		
Guía de validación: *Comprobaciones basadas en la documentación:* La misma que en P2/U2. *Comprobaciones funcionales:* La misma que en P2/U2.		
Ejemplo de solución aceptable: Una marca impresa en la placa de características del instrumento que identifique el software		

10.1.4 Ejemplos de parámetros legalmente relevantes

Los contadores de agua tienen parámetros, como constantes de cálculo, de configuración, etc., pero también tienen parámetros para el ajuste de la funcionalidad del dispositivo. Con respecto a la identificación y protección de los parámetros y el conjunto de parámetros, véanse los requisitos P2 y P7 de la guía P.

A continuación, se proporcionan algunos parámetros típicos de los contadores de agua . Esta tabla se actualizará cuando el grupo de trabajo 11 de WELMEC haya decido su contenido final.

Parámetro	Protegido	Configurable	Comentario
Factor de calibración	x		
Factor de linealidad	x		

10.1.5 Otros aspectos

En el caso de aplicaciones domésticas, se supone que la descarga de software (extensión D, capítulo 9) no será muy importante.
El registro de energía o volumen acumulados de instrumentos domésticos no es un almacenamiento a largo plazo en el sentido de la extensión L (capítulo 6). En el caso de instrumentos que solo midan energía/volumen acumulados, no es necesario aplicar la extensión L.

10.1.6 Asignación de la clase de riesgo

Hasta ahora, según las decisiones del grupo de trabajo responsable de WELMEC nº 11 (segunda reunión, 3-4 de marzo de 2005), se consideran adecuadas las siguientes clases de riesgo y deberían aplicarse si se llevan a cabo exámenes de software basados en la presente guía para los contadores de agua (controlados mediante software).

- Clase de riesgo C para instrumentos de tipo P

Sin embargo, no se ha tomado todavía ninguna decisión definitiva y el grupo de trabajo nº 11 reconsiderará este tema en relación con el debate sobre las clases de riesgo adecuadas para los instrumentos de tipo U.

10.2 Contadores de gas y dispositivos de conversión volumétrica

10.2.1 Reglamentos específicos, normas y otros documentos normativos

Los Estados miembros pueden —según el artículo 2 de la MID— prescribir el uso de los contadores de gas y dispositivos de conversión volumétrica sometidos a la regulación de la MID en el uso residencial, comercial y de industria ligera.

Los requisitos específicos de este capítulo se basan exclusivamente en el anexo MI-002.

No se han tenido en cuenta las recomendaciones y normas de la OIML.

10.2.2 Descripción técnica

10.2.2.1 Configuración hardware

Los contadores de gas y dispositivos de conversión volumétrica suelen construirse como dispositivos desarrollados específicamente (tipo P en esta guía). Pueden tener una o varias entradas para unidades de sensores externas y los contadores y dispositivos de conversión pueden ser unidades de hardware separadas.

10.2.2.2 Configuración de software

Es específica de cada fabricante, pero normalmente debería esperarse que siguiera las recomendaciones proporcionadas en el cuerpo principal de esta guía.

10.2.2.3 Principio de medida

Los contadores de gas acumulan continuamente el volumen consumido. El volumen acumulado se muestra en el instrumento. Se emplean varios principios. Se utiliza un dispositivo de conversión volumétrica para calcular el volumen en condiciones de base. El convertidor puede ser una parte integral del contador.

La medición de volumen no puede repetirse.

10.2.2.4 Detección de fallos y reacción ante ellos

El requisito MI-002, 4.3.1 trata las perturbaciones electromagnéticas. Es necesario interpretar este requisito para los instrumentos controlados por software porque solo se puede detectar una perturbación y recuperarse de la misma mediante acción combinada de determinadas partes del hardware y del software específico. Desde el punto de vista del software no importa cuál sea el motivo de una perturbación (electromagnético, eléctrico, mecánico, etc.): los procedimientos de recuperación son los mismos.

10.2.3 Requisitos de software específicos (contadores de gas y dispositivos de conversión volumétrica)

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I2-1: Recuperación ante fallos *El software se recuperará de una perturbación y pasará al funcionamiento normal.*		
Especificaciones: Deberán activarse indicadores con la fecha para facilitar el registro de periodos de mal funcionamiento.		
Documentación requerida: Una breve descripción del mecanismo de recuperación ante fallos y cuándo se activa.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si la implementación de la recuperación ante fallos es adecuada. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: Una subrutina microprocesada reinicia periódicamente un "temporizador de control hardware" (hardware *watchdog*) evitando su disparo. Si alguna función no se ha procesado o – en el peor de los casos – el microprocesador se cuelga en un bucle infinito, este reinicio no tiene lugar y el temporizador de control se dispara al cabo del tiempo establecido.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I2-2: Funcionalidades para la generación de copias de seguridad *Existirá una funcionalidad que, en caso de que se produzca alguna perturbación, proporcione copias de seguridad periódicas de los datos legalmente relevantes como los valores de medición y el estado actual del proceso. Estos datos se guardarán en un almacenamiento no volátil.*		
Especificaciones: Los intervalos de almacenamiento deben ser suficientemente breves como para que la discrepancia entre los valores actuales y los acumulativos sea pequeña.		
Documentación requerida: Una breve descripción de sobre qué datos se ha realizado copia de seguridad y de cuándo se realizó dicha copia. Un cálculo del error máximo que puede producirse para los valores acumulativos.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará que todos los datos legalmente relevantes se guardan en un almacenamiento no volátil y que se pueden recuperar. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: Se realizan copias de seguridad de los datos legalmente relevantes según se requiera (p. ej., cada 60 minutos).		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I2-3: MI-002, 5.2 (idoneidad de la indicación) El dispositivo indicador del volumen total sin corregir tendrá un número de dígitos suficiente para asegurar que, cuando el contador funcione durante 8 000 horas con $Q_{máx}$, la indicación no vuelva a su valor inicial.		
Especificaciones:		
Documentación requerida: Documentación de la representación interna del registro de volumen.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si la capacidad de almacenamiento es suficiente.		
Ejemplo de solución aceptable: Los valores típicos del contador de gas doméstico son: $Q_{máx} = 6\ m^3/h$. El rango necesario es de 48 000 m^3 (en la actualidad los contadores de gas electrónicos muestran hasta 99 999 m^3).		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I2-4: Anexo I, 8.5 de la MID (Evitar la puesta a cero de los valores de medida acumulativos) *En el caso de los instrumentos de medida de empresas de servicio público el indicador de la cantidad total suministrada o los indicadores de los que puede extraerse la cantidad total suministrada, que sirvan de referencia total o parcial para el pago, no podrán ponerse a cero durante su utilización.*		
Especificaciones: Los registros acumulativos de un instrumento de medida pueden ponerse a cero antes de su puesta en servicio.		
Documentación requerida: Documentación de los medios de protección frente a la puesta a cero de los registros de volumen.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará que los valores de medida legalmente relevantes y acumulativos no puedan ponerse a cero sin dejar rastro. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: Los registros de volumen están protegidos frente a los cambios y la puesta a cero, del mismo modo que los parámetros (véase P7).		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I2-5: MI-002, 5.2 (Vida útil de la fuente de alimentación) *Una fuente de alimentación dedicada deberá tener una vida útil de al menos cinco años. Deberá aparecer una adecuada advertencia una vez transcurrido el 90 % de su vida útil.*		
Especificaciones: Vida útil se utiliza aquí en el sentido de capacidad de energía disponible. Si la fuente de energía puede sustituirse "in situ", ni los parámetros ni los datos legalmente relevantes resultarán dañados durante el cambio.		
Documentación requerida: Documentación sobre la capacidad de la fuente de alimentación, vida útil (independiente del consumo de energía), medidas para determinar la energía consumida o disponible y descripción de los medios de advertencia de nivel bajo de energía disponible .		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si las medidas que se han tomado son adecuadas para vigilar la energía disponible.		
Ejemplo de solución aceptable: Se cuentan las horas operativas o los sucesos de reactivación del dispositivo, se almacenan en una memoria no volátil y se comparan con el valor nominal de vida útil de la batería. Si ha transcurrido el 90% de la vida útil, se mostrará la adecuada advertencia. El software detecta el intercambio de la fuente de alimentación y reinicia el contador. Otra solución sería monitorizar continuamente el nivel del suministro de energía.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I2-6: MI-002, 9.1 (Dispositivo de conversión electrónico) *Un dispositivo de conversión electrónico deberá poder detectar cuándo funciona fuera del rango de funcionamiento declarado por el fabricante para los parámetros que son relevantes en la exactitud de la medida. Si eso sucediera, el dispositivo de conversión deberá interrumpir la integración de la cantidad convertida y poder totalizar por separado la cantidad convertida durante el tiempo que se encuentre fuera del rango de funcionamiento.*		
Especificaciones: Deberá existir una indicación visual del estado de error.		
Documentación requerida: Documentación de los diferentes registros para la cantidad convertida y la cantidad durante el fallo.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si las medidas tomadas son adecuadas para la gestión de condiciones operativas inusuales.		
Ejemplo de solución aceptable: El software controla los valores de entrada relevantes y los compara con los límites predefinidos. Si todos los valores están dentro de los límites, la cantidad convertida se integrará en el registro normal (una variable dedicada). En caso contrario, totaliza la cantidad en otra variable. Otra solución sería disponer de un solo registro de acumulación, pero grabar la fecha y la hora de inicio y de fin, así como los valores de registro del periodo que esté fuera del intervalo en un *log* de sucesos (véase P7). Se pueden indicar ambas cantidades. El usuario puede identificar y distinguir claramente la indicación regular y la indicación durante el fallo, mediante una indicación del estado.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I2-7: MI-002, 5.5 (elemento de ensayo) *El contador de gas dispondrá de un elemento de ensayo que permitirá realizar pruebas en un plazo de tiempo razonable.*		
Especificaciones: El elemento de ensayo para acelerar los procedimientos de ensayo que consumen mucho tiempo se utiliza normalmente para realizar la comprobación antes de la instalación y el funcionamiento normal. Durante el modo de ensayo deberán utilizarse los mismos registros y partes del software que en el modo operativo estándar.		
Documentación requerida: Documentación del elemento de ensayo e instrucciones para activar el modo de ensayo.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si todos los procedimientos de ensayo del contador de gas que consumen mucho tiempo pueden realizarse mediante el elemento de ensayo.		
Ejemplo de solución aceptable: La base de tiempo del reloj interno puede acelerarse. Los procesos que duran, por ejemplo, una semana, un mes o incluso un año y desbordan los registros pueden comprobarse en el modo de prueba en minutos u horas.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I2-8: Comportamiento dinámico *El software legalmente no relevante no deberá influir de forma negativa en el comportamiento dinámico de un proceso de medida.*		
Especificaciones: • Este requisito se aplica junto con S-1, S-2 y S-3 si se ha realizado separación de software conforme a la extensión S. • Este requisito adicional garantiza que, para aplicaciones en tiempo real de los contadores, el comportamiento dinámico del software legalmente relevante no se ve influenciado de forma inadmisible por el software legalmente no relevante, es decir, que los recursos del software legalmente relevante no se vean reducidos por la parte no legal de forma inadmisible.		
Documentación requerida: • Descripción de la jerarquía de interrupción. • Diagrama de tiempos de las tareas de software. Límites del ejecutable proporcionado para tareas legalmente no relevantes.		
Guía de validación: *Comprobaciones basadas en la documentación:* La documentación de los límites del ejecutable proporcionado para tareas legalmente no relevantes estará disponible para el programador de la parte del software legalmente no relevante. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: La jerarquía de interrupción está diseñada de manera que impide influencias adversas.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I2-9: Identificación impresa del software *La identificación del software suele presentarse en un dispositivo indicador. Como excepción para los contadores de gas y dispositivos de conversión volumétrica, será una solución aceptable una impresión que identifique el software en la placa de características del instrumento siempre que se cumplan las siguientes condiciones:* *A. La interfaz de usuario no tiene capacidad de control para activar la indicación de la identificación del software en el dispositivo indicador o este técnicamente no permite mostrar la identificación del software (contador mecánico).* *B. El instrumento no tiene ninguna interfaz para comunicar la identificación del software.* *C. No es posible cambiar el software del contador después de su fabricación o solo es posible si se cambia también el hardware o un componente hardware.*		
Especificaciones: • El fabricante del hardware o del componente hardware pertinente es responsable de que la identificación del software esté correctamente marcado en dicho hardware. • Se aplican todas las demás especificaciones de P2/U2.		
Documentación requerida: La misma que en P2/U2.		
Guía de validación: *Comprobaciones basadas en la documentación:* La misma que en P2/U2. *Comprobaciones funcionales:* La misma que en P2/U2.		
Ejemplo de solución aceptable: Una marca impresa en la placa de características del instrumento que identifique el software.		

10.2.4 Ejemplos de parámetros legalmente relevantes

Los contadores de gas y los dispositivos de conversión volumétrica suelen tener muchos parámetros.

Se utilizan como constantes de cálculo, de configuración, etc., pero también para el ajuste de la funcionalidad del dispositivo. Con respecto a la identificación y protección de los parámetros y el conjunto de parámetros, véanse los requisitos P2 y P7 de la guía P.

A continuación se proporcionan algunos parámetros típicos de los contadores de gas y dispositivos de conversión volumétrica. Esta tabla se actualizará cuando el grupo de trabajo 11 de WELMEC haya decido su contenido final.

Parámetro	Protegido	Configurable	Comentario
Factor de calibración	x		
Factor de linealidad	x		

10.2.5 Otros aspectos

En el caso de aplicaciones domésticas, se supone que la descarga de software (extensión D, capítulo 9) no será muy importante.

El registro de energía o volumen acumulados de instrumentos domésticos no es un almacenamiento a largo plazo en el sentido de la extensión L (capítulo 6). En el caso de instrumentos que solo midan energía/volumen acumulados, no es necesario aplicar la extensión L.

10.2.6 Asignación de la clase de riesgo

Hasta ahora, según las decisiones del grupo de trabajo responsable de WELMEC nº 11 (segunda reunión, 3-4 de marzo de 2005), se consideran adecuadas las siguientes clases de riesgo y deberían aplicarse si se llevan a cabo exámenes de software basados en la presente guía para los contadores de gas y dispositivos de conversión volumétrica (controlados mediante software):

- **Clase de riesgo C para instrumentos de tipo P**

Sin embargo, no se ha tomado todavía ninguna decisión definitiva y el grupo de trabajo nº 11 reconsiderará este tema en relación con el debate sobre las clases de riesgo adecuadas para los instrumentos de tipo U.

El grupo de trabajo nº 11 considera que la funcionalidad de prepago y de medición en intervalos son adicionales a aquellas funciones de medición esenciales especificadas en el anexo MI-002 de la MID. Por lo tanto, a estas variantes no se les asigna una categoría de riesgos mayor que la asignada a los contadores de tipo básico contemplados en esta guía. Sin embargo, debería evaluarse la función de medición básica, como ocurre con todos los demás instrumentos de tipo P junto con cualquier otra evaluación que se considere necesaria para demostrar que el software asociado que proporciona estas funciones no tiene una influencia inadmisible sobre la medición básica.

10.3 Contadores de energía eléctrica activa

10.3.1 Reglamentos específicos, normas y otros documentos normativos

Los Estados miembros pueden —según el artículo 2 de la MID— prescribir el uso de los contadores de energía eléctrica activa sometidos a la regulación de la MID en el uso residencial, comercial y de industria ligera.

Los requisitos específicos de este capítulo se basan exclusivamente en el anexo MI-003.

No se han tenido en cuenta las recomendaciones y normas de la OIML ni las normas IEC.

10.3.2 Descripción técnica

Los contadores de energía eléctrica activa toman como entrada las medidas de tensión e intensidad de corriente, obtienen a partir el ellas la potencia eléctrica activa y la integran con respecto al tiempo para aportar la energía eléctrica activa.

10.3.2.1 Configuración hardware

Los contadores de energía eléctrica activa suelen construirse como dispositivos desarrollados específicamente (tipo P en esta guía). Pueden tener una o varias entradas y pueden combinarse con transformadores externos.

10.3.2.2 Configuración software

Es específica de cada fabricante, pero normalmente debería esperarse que siguiera las recomendaciones proporcionadas en el cuerpo principal de esta guía.

10.3.2.3 Principio de medida

Los contadores de energía eléctrica activa acumulan continuamente la energía consumida en un circuito. El valor de energía acumulativo se muestra en el instrumento. Se emplean transductores y multiplicadores basados en varios principios.

La medición de energía no puede repetirse.

10.3.2.4 Detección de fallos y reacción ante ellos

El requisito MI-003, 4.3.1 trata las perturbaciones electromagnéticas. Es necesario interpretar este requisito para los instrumentos controlados por software porque solo se puede detectar una perturbación y recuperarse de la misma mediante acción combinada de determinadas partes del hardware y del software específico. Desde el punto de vista del software no importa cuál sea el motivo de una perturbación (electromagnético, eléctrico, mecánico, etc.): los procedimientos de recuperación son los mismos.

10.3.3 Requisitos de software específicos (contadores de energía eléctrica activa)

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I3-1: Recuperación ante fallos *El software se recuperará de una perturbación y pasará al funcionamiento normal.*		
Especificaciones:		
Documentación requerida: Una breve descripción del mecanismo de recuperación ante fallos y cuándo se activa. Breve descripción de las comprobaciones relacionadas realizadas por el fabricante.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si la implementación de la recuperación ante fallos es adecuada. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: Una subrutina microprocesada reinicia periódicamente un "temporizador de control hardware" (hardware *watchdog*) evitando su disparo. Si alguna función no se ha procesado o – en el peor de los casos – el microprocesador se cuelga en un bucle infinito, este reinicio no tiene lugar y el temporizador de control se dispara al cabo del tiempo establecido.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I3-2: Funcionalidades para la generación de copias de seguridad *Existirá una funcionalidad que, en caso de que se produzca alguna perturbación, proporcione copias de seguridad periódicas de los datos legalmente relevantes como los valores de medición y el estado actual del proceso. Estos datos se guardarán en un almacenamiento no volátil.*		
Especificaciones: Si se utiliza la funcionalidad de copia de seguridad para la recuperación de fallos, deberá calcularse el intervalo mínimo para garantizar que no se exceda el valor crítico de cambio.		
Documentación requerida: Una breve descripción de sobre qué datos se ha realizado copia de seguridad y de cuándo se realizó dicha copia.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará que todos los datos legalmente relevantes se guardan en un almacenamiento no volátil y que se pueden recuperar. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: Se realizan copias de seguridad de los datos legalmente relevantes según se requiera.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I3-3: MI-003, 5.2 (aptitud de la indicación) *El dispositivo indicador de la energía total tendrá un número de dígitos suficiente para asegurar que, cuando el contador funcione durante 4 000 horas a carga completa ($I = I_{máx}$, $U = U_n$ y $FP = 1$), la indicación no vuelva a su valor inicial.*		
Especificaciones:		
Documentación requerida: Documentación de la representación interna del registro de energía eléctrica y magnitudes auxiliares (tipos de variables).		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si la capacidad de almacenamiento es suficiente.		
Ejemplo de solución aceptable: Los valores típicos para los contadores de electricidad trifásicos son: $P_{máx}$ (4 000 h) = 3 * 60 A * 230 V * 4 000 h = 165 600 kWh. Esto requiere una representación interna de 4 bytes.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I3-4: Anexo I, 8.5 de la MID (Evitar la puesta a cero de los valores de medida acumulativos) *En el caso de los instrumentos de medida de empresas de servicio público el indicador de la cantidad total suministrada o los indicadores de los que puede extraerse la cantidad total suministrada, que sirvan de referencia total o parcial para el pago, no podrán ponerse a cero durante su utilización.*		
Especificaciones: Los registros acumulativos de un instrumento de medida pueden ponerse a cero antes de su puesta en servicio.		
Documentación requerida: Documentación de los medios de protección frente a la puesta a cero de los registros de energía.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará que los valores de medida legalmente relevantes y acumulativos no puedan ponerse a cero sin evidencia de la intervención. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento. Véase P3 y P4.		
Ejemplo de solución aceptable: Los registros de energía están protegidos frente a los cambios y la puesta a cero del mismo modo que los parámetros (véase P7).		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I3-5: Comportamiento dinámico *El software legalmente no relevante no deberá influir de forma negativa en el comportamiento dinámico de un proceso de medición.*		
Especificaciones: • Este requisito se aplica junto con S-1, S-2 y S-3 si se ha realizado separación de software conforme a la extensión S. • Este requisito adicional garantiza que, para aplicaciones en tiempo real de los contadores, el comportamiento dinámico del software legalmente relevante no se ve influenciado de forma inadmisible por el software legalmente no relevante, es decir, que los recursos del software legalmente relevante no se vean reducidos de forma inadmisible por la parte no legal.		
Documentación requerida: • Descripción de la jerarquía de interrupción. • Diagrama de tiempos de las tareas de software. Límites del ejecutable proporcionado para tareas legalmente no relevantes.		
Guía de validación: *Comprobaciones basadas en la documentación:* La documentación de los límites del ejecutable proporcionado para tareas legalmente no relevantes estará disponible para el programador de la parte del software legalmente no relevante. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: La jerarquía de interrupción está diseñada de manera que impida influencias adversas.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I3-6: Identificación impresa del software *La identificación del software suele presentarse en un dispositivo indicador. Como excepción para los contadores de energía eléctrica activa, será una solución aceptable una impresión que identifique el software en la placa de características del instrumento siempre que se cumplan las siguientes condiciones:* *A. La interfaz de usuario no tiene capacidad de control para activar la indicación de la identificación del software en el dispositivo indicador o este técnicamente no permite mostrar la identificación del software (contador mecánico).* *B. El instrumento no tiene ninguna interfaz para comunicar la identificación del software.* *C. No es posible cambiar el software del contador después de su fabricación o solo es posible si se cambia también el hardware o un componente hardware.*		
Especificaciones: • El fabricante del hardware o del componente hardware pertinente es responsable de que la identificación del software esté correctamente marcado en dicho hardware. • Se aplican todas las demás especificaciones de P2/U2.		
Documentación requerida: • La misma que en P2/U2.		
Guía de validación: *Comprobaciones basadas en la documentación:* La misma que en P2/U2. *Comprobaciones funcionales:* La misma que en P2/U2.		
Ejemplo de solución aceptable: Una marca impresa en la placa de características del instrumento que identifique el software.		

10.3.4 Ejemplos de parámetros legalmente relevantes

Los contadores electrónicos de suministros de servicios públicos suelen tener muchos parámetros. Se utilizan como constantes de cálculo, de configuración, etc., pero también para el ajuste de la funcionalidad del dispositivo. Con respecto a la identificación y protección de los parámetros y el conjunto de parámetros, véanse los requisitos P2 y P7 de la guía P.

A continuación se proporcionan algunos parámetros típicos de los contadores de energía eléctrica activa. Esta tabla se actualizará cuando el grupo de trabajo 11 de WELMEC haya decido su contenido final.

Parámetro	Protegido	Configurable	Comentario
Factor de calibración	x		
Factor de linealidad	x		

10.3.5 Otros aspectos

En el caso de aplicaciones domésticas, se supone que la descarga de software (extensión D, capítulo 9) no será muy importante.

El registro de energía o volumen acumulados de instrumentos domésticos no es un almacenamiento a largo plazo en el sentido de la extensión L (capítulo 6). En el caso de instrumentos que solo midan energía/volumen acumulados, no es necesario aplicar la extensión L.

10.3.6 Asignación de la clase de riesgo

Hasta ahora, según las decisiones del grupo de trabajo responsable de WELMEC nº 11 (segunda reunión, 3-4 de marzo de 2005), se consideran adecuadas las siguientes clases de riesgo y deberían aplicarse si se llevan a cabo exámenes de software basados en la presente guía para los contadores de energía eléctrica activa (controlados mediante software):

- **Clase de riesgo C para instrumentos de tipo P**

Sin embargo, no se ha tomado todavía ninguna decisión definitiva y el grupo de trabajo nº 11 reconsiderará este tema en relación con el debate sobre las clases de riesgo adecuadas para los instrumentos de tipo U.

El grupo de trabajo nº 11 considera que la funcionalidad de prepago y de medición en intervalos son adicionales a aquellas funciones de medición esenciales especificadas en el anexo MI-003 de la MID.

Por lo tanto, a estas variantes no se les asigna una categoría de riesgos mayor que la asignada a los contadores de tipo básico contemplados en esta guía. Sin embargo, debería evaluarse la función de medición básica, como ocurre con todos los demás instrumentos de tipo P junto con cualquier otra evaluación que se considere necesaria para demostrar que el software asociado que proporciona estas funciones no tiene una influencia inadmisible sobre la medición básica.

10.4 Contadores de energía térmica

10.4.1 Reglamentos específicos, normas y otros documentos normativos

Los Estados miembros pueden —según el artículo 2 de la MID— prescribir el uso de los contadores de energía térmica sometidos a la regulación de la MID en el uso residencial, comercial y de industria ligera.

Los requisitos específicos de este capítulo se basan exclusivamente en el anexo MI-004.

No se han tenido en cuenta las recomendaciones y normas de la OIML.

10.4.2 Descripción técnica

10.4.2.1 Configuración hardware

Los contadores de energía térmica suelen construirse como dispositivos desarrollados específicamente (tipo P en esta guía). Un contador de energía térmica puede ser un instrumento completo o un instrumento combinado que consta de los subconjuntos: sensor de flujo, par sensor de temperatura, y calculador, según se define en el artículo 4 b), o una combinación de estos.

10.4.2.2 Configuración software

Es específica de cada fabricante, pero normalmente debería esperarse que siguiera las recomendaciones proporcionadas en el cuerpo principal de esta guía.

10.4.2.3 Principio de medida

Los contadores de energía térmica acumulan continuamente la energía consumida en un circuito de calefacción. La energía térmica acumulada se muestra en el instrumento. Se emplean varios principios. La medición de energía no puede repetirse.

10.4.2.4 Detección de fallos y reacción ante ellos

Los requisitos MI-004, 4.1 y 4.2 tratan las perturbaciones electromagnéticas. Es necesario interpretar este requisito para los instrumentos controlados por software porque solo se puede detectar una perturbación y recuperarse de la misma mediante acción combinada de determinadas partes del hardware y del software específico. Desde el punto de vista del software no importa cuál sea el motivo de una perturbación (electromagnético, eléctrico, mecánico, etc.): los procedimientos de recuperación son los mismos.

10.4.3 Requisitos específicos de software (contadores de energía térmica)

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I4-1: Recuperación ante fallos *El software se recuperará de una perturbación y pasará al funcionamiento normal.*		
Especificaciones: Deberán activarse indicadores con la fecha para facilitar el registro de periodos de mal funcionamiento.		
Documentación requerida: Una breve descripción del mecanismo de recuperación ante fallos y cuándo se activa.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si la implementación de la recuperación ante fallos es adecuada. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: Una subrutina microprocesada reinicia periódicamente un "temporizador de control hardware" (hardware *watchdog*) evitando su disparo. Si alguna función no se ha procesado o – en el peor de los casos – el microprocesador se cuelga en un bucle infinito, este reinicio no tiene lugar y el temporizador de control se dispara al cabo del tiempo establecido.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I4-2: Funcionalidades para la generación de copias de seguridad *Existirá una funcionalidad que, en caso de que se produzca alguna perturbación, proporcione copias de seguridad periódicas de los datos legalmente relevantes, como los valores de medición y el estado actual del proceso. Estos datos se guardarán en un almacenamiento no volátil.*		
Especificaciones: Los intervalos de almacenamiento deben ser suficientemente breves como para que la discrepancia entre los valores actuales y los acumulativos sea pequeña.		
Documentación requerida: Una breve descripción de sobre qué datos se ha realizado copia de seguridad y de cuándo se realizó dicha copia. Un cálculo del error máximo que puede producirse para los valores acumulativos.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará que todos los datos legalmente relevantes se guardan en un almacenamiento no volátil y que se pueden recuperar. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: Se realizan copias de seguridad de los datos legalmente relevantes según se requiera (p. ej., cada 60 minutos).		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I4-3: Anexo I, 8.5 de la MID (Evitar la puesta a cero de los valores de medida acumulativos) *En el caso de los instrumentos de medida de empresas de servicio público el indicador de la cantidad total suministrada o los indicadores de los que puede extraerse la cantidad total suministrada, que sirvan de referencia total o parcial para el pago, no podrán ponerse a cero durante su utilización.*		
Especificaciones: Los registros acumulativos de un instrumento de medida pueden ponerse a cero antes de su puesta en servicio.		
Documentación requerida: Documentación de los medios de protección frente a la puesta a cero de los registros de volumen.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará que los valores de medida legalmente relevantes y acumulativos no puedan ponerse a cero sin dejar rastro. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: Los registros de volumen están protegidos frente a los cambios y la puesta a cero del mismo modo que los parámetros (véase P7).		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I4-4: Comportamiento dinámico *El software legalmente no relevante no deberá influir de forma negativa en el comportamiento dinámico de un proceso de medición.*		
Especificaciones: • Este requisito se aplica junto con S-1, S-2 y S-3 si se ha realizado separación de software conforme a la extensión S. • Este requisito adicional garantiza que, para aplicaciones en tiempo real de los contadores, el comportamiento dinámico del software legalmente relevante no se ve influenciado de forma inadmisible por el software legalmente no relevante, es decir, que los recursos del software legalmente relevante no se vean reducidos por la parte no legal de forma inadmisible.		
Documentación requerida: • Descripción de la jerarquía de interrupción. • Diagrama de tiempos de las tareas de software. Límites del ejecutable proporcionado para tareas legalmente no relevantes.		
Guía de validación: *Comprobaciones basadas en la documentación:* La documentación de los límites del ejecutable proporcionado para tareas legalmente no relevantes estará disponible para el programador de la parte del software legalmente no relevante. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: La jerarquía de interrupción está diseñada de manera que impida influencias adversas.		

Clase de riesgo B	**Clase de riesgo C**	**Clase de riesgo D**

I4-5: Identificación impresa del software

La identificación del software suele presentarse en un dispositivo indicador. Como excepción para los contadores de energía térmica, será una solución aceptable una impresión que identifique el software en la placa de características del instrumento siempre que se cumplan las siguientes condiciones:

A. La interfaz de usuario no tiene capacidad de control para activar la indicación de la identificación del software en el dispositivo indicador o este técnicamente no permite mostrar la identificación del software (contador mecánico).

B. El instrumento no tiene ninguna interfaz para comunicar la identificación del software.

C. No es posible cambiar el software del contador después de su fabricación o solo es posible si se cambia también el hardware o un componente hardware.

Especificaciones:

- El fabricante del hardware o del componente hardware pertinente es responsable de que la identificación del software esté correctamente marcado en dicho hardware.
- Se aplican todas las demás especificaciones de P2/U2.

Documentación requerida:

La misma que en P2/U2.

Guía de validación:

Comprobaciones basadas en la documentación:

La misma que en P2/U2.

Comprobaciones funcionales:

La misma que en P2/U2.

Ejemplo de solución aceptable:

Una marca impresa en la placa de características del instrumento que identifique el software.

10.4.4 Ejemplos de parámetros legalmente relevantes

Los contadores de energía térmica tienen parámetros, como constantes de cálculo, de configuración, etc., pero también parámetros para el ajuste de la funcionalidad del dispositivo. Con respecto a la identificación y protección de los parámetros y el conjunto de parámetros, véanse los requisitos P2 y P7 de la guía P.

A continuación, se proporcionan algunos parámetros típicos de los contadores de energía térmica. Esta tabla se actualizará cuando el grupo de trabajo 11 de WELMEC haya decido su contenido final.

Parámetro	Protegido	Configurable	Comentario
Factor de calibración	x		
Factor de linealidad	x		

10.4.5 Otros aspectos

En el caso de aplicaciones domésticas, se supone que la descarga de software (extensión D, capítulo 9) no será muy importante.

El registro de energía o volumen acumulados de instrumentos domésticos no es un almacenamiento a largo plazo en el sentido de la extensión L (capítulo 6). En el caso de instrumentos que solo midan energía/volumen acumulados, no es necesario aplicar la extensión L.

10.4.6 Asignación de la clase de riesgo

Hasta ahora, según las decisiones del grupo de trabajo responsable de WELMEC nº 11 (segunda reunión, 3-4 de marzo de 2005), se consideran adecuadas las siguientes clases de riesgo y deberían

aplicarse si se llevan a cabo exámenes de software basados en la presente guía para los contadores de energía térmica (controlados mediante software):

- Clase de riesgo C para instrumentos de tipo P

Sin embargo, no se ha tomado todavía ninguna decisión definitiva y el grupo de trabajo nº 11 reconsiderará este tema en relación con el debate sobre las clases de riesgo adecuadas para los instrumentos de tipo U.

10.5 Sistemas para la medición continua y dinámica de cantidades de líquidos distintos del agua.

Los sistemas para la medición continua y dinámica de cantidades de líquidos distintos del agua están sometidos a la regulación de la MID. Los requisitos específicos se encuentran en el anexo MI-005. Aún no se han tenido en cuenta ni estos requisitos específicos ni los documentos normativos.

Los apartados 10.5.1 y 10.5.2 se rellenarán en el futuro si se considera necesario.

10.5.3 Requisitos de software específicos (Sistemas para la medición de líquidos distintos del agua)

Clase de riesgo B	**Clase de riesgo C**	**Clase de riesgo D**
I5-1: Identificación impresa del software *La identificación del software suele presentarse en un dispositivo indicador. Como excepción para los componentes de un sistema de medición de líquidos distintos del agua, será una solución aceptable una impresión que identifique el software en la placa de características del instrumento siempre que se cumplan las siguientes condiciones:* *A. La interfaz de usuario no tiene capacidad de control para activar la indicación de la identificación del software en el dispositivo indicador o este técnicamente no permite mostrar la identificación del software (contador mecánico).* *B. El instrumento no tiene ninguna interfaz para comunicar la identificación del software.* *C. No es posible cambiar el software del componente después de su fabricación o solo es posible si se cambia también el hardware o un componente hardware.*		
Especificaciones: • La etiqueta con la identificación del software debe ser indeleble y no transferible • El fabricante del hardware o del componente hardware pertinente es responsable de que la identificación del software esté correctamente marcado en dicho hardware. • Se aplican todas las demás especificaciones de P2/U2.		
Documentación requerida: La misma que en P2/U2.		
Guía de validación: *Comprobaciones basadas en la documentación:* La misma que en P2/U2. *Comprobaciones funcionales:* La misma que en P2/U2.		
Ejemplo de solución aceptable: Una marca impresa en la placa de características del instrumento que identifique el software.		

Los apartados 10.5.4 y 10.5.5 se rellenarán en el futuro si se considera necesario.

10.5.6 Asignación de la clase de riesgo

Por ahora, y según el resultado del cuestionario de 2004 del grupo de trabajo 7 de WELMEC y sujeto a futuras decisiones del grupo de trabajo responsable de WELMEC, deberían aplicarse si se llevan a

cabo exámenes de software basados en la presente guía para los sistemas de medida para medir de forma continua y dinámica magnitudes de líquidos distintos del agua (controlados mediante software):

- Clase de riesgo C

10.6 Instrumentos de pesaje

Los instrumentos de pesaje se dividen en dos categorías principales:

1. Instrumentos de pesaje de funcionamiento no automático (IPFNA) e
2. Instrumentos de pesaje de funcionamiento automático (IPFA).

La mayoría de los IPFA están sometidos a la MID; sin embargo, los IPFNA están sometidos todavía a la Directiva europea 90/384/CEE. **Por lo tanto, la guía de software WELMEC 2.3 se aplica a los IPFNA, mientras que la presente guía de software se aplica a los IPFA.**

Los requisitos específicos de este capítulo se basan en el anexo MI-006 y en los documentos normativos mencionados en el apartado 10.6.1, que facilitan la interpretación de los requisitos de la MID.

10.6.1 Reglamentos específicos, normas y otros documentos normativos

Hay cinco categorías de instrumentos de pesaje de funcionamiento automático sometidas al anexo MI-006 de la MID:

- Seleccionadoras ponderales automáticas (R 51)
- Instrumentos gravimétricos de llenado de funcionamiento automático (R 61)
- Totalizador discontinuo (R 107)
- Totalizador continuo (cinta de pesaje) (R 50)
- Báscula puente de ferrocarril (R 106).

Los números entre paréntesis hacen referencia a las respectivas recomendaciones de la OIML que son documentos normativos en el sentido de la MID. Además, WELMEC ha publicado la guía WELMEC 2.6 que facilita los ensayos de las seleccionadoras ponderales automáticas.

Hay una categoría de IPFA que no está sometida a la MID.

- Instrumentos de pesaje automáticos para vehículos en movimiento (R 134).

Los IPFA de todas las categorías pueden diseñarse como tipo P o tipo U y todas las extensiones podrían ser relevantes para cada categoría.

Sin embargo, de estas seis categorías, solo los **totalizadores discontinuos** y los **totalizadores continuos** (cintas de pesaje) se han identificado como susceptibles de necesitar requisitos de software específicos de los instrumentos (véase 10.6.3). Esto se debe a que la medición es acumulativa durante un periodo de tiempo relativamente largo y no se puede repetir si aparece un fallo significativo.

10.6.2 Descripción técnica

10.6.2.1 Configuración hardware

Un totalizador discontinuo es una pesadora-totalizadora de tolva que determina la masa de un producto a granel (p. ej. el grano) dividiéndolo en cargas discretas. El sistema normalmente consta de una o varias tolvas apoyadas en células de carga, fuente de alimentación, controles electrónicos y dispositivo indicador.

Un totalizador continuo es una cinta de pesaje que mide la masa de un producto mientras la cinta transportadora pasa sobre una célula de carga. El sistema normalmente consta de una cinta transportadora, rodillos, receptor de carga apoyado en células de carga, fuente de alimentación, controles electrónicos y dispositivo indicador. Habrá un modo de ajustar la tensión de la cinta.

10.6.2.2 Configuración software

Es específica de cada fabricante, pero normalmente debería esperarse que siguiera las recomendaciones proporcionadas en el cuerpo principal de esta guía.

10.6.2.3 Principio de medida

En el caso de un totalizador discontinuo el producto a granel se introduce en una tolva y se pesa. La masa de cada carga discreta se determina secuencialmente y se suma. A continuación, cada carga discreta se devuelve a granel.

En el caso de un totalizador continuo, la masa se mide continuamente mientras pasa el producto por el receptor de carga. Las mediciones se realizan en unidades discretas de tiempo que dependen de la velocidad de la cinta y de la fuerza sobre el receptor de carga. No se produce ninguna subdivisión deliberada del producto, ni ninguna interrupción de la cinta transportadora como sucede con el totalizador discontinuo. La masa total es una integración de las muestras discretas. Hay que destacar que el receptor de carga podría utilizar células de carga con galgas extensométricas u otras tecnologías como hilo vibrante.

10.6.2.4 Defectos

Las juntas en la cinta podrían causar impacto que pueden dar lugar a errores en la puesta a cero. En el caso de los totalizadores discontinuos, podrían perderse uno o todos los resultados de pesaje de cargas discretas antes de ser sumados.

10.6.3 Requisitos específicos de software (totalizadores continuos y discontinuos)

El anexo MI-006 de la MID, capítulo IV apartado 8 y capítulo V apartado 6, trata las perturbaciones electromagnéticas. Es necesario interpretar estos requisitos para los instrumentos controlados por software porque solo se puede detectar una perturbación (fallo) y recuperarse de la misma mediante la acción combinada de determinadas partes del hardware y del software específico. Desde el punto de vista del software no importa cuál sea el motivo de una perturbación (electromagnético, eléctrico, mecánico, etc.): los procedimientos de recuperación son los mismos.

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I6-1: Detección de fallos *El software detectará que el procesamiento normal se ha visto perturbado.*		
Especificaciones: Al detectar un fallo: a. Las mediciones acumulativas y otros datos legalmente relevantes se guardarán automáticamente en un almacenamiento no volátil (véase el requisito I6-2) y b. la pesadora de tolva o cinta transportadora se detendrá de forma automática o se activará una alarma visible o audible (véase la documentación requerida).		
Documentación requerida: Una breve descripción de lo que se comprueba, qué se requiere para activar el proceso de detección de fallos y cómo actuar si se detecta un fallo. Si al detectar un fallo no es posible detener el sistema de transporte de manera automática y sin retraso (p. ej., debido a razones de seguridad), la documentación incluirá una descripción de cómo tratar el material que no se haya medido o de cómo tenerlo en cuenta debidamente.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si la implementación de la detección de fallos es adecuada. *Comprobaciones funcionales:* Si es posible: simule determinados fallos de hardware y compruebe si el software los detecta y reacciona ante ellos como se describe en la documentación.		
Ejemplo de solución aceptable: Una subrutina microprocesada reinicia periódicamente un "temporizador de control hardware" (hardware *watchdog*) evitando su disparo. Antes de reiniciar, la subrutina comprueba el estado del sistema, por ejemplo, si durante el último intervalo se han procesado todas las subrutinas metrológicamente relevantes. Si alguna función no se ha procesado o – en el peor de los casos – el microprocesador se cuelga en un bucle infinito, este reinicio no tiene lugar y el temporizador de control se dispara al cabo del tiempo establecido.		

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I6-2: Funcionalidades para la generación de copias de seguridad *Existirá una funcionalidad que, en caso de que se produzca alguna perturbación, proporcione copias de seguridad de los datos legalmente relevantes como los valores de medición y el estado actual del proceso.*		
Especificaciones: a. Las características de estado y los datos importantes se guardarán en un almacenamiento no volátil. b. Este requisito normalmente implica un sistema de almacenamiento controlado que efectúe copias de seguridad automáticas en caso de perturbación. Las copias de seguridad periódicas solo se aceptarán si no se dispone de un sistema de almacenamiento controlado debido a restricciones funcionales o de hardware. En ese caso excepcional los intervalos de almacenamiento han de ser lo suficientemente pequeños, es decir, la discrepancia máxima posible entre los valores actuales y los guardados ha de estar dentro de una fracción definida del error máximo permitido (véase la documentación requerida). c. Las funcionalidades de copia de seguridad deberían incluir normalmente funciones de reactivación adecuadas para que el sistema de pesaje, incluido su software, no entre en un estado indefinido causado por alguna perturbación.		
Documentación requerida: • Una breve descripción del mecanismo de copias de seguridad y los datos que se copian y cuándo se realiza la copia. • Especificación o cálculo del error máximo que puede producirse para los valores acumulativos si se ha implementado una copia de seguridad cíclica (periódica).		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si en caso de perturbación se guardan todos los datos legalmente relevantes . *Comprobaciones funcionales:* Se comprobará, simulando una perturbación, si el mecanismo de copias de seguridad funciona tal y como se describe en la documentación.		
Ejemplo de solución aceptable: Se dispara un "temporizador de control hardware" (hardware *watchdog*) cuando no se haya reiniciado cíclicamente. Esto activa una interrupción en el microprocesador. La rutina asignada a la interrupción recoge simultáneamente los valores de medición, los valores de estado y otros datos relevantes, y los guarda en un almacenamiento no volátil como, por ejemplo, una EEPROM u otro almacenamiento adecuado. *Nota*: Se supone que la interrupción generada por el temporizador de control tiene la prioridad de interrupción más alta y domina sobre cualquier proceso normal o cualquier bucle arbitrario infinito, es decir, el control del programa siempre salta hasta la rutina de interrupción si se dispara el temporizador de control.		

10.6.4 Ejemplos de funciones y datos legalmente relevantes

Tabla 10-1: Ejemplos de funciones legalmente relevantes específicas del dispositivo (FD), datos legalmente relevantes específicos del dispositivo (DD) y funciones legalmente relevantes específicas del tipo (FT), datos legalmente relevantes específicos del tipo (DT) para los IPFA en comparación con aquellos para los IPFNA (R 76). VV indica valores variables.

Funciones/datos	Tipo	OIML nº						
		50	51 (X)	51 (Y)	61	76	106	107
Cálculo del peso	FT, DT	X	X	X	X	X	X	X
Análisis de estabilidad	FT, DT		X	X	X	X	X	X
Cálculo del precio	FT, DT		X			X		
Algoritmo de redondeo del precio	FT, DT		X			X		
Intervalo (sensibilidad)	DD	X	X	X	X	X	X	X
Correcciones debidas a la falta de linealidad	DD (DT)	X	X	X	X	X	X	X
Máx., mín., e, d	DD (DT)	X	X	X	X	X	X	X
Unidades de medida (p. ej. g, kg)	DD (DT)	X	X	X	X	X	X	X
Valor del peso como se indica (redondeado a múltiplos de e o d)	VV	X		X		X	X	X
Tara, tara predeterminada	VV		X	X	X	X	X	
Precio unitario, precio a pagar	VV			X		X		X
Valor del peso en resolución interna	VV	X	X	X	X	X	X	X
Señales de estado (p. ej. indicación de cero, estabilidad del equilibrio)	FT	X	X	X	X	X	X	X
Comparación entre el peso real y el valor preestablecido	FT		X		X			
Impresión automática (p. ej. En la interrupción del funcionamiento automático)	FT	X						X
Tiempo de calentamiento	FT (DT)	X	X	X	X	X	X	X
Interbloqueo entre funciones	FT		X	X				
p. ej. puesta cero/tara			X	X	X	X		
operación automática/no automática							X	
puesta a cero/totalización		X						X
Registro del acceso al ajuste dinámico	FT (VV)		X	X				
Valor máximo de funcionamiento/intervalo de velocidad de funcionamiento (pesaje dinámico)	DD (DT)	X	X	X	X		X	X
Parámetros (del producto) para el cálculo dinámico del peso	VV		X	X			X	
Amplitud del intervalo de ajuste	DD (DT)		X	X				
Criterio para la puesta a cero automática (p. ej. intervalo de tiempo, fin del ciclo de pesaje)	DD (DT)		X	X	X		X	X
Descarga mínima, valor mínimo de carga	DD				X			X
Valor límite de fallo significativo (si es distinto de 1 e ó 1 d)	DD (DT)	X			X			
Valor límite de la tensión de la batería	DD (DT)	X	X	X	X		X	X

Tabla 10-1: Ejemplos de funciones y datos legalmente relevantes específicos del dispositivo y del modelo.

Es probable que las funciones y los parámetros marcados en la tabla anterior estén presentes en los distintos tipos de instrumentos de pesaje. Si alguno de ellos está presente, deberá tratarse como "legalmente relevante". Sin embargo, la tabla no es una lista obligatoria que indique que cada función o parámetro de los mencionados deba estar presente en cada instrumento.

10.6.5 Otros aspectos

Ninguno

10.6.6 Asignación de la clase de riesgo

Hasta ahora, según las decisiones del grupo de trabajo responsable de WELMEC (24ª reunión del grupo de trabajo nº 2, 22-23 de enero de 2004), se aplicará en general la clase de riego "B" a todas las categorías de IPFA independientemente del tipo (P o U).

Sin embargo, como consecuencia del cuestionario del grupo de trabajo nº 7 (2004), se considera adecuada la siguiente diferenciación con respecto a los instrumentos de tipo P y U y a los instrumentos totalizadores continuos y discontinuos y dicha diferenciación se discutirá de nuevo en el grupo de trabajo nº 2 de WELMEC (decisión de la 25ª reunión del grupo de trabajo nº 2, 14-15 de octubre de 2004):

- **Clase de riesgo B para instrumentos de tipo P (excepto los totalizadores)**
- **Clase de riesgo C para instrumentos de tipo U y totalizadores de tipo P y tipo U**

10.7 Taxímetros

Los taxímetros están sometidos a la regulación de la MID. Los requisitos específicos se encuentran en el anexo MI-007. Aún no se han tenido en cuenta ni estos requisitos específicos ni los documentos normativos.

10.7.1 Reglamentos específicos, normas y documentos normativos

Aún no se ha considerado la norma europea EN50148 que podría convertirse en un documento normativo en el sentido de la MID. Existe una publicación de un documento orientativo sobre taxímetros como consecuencia del proyecto sobre procedimientos de la MID. En el futuro, este documento constituirá la base de una guía WELMEC. Existe también un primer borrador de recomendación de la OIML sobre taxímetros. Sin embargo, el documento de la OIML no se encuentra en una fase en la que pueda utilizar como documento normativo (situación de octubre de 2004).

10.7.2 Descripción técnica

Un taxímetro, según se define en la MID, mide el tiempo, la distancia (usando la salida de un generador de señales de distancia que no está cubierto por la MID) y calcula el importe de un viaje según las tarifas aplicables.

Los taxímetros actuales utilizan una arquitectura integrada, lo que significa que los taxímetros son instrumentos desarrollados específicamente (tipo P) en según esta guía. En el futuro, se espera que los taxímetros también se fabriquen utilizando ordenadores universales (tipo U).

10.7.3 Requisitos específicos de software

Anexo MI-007, 9 de la MID:

En caso de disminución del suministro de tensión hasta un valor inferior al límite mínimo de funcionamiento especificado por el fabricante, el taxímetro deberá:

- seguir funcionando correctamente o reanudar su funcionamiento correcto sin pérdida de los datos de que se disponía antes de la bajada de corriente si la interrupción de corriente es temporal, por ejemplo debido a que se ha vuelto a poner en marcha el motor;
- interrumpir la medición existente y volver a la posición "Libre" si la interrupción de corriente es durante un período más largo.

Los taxímetros también necesitan disponer de un almacenamiento a largo plazo; los datos han de estar disponibles en el taxímetro durante al menos un año (véase MI-007, 15.2).

Clase de riesgo B	Clase de riesgo C	Clase de riesgo D
I7-1: Funcionalidades para la generación de copias de seguridad *Existirá una funcionalidad que realizará copias de seguridad de los datos esenciales de forma automática como, por ejemplo, los valores de medida y el estado actual del proceso si la tensión disminuye durante un período de tiempo mayor.*		
Especificaciones: 1) Normalmente, estos datos deberían guardarse en un almacenamiento no volátil. 2) Se considera necesario un detector del nivel de tensión para detectar cuándo almacenar valores de medición. 3) Las funcionalidades de copia de seguridad incluirán funcionalidades de reactivación adecuadas para que el taxímetro, incluido su software, no entre en un estado indefinido.		
Documentación requerida: Una breve descripción de sobre qué datos se ha realizado copia de seguridad y de cuándo se realizó dicha copia.		
Guía de validación: *Comprobaciones basadas en la documentación:* Se comprobará si la implementación de la recuperación ante fallos es adecuada. *Comprobaciones funcionales:* Ninguna, aparte de las realizadas durante el examen de modelo para confirmar el correcto funcionamiento en presencia de determinadas magnitudes de influencia.		
Ejemplo de solución aceptable: El detector del nivel de tensión dispara una interrupción cuando el nivel de tensión desciende durante 15 s. La rutina de interrupción asignada recopila los valores de medición, los valores de estado y otros datos relevantes, y los guarda en un almacenamiento no volátil como, por ejemplo, una EEPROM. Cuando el nivel de tensión aumenta de nuevo, los datos se restauran y el funcionamiento continúa o se detiene (véase MI-007, 9). *Nota*: Se supone que la interrupción generada por el nivel de tensión tiene una prioridad de interrupción alta y domina sobre cualquier proceso normal o cualquier bucle arbitrario infinito, es decir, el control del programa siempre salta hasta la rutina de interrupción si cae la tensión.		

10.7.4 Ejemplos de funciones y datos legalmente relevantes

A continuación, se proporcionan algunos parámetros típicos de los taxímetros.

Parámetro	Protegido	Configurable	Comentario
Factor k	X		Impulsos por km
Tarifas	X	X	Unidad monetaria/km, unidad monetaria/h.
Parámetros de la interfaz		X	Velocidad de transmisión en baudios, etc.

10.7.5 Otros aspectos

Se recomienda la revisión de la Directiva relativa a la homologación de vehículos o que se lleve a cabo cualquier otra regulación que especifique los requisitos de los generadores de señales de distancia de los vehículos utilizados como taxis. Una propuesta preliminar establece:

Para los vehículos que se van a utilizar como taxis, se aplicarán los siguientes requisitos:

1. El generador de señales de distancia proporcionará una señal con una resolución de al menos 2 m.
2. El generador de señales de distancia proporcionará una señal estable a cualquier velocidad del vehículo.
3. El generador de señales de distancia tendrá características definidas en lo que se refiere al nivel de tensión, la amplitud de pulsos y la relación entre velocidad y frecuencia.
4. Facilidad de ensayo…

10.7.6 Asignación de la clase de riesgo

Hasta ahora, y según los resultados del cuestionario de 2004 del grupo de trabajo 7 de WELMEC y sujeto a futuras decisiones del grupo de trabajo de WELMEC responsable, deberían aplicarse las siguientes clases de riesgo si se llevan a cabo exámenes de software basados en la presente guía para los taxímetros (controlados por software):

- Clase de riesgo C para instrumentos de tipo P
- Clase de riesgo D para instrumentos de tipo U

10.8 Medidas materializadas

Las medidas materializadas están sometidas a las regulaciones de la MID. Los requisitos específicos se encuentran en el anexo MI-008.

Sujeto a futuros desarrollos y decisiones, las medidas materializadas en el sentido del anexo MI-008 de la MID no se consideran instrumentos de medida controlados por software.

Por lo tanto, por ahora, la presente guía de software no se aplica a medidas materializadas.

10.9 Instrumentos para medidas dimensionales

Los instrumentos para medidas dimensionales están sometidos a las regulaciones de la MID. Los requisitos específicos se encuentran en el anexo MI-009. Aún no se han tenido en cuenta ni estos requisitos específicos ni los documentos normativos.

Los apartados 10.9.1–10.9.5 se completarán en el futuro si se considera necesario.

10.9.6 Asignación de la clase de riesgo

Hasta ahora, y según los resultados del cuestionario de 2004 del grupo de trabajo 7 de WELMEC y sujeto a futuras decisiones del grupo de trabajo de WELMEC responsable, deberían aplicarse las siguientes clases de riesgo si se llevan a cabo exámenes de software basados en la presente guía para instrumentos para medidas dimensionales (controlados por software):

- Clase de riesgo B para instrumentos de tipo P
- Clase de riesgo C para instrumentos de tipo U

10.10 Analizadores de gases de escape

Los analizadores de gases de escape están sometidos a las regulaciones de la MID. Los requisitos específicos se encuentran en el anexo MI-010. Aún no se han tenido en cuenta ni estos requisitos específicos ni los documentos normativos.

Los apartados 10.10.1–10.10.5 se completarán en el futuro si se considera necesario.

10.10.6 Asignación de la clase de riesgo

Hasta ahora, y según los resultados del cuestionario de 2004 del grupo de trabajo 7 de WELMEC y sujeto a futuras decisiones del grupo de trabajo de WELMEC responsable, deberían aplicarse las siguientes clases de riesgo si se llevan a cabo exámenes de software basados en la presente guía para analizadores de gases de escape (controlados por software):

- **Clase de riesgo B para instrumentos de tipo P**
- **Clase de riesgo C para instrumentos de tipo U**

11 Definición de las clases de riesgo

11.1 Principio general

Los requisitos de esta guía se distinguen según las clases de riesgo (software). Los riesgos se refieren exclusivamente al software del instrumento de medida y a ningún otro riesgo. Por comodidad, se utiliza el término abreviado «clase de riesgo». A cada instrumento de medida se le debe asignar una clase de riesgo porque los requisitos del software que hay que aplicar están determinados por la clase de riesgo a la que pertenece el instrumento. Una clase de riesgo se define como la combinación de los niveles adecuados requeridos de protección, examen y conformidad del software. Se presentan tres niveles para cada una de estas categorías: bajo, medio y alto.

11.2 Descripción de los niveles de protección, examen y conformidad

Las siguientes definiciones se utilizan para los niveles correspondientes.

Niveles de protección del software

Bajo: No se requieren medidas de protección concretas frente a los cambios intencionados.

Medio: El software está protegido frente a los cambios intencionados realizados utilizando herramientas software simples, comunes y fácilmente disponibles (por ej.: editores de texto).

Alto: El software está protegido frente a cambios intencionados realizados utilizando herramientas software sofisticadas (por ej.: depuradores y editores de disco duro, herramientas de desarrollo de software, etc.).

Niveles de examen del software

Bajo: Se realizan las comprobaciones funcionales estándar de examen de modelo del instrumento. No es necesario realizar pruebas de software adicionales.

Medio: Además de las comprobaciones correspondientes al nivel bajo, el software se examina según su documentación. La documentación incluye la descripción de las funciones implementadas por software, la descripción de los parámetros, etc. Para verificar la fiabilidad de la documentación y la eficacia de las medidas de protección, pueden realizarse comprobaciones prácticas aleatorias de las funciones compatibles con el software.

Alto: Además de las comprobaciones correspondientes al nivel medio, se lleva a cabo una comprobación del software en profundidad, que suele basarse en el código fuente.

Niveles de conformidad del software

Bajo: La funcionalidad del software implementado en cada uno de los instrumentos individuales es conforme con la documentación aprobada.

Medio: Además de la conformidad del nivel "bajo", en función de las características técnicas, partes del software se definirán como fijas en el examen de modelo, es decir, modificables solamente con la aprobación previa del organismo notificado. La parte fija será idéntica en cada uno de los instrumentos individuales.

Alto: El software implementado en cada uno de los instrumentos individuales es completamente idéntico al aprobado.

11.3 Asignación de las clases de riesgo

De las 27 permutaciones de nivel teóricamente posibles, solo cuatro o, a lo sumo cinco, tienen interés práctico (clases de riesgo B, C, D y E, eventualmente F). Abarcan todas las clases de instrumentos que están incluidas en la regulación de la MID. Además, proporcionan suficiente rango en caso de que se modifiquen las evaluaciones de riesgo. En la tabla siguiente se definen las clases de riesgo.

Clase de riesgo	Protección del software	Examen del software	Grado de conformidad del software
A	*bajo*	*bajo*	*bajo*
B	*medio*	*medio*	*bajo*
C	*medio*	*medio*	*medio*
D	*alto*	*medio*	*medio*
E	*alto*	*alto*	*medio*
F	*alto*	*alto*	*alto*

Tabla 11-1: Definición de las clases de riesgo

11.4 Interpretación de las clases de riesgo

Clase de riesgo A: Es la clase de riesgo más baja de todas. No se requieren medidas de protección concretas frente a los cambios intencionados del software. El examen de software forma parte de la comprobación funcional del dispositivo. Se requiere conformidad a nivel documental. No es de esperar que ningún instrumento se clasifique con una clase de riesgo A. Sin embargo, al introducir esta clase, se mantiene abierta esta posibilidad.

Clase de riesgo B: En comparación con la clase de riesgo A, se requiere una protección de software de nivel medio. En consecuencia, el nivel de examen aumenta al nivel medio. La conformidad es la misma que la de la clase de riesgo A.

Clase de riesgo C: En comparación con la clase de riesgo B, la conformidad aumenta hasta el nivel medio. Esto significa que partes del software pueden declararse como fijas en el examen de modelo. El resto del software requiere conformidad en el nivel funcional. Los niveles de protección y examen son los mismos que en la clase de riesgo B.

Clase de riesgo D: Si se compara con la clase de riesgo C, la protección aumenta hasta el nivel alto. Puesto que el examen se mantiene invariable en el nivel medio, debe proporcionarse documentación suficientemente informativa para demostrar que las medidas de

protección tomadas son adecuadas. El nivel de conformidad es el mismo que en la clase de riesgo C.

Clase de riesgo E: En comparación con la clase de riesgo D, el examen aumenta hasta el nivel alto. Los niveles de protección y conformidad no cambian.

Clase de riesgo F: Todos los aspectos (protección, examen y conformidad) se establecen en el nivel alto. Al igual que en la clase de riesgo A, no es de esperar que ningún instrumento se clasifique en esta clase. Sin embargo se mantiene abierta esta posibilidad.

12 Modelo del informe de ensayos (incluidas las listas de comprobación)

Este es un modelo de un informe de ensayo, que consta de una parte principal y dos anexos. La parte principal contiene información general del objeto a ensayar. En la práctica debe adaptarse según corresponda. El anexo 1 consta de dos listas de comprobación que facilitan la selección de las partes de la guía que deben aplicarse. El anexo 2 consta de listas de comprobación específicas de las respectivas partes técnicas de la guía. Estos anexos son recomendables para ayudar a que el fabricante y examinador comprueben que han tenido en cuenta todos los requisitos aplicables.

Además del modelo de informe de ensayo y de las listas de comprobación, se incluye la información necesaria para el certificado de examen de modelo en el último subapartado de este capítulo.

12.1 Modelo de la parte general del informe de ensayos

Informe de ensayo n.º XYZ122344

Modelo de caudalímetro Dynaflow DF101

Validación del software

(n anexos)

Comisión

La MID proporciona los requisitos esenciales para determinados instrumentos de medida que utilizados en la Unión Europea. El software del instrumento de medida se ha validado para demostrar su conformidad con los requisitos esenciales de la MID.

La validación se ha basado en el informe de WELMEC sobre los requisitos de software de la MID (guía WELMEC 7.2), donde se interpretan y explican los requisitos esenciales de software. Este informe describe el examen de software necesario para establecer la conformidad con la MID.

Cliente

Dynaflow
P.O. Box 1120333
100 Reykiavik
Islandia
Referencia: Sr. Bjarnur Sigfridson

Objeto del ensayo

El caudalímetro Dynaflow DF100 es un instrumento de medida para medir caudal de líquidos.

El rango de medida oscila entre 1 l/s y 2.000 l/s. Las funciones básicas del instrumento son:

- medida del caudal de líquidos,
- indicación del volumen medido,
- interfaz del transductor.

Según la guía WELMEC 7.2, el caudalímetro se describe del siguiente modo:

- instrumento de medida desarrollado específicamente (sistema embebido),
- almacenamiento a largo plazo de datos legalmente relevantes.

El caudalímetro DF100 es un instrumento independiente con un transductor conectado. El transductor está fijado al instrumento y no puede desconectarse. El volumen medido se indica en una pantalla. No es posible establecer comunicación con otros dispositivos.

El software integrado en el instrumento de medida ha sido desarrollado por:

Dynaflow, P.O. Box 1120333, 100 Reykiavik, Islandia

La versión del software validado es **V1.2.c.** El código fuente consta de los siguientes archivos:

main.c	12.301 bytes	23 nov 2007
int.c	6.509 bytes	23 nov 2003
filter.c	10.897 bytes	20 oct 2003
input.c	2.004 bytes	20 oct 2003
display.c	32.000 bytes	23 nov 2003
Ethernet.c	23.455 bytes	15 jun 2002
driver.c	11.670 bytes	15 jun 2002
calculate.c	6.788 bytes	23 nov 2003

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

- Manual de usuario del DF100,
- Manual de mantenimiento del DF100,
- Descripción del software del DF100 (documento de diseño interno, con fecha de 22 de noviembre de 2003).
- Diagrama del circuito electrónico del DF100 (dibujo nº 222-31, con fecha de 5 de octubre de 2003)

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

Procedimiento de examen

La validación se ha realizado según la guía de software WELMEC 7.2, edición 1 (que se puede descargar de www.welmec.org).

La validación se realizó ente el 1 de noviembre y el 23 de diciembre de 2003. El 3 de diciembre, el Dr. K. Fehler realizó, en la sede central de Dynaflow en Reykiavik, una revisión del diseño. El Dr. K. Fehler y M. S. Problème llevaron a cabo otros trabajos de validación en el laboratorio *National Testing & Measurement* .

Se han validado los siguientes requisitos:

- requisitos específicos del instrumento de medida desarrollado específicamente (tipo P);
- extensión L: - almacenamiento a largo plazo de datos legalmente relevantes.

La lista de comprobación para la selección de configuración se encuentra en el anexo 1 de este informe.

A este instrumento se le ha aplicado la clase de riesgo C.

Los métodos de validación aplicados son los siguientes:

- identificación del software,
- completitud de toda la documentación,
- examen del manual de funcionamiento,
- comprobación funcional,
- revisión del diseño del software,
- revisión de la documentación del software,
- análisis del flujo de datos,
- simulación de las señales de entrada.

Resultado

Se han validado sin encontrar fallos los siguientes requisitos de la guía de software WELMEC 7.2:

- P1, P2, P3, P5, P6, P7 (El requisito P4 no se considera aplicable.)
- L1, L2, L3, L4, L5, L6, L7

La lista de comprobación de los requisitos P figura en el anexo 2.1 de este informe.

La lista de comprobación de los requisitos L figura en el anexo 2.2 de este informe.

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

Se encontró un fallo de software que limitaba el mes de febrero a 28 días también en los años bisiestos en el paquete de software V1.2b. Este fallo se ha corregido en el paquete V1.2c.

El software de Dynaflow DF100 V1.2c cumple los requisitos esenciales de la MID.

El resultado solo se aplica al objeto ensayado.

National Testing & Measurement Lab
Departamento de Software

Dr. K.E.I.N. Fehler
Director técnico

M. S. A. N. S. Problème
Técnico

Fecha: 23 de diciembre de 2003

12.2 Anexo 1 del informe de ensayos: Listas de comprobación que facilitan la selección del conjunto de requisitos adecuado

La primera lista de comprobación ayuda al usuario a decidir qué configuración básica P o U se aplica al instrumento que se está comprobando.

Decisión sobre el tipo de instrumento				
		(P)		**Comentarios**
1	¿Toda la aplicación software se ha desarrollado con el propósito específico de la medición?	**(S)**		
2	En caso de que haya software de propósito general, ¿es accesible o visible para el usuario?	**(N)**		
3	¿Se impide al usuario acceder al sistema operativo en caso de que sea posible cambiar a un modo operativo que no esté sometido a control legal?	**(S)**		
4	¿Son invariables los programas implementados y el entorno de software (aparte de las actualizaciones)?	**(S)**		
5	¿Hay alguna manera de programarlo?	**(N)**		
Marque la casilla que corresponda				

Si y solo si todas las respuestas a las cinco preguntas anteriores están en la columna P, se aplicarán los requisitos del apartado P (capítulo 4). En los demás casos, se aplicarán los requisitos del apartado U (capítulo 5).

La segunda lista de comprobación ayuda a decidir qué configuración TI se aplica al instrumento bajo ensayo.

Decisión sobre las extensiones requeridas					
Extensión requerida		**SÍ**	**NO**	**No aplicable**	**Comentarios**
L	¿Tiene el dispositivo la posibilidad de almacenar los datos de medición en un almacenamiento integrado o en un almacenamiento remoto o extraíble?				
T	¿Posee el dispositivo interfaces para la transmisión de datos a dispositivos sometidos a control legal **o** recibe datos de otro dispositivo sometido a control legal?				
S	¿Hay partes del software con funciones que no estén sometidas a control legal **y** se desea cambiarlas tras el examen de modelo?				
D	¿Es posible o deseable cargar software?				
Considere la extensión requerida para cada una de las respuestas afirmativa.					

12.3 Anexo 2 del informe de ensayos: Listas de comprobación específicas de las respectivas partes técnicas

1) Lista de comprobación de los requisitos básicos para instrumentos tipo P

Lista de comprobación de los requisitos de tipo P						
Requisito	**Procedimientos de ensayo**		**Aceptado**	**Rechazado**	**No aplicable**	**Comentarios***
P1		¿La documentación requerida del fabricante cumple el requisito P1 (a-f)?				
P2		¿La identificación del software se ha implementado según se requiere en P2?				
P3		¿Se impide que los comandos introducidos a través de la interfaz de usuario influyan de manera inadmisible en el software legalmente relevante y en los datos de medida?				
P4		¿Se impide que los comandos introducidos a través de interfaces de comunicación no protegidas del instrumento influyan de manera inadmisible en el software legalmente relevante y en los datos de medida?				
P5		¿El software legalmente relevante y los datos de medida están protegidos frente a cambios accidentales o no intencionados?				
P6		¿El software legalmente relevante está protegido frente a modificaciones, cargas o intercambios (*swapping*) inadmisibles de la memoria hardware?				
P7		¿Los parámetros que fijan las características legalmente relevantes de los instrumentos de medida están protegidos frente a modificaciones no autorizadas?				
* *Deberán añadirse aclaraciones si hay desviaciones a los requisitos de software.*						

2) Lista de comprobación de los requisitos básicos para instrumentos tipo U

Lista de comprobación de los requisitos de tipo U						
Requisito	**Procedimientos de ensayo**		**Aceptado**	**Rechazado**	**No aplicable**	**Comentarios***
U1		¿La documentación requerida del fabricante cumple el requisito U1 (a-g)?				
U2		¿La identificación del software se ha implementado según se requiere en U2?				
U3		¿Se impide que los comandos introducidos a través de la interfaz de usuario influyan de forma inadmisible en el software legalmente relevante y en los datos de medida?				
U4		¿Se impide que los comandos introducidos a través de interfaces de comunicación no protegidas del instrumento influyan de forma inadmisible en el software legalmente relevante y en los datos de medida?				
U5		¿El software legalmente relevante y los datos de medida están protegidos frente a cambios accidentales o no intencionados?				
U6		¿El software legalmente relevante está protegido frente a modificaciones inadmisibles?				
U7		¿Los parámetros legalmente relevantes están protegidos frente a modificaciones no autorizadas?				
U8		¿Se han utilizado medios para garantizar la autenticidad del software legalmente relevante y se garantiza la autenticidad de los resultados que se presentan?				
U9		¿El software legalmente relevante está diseñado de tal manera que otro software no influya en él de modo inadmisible?				
** Deberán añadirse aclaraciones si hay desviaciones a los requisitos de software.*						

3) Lista de comprobación de los requisitos específicos de la extensión L

Lista de comprobación de los requisitos de la extensión L						
Requisito	**Procedimientos de ensayo**		**Aceptado**	**Rechazado**	**No aplicable**	**Comentarios***
L1		¿Los datos de medida almacenados contienen toda la información relevante necesaria para reconstruir una medición anterior?				
L2		¿Los datos almacenados están protegidos frente a cambios accidentales o no intencionados?				
L3		¿Los datos de medida almacenados están protegidos frente a cambios intencionados llevados acabo con *herramientas de software comunes y simples* (para las clases de riesgo B y C) o *herramientas de software sofisticadas especiales* (para las clases de riesgo D y E)?				
L4		¿Es posible rastrear fielmente los datos de medida almacenados hasta la medición que los generó?				
L5		(B y C) ¿Se tratan las claves como datos legalmente relevantes y se mantienen en secreto y protegidas frente a los posibles riesgos originados por *herramientas de software simples*?				
		(D y E) ¿Se tratan las claves y los datos que estas incluyen como datos legalmente relevantes y se mantienen en secreto y protegidos frente a posibles riesgos originados por herramientas de software sofisticadas? ¿Se usan métodos apropiados equivalentes a los usados en el pago electrónico? ¿Puede el usuario verificar la autenticidad de la clave pública?				
L6		¿El software utilizado para verificar los datos de medida almacenados visualiza o imprime información, comprueba los datos en busca de cambios y avisa de las modificaciones realizadas? ¿Existen medios para evitar que se utilicen los datos corruptos detectados?				
L7		¿Los datos de medida se almacenan automáticamente cuando finaliza la medición?				
L8		¿El almacenamiento a largo plazo tiene capacidad suficiente para el propósito deseado?				
** Deberán añadirse aclaraciones si hay desviaciones de los requisitos de software*.						

4) *Lista de comprobación* de los requisitos específicos de la extensión T

***Lista de comprobación* de los requisitos de la extensión T**						
Requisito	**Procedimientos de ensayo**		**Aceptado**	**Rechazado**	**No aplicable**	**Comentarios***
T1		¿Los datos transmitidos contienen toda la información relevante necesaria para presentar o procesar posteriormente el resultado de medida en el módulo receptor?				
T2		¿Los datos transmitidos están protegidos frente a cambios accidentales o no intencionados?				
T3		¿Los datos legalmente relevantes que se transmiten están protegidos frente a cambios intencionados llevados a cabo mediante herramientas de software comunes y simples (para las clases de riesgo B y C) o mediante herramientas de software sofisticadas especiales (para las clases de riesgo D y E)?				
T4		¿Puede el programa que recibe los datos relevantes transmitidos verificar su autenticidad y asignar los valores de medida a una medición determinada?				
T5		B y C) ¿Se tratan las claves como datos legalmente relevantes y se mantienen en secreto y protegidas frente a los posibles riesgos originados por *herramientas de software simples*?				
		D y E) ¿Se tratan las claves y los datos que estas incluyen como datos legalmente relevantes y se mantienen en secreto y protegidos frente a posibles riesgos originados por herramientas de software sofisticadas? ¿Se usan métodos apropiados equivalentes a los usados en el pago electrónico? ¿Puede el usuario verificar la autenticidad de la clave pública?				
T6		¿Se impide el uso de los datos que han sido detectados como corruptos?				
T7		¿Se garantiza que la medida no está influida de modo inadmisible por una demora en la transmisión?				
T8		¿Se garantiza que no se perderán los datos de medición si los servicios de red dejan de estar disponibles?				

** Deberán añadirse aclaraciones si hay desviaciones de los requisitos de software.*

5) Lista de comprobación de los requisitos específicos de la extensión S

Lista de comprobación de los requisitos de la extensión S						
Requisito	**Procedimientos de ensayo**		**Aceptado**	**Rechazado**	**No aplicable**	**Comentarios***
S1		¿El software sometido a control legal contiene todo el software y los parámetros legalmente relevantes?				
S2		¿Se garantiza que la información adicional generada por la parte de software legalmente no relevante que aparezca en pantalla o impresa no se confunde con la información que se origina en la parte legalmente relevante?				
S3		¿El intercambio de datos entre el software legalmente relevante y el software legalmente no relevante se realiza mediante una interfaz de software protectora, que incluye el control de las interacciones y el flujo de datos?				
** Deberán añadirse aclaraciones si hay desviaciones de los requisitos de software.*						

6) Lista de comprobación de los requisitos específicos de la extensión D

Lista de comprobación de los requisitos de la extensión D						
Requisito	**Procedimientos de ensayo**		**Aceptado**	**Rechazado**	**No aplicable**	**Comentarios***
D1		¿La descarga y posterior instalación del software son automáticas? ¿Se garantiza que el entorno de protección del software se encuentre en el nivel aprobado al terminar la descarga e instalación?				
D2		¿Se han utilizado medios para garantizar que la descarga de software es auténtica y para indicar que el software descargado lo ha aprobado un organismo notificado?				
D3		¿Se han utilizado medios para garantizar que el software descargado no ha sido modificado de forma inadmisible durante dicho proceso?				
D4		¿Se garantiza mediante los medios técnicos adecuados que las descargas de software legalmente relevante puedan rastrearse adecuadamente dentro del instrumento para realizar controles posteriores?				
** Deberán añadirse aclaraciones si hay desviaciones de los requisitos de software.*						

12.4 Información que debe incluirse en el certificado de examen de modelo

Aunque el informe de ensayos completo es una documentación del equipo sometido a ensayo, de la validación realizada y de los resultados, solo se requiere una selección determinada de la información incluida en el informe de ensayos para el certificado de examen de modelo. La siguiente información deberá incluirse adecuadamente en el certificado de examen de modelo:

- Referencia a la documentación presentada para el examen de modelo
- Identificación y descripción de los componentes (subconjuntos, módulos) electrónicos (hardware) que son importantes para el software/funciones TI de los instrumentos de medida
- Descripción general del entorno software necesario para utilizar el software bajo examen
- Descripción general de los módulos de software bajo control legal (incluida la separación de software, si se ha implementado)
- Descripción general e identificación de las interfaces de hardware y software (si es relevante) que son importantes para el software/funciones TI del instrumento de medida (incluidos infrarrojos, Bluetooth, LAN inalámbrica...)
- Identificación y descripción de las ubicaciones de los componentes software en el instrumento de medida (es decir, EPROM, procesador, disco duro…) que deben precintarse o protegerse
- Instrucciones de cómo comprobar la identificación del software (para la supervisión metrológica)
- En caso de precinto electrónico: instrucciones para la inspección de los registros de actividades.

13 Referencias cruzadas entre los requisitos de software de la MID y los artículos y anexos de la MID

(Versión de la MID utilizada: Directiva 2004/22/EC del 31 de marzo de 2004)

13.1 Referencias a la MID para cada requisito de software

Requisito		**MID**	
N.º	**Descripción**	**N.º de artículo/anexo** (AI = Anexo I)	**Descripción**
	Guía básica P		
P1	Documentación del fabricante	AI-9.3 AI-12 Artículo 10	Información que deberá figurar en el instrumento y acompañarlo Evaluación de la conformidad Documentación técnica
P2	Identificación del software	AI-7.6 AI-8.3	Aptitud Protección frente a la corrupción
P3	Influencia a través de la interfaz de usuario	AI-7.1	Aptitud
P4	Influencia a través de la interfaz de comunicación	AI-7.1 AI-8.1	Aptitud Protección frente a la corrupción
P5	Protección frente a los cambios accidentales o no intencionados	AI-7.1, AI-7.2 AI-8.4	Aptitud Protección frente a la corrupción
P6	Protección frente a los cambios intencionados	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Aptitud Nota: En lo que se refiere al contenido, el apartado 7.1 de la Directiva relativa a los instrumentos de medida Anexo I no es un problema de «aptitud» si no de «protección frente a la corrupción» (párrafo 8) Protección frente a la corrupción
P7	Protección de parámetros	AI-7.1	Aptitud

Requisito		MID	
N.º	**Descripción**	**N.º de artículo/anexo** (AI = Anexo I)	**Descripción**
		AI-8.2, AI-8.3, AI-8.4	Protección frente a la corrupción
	Guía básica U		
U1	Documentación del fabricante	AI-9.3 AI-12 Artículo 10	Información que deberá figurar en el instrumento y acompañarlo Evaluación de la conformidad Documentación técnica
U2	Identificación del software	AI-7.6 AI-8.3	Aptitud Protección frente a la corrupción
U3	Influencia a través de las interfaces de usuario	AI-7.1	Aptitud
U4	Influencia a través de la interfaz de comunicación	AI-7.1 AI-8.1	Aptitud Protección frente a la corrupción
U5	Protección frente a los cambios accidentales o no intencionados	AI-7.1, AI-7.2 AI-8.4	Aptitud Protección frente a la corrupción
U6	Protección frente a los cambios intencionados	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Aptitud Protección frente a la corrupción
U7	Protección de parámetros	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Aptitud Protección frente a la corrupción
U8	Autenticidad del software y presentación de los resultados	AI-7.1, AI-7.2, AI-7.6 AI-8.3 AI-10.2, AI-10.3, AI-10.4	Aptitud Protección frente a la corrupción Indicación del resultado
U9	Influencia de otro software	AI-7.6	Aptitud
	Extensión L		
L1	Completitud de los datos almacenados	AI-7.1 AI-8.4 AI-10.2	Aptitud Protección frente a la corrupción Indicación del resultado
L2	Protección frente a los cambios accidentales o no intencionados	AI-7.1, AI-7.2 AI-8.4	Aptitud Protección frente a la corrupción
L3	Integridad de los datos	AI-7.1 AI-8.4	Aptitud Protección frente a la corrupción
L4	Autenticidad de los datos almacenados	AI-7.1 AI-8.4 AI-10.2	Aptitud Protección frente a la corrupción Indicación del resultado
L5	Confidencialidad de las claves	AI-7.1 AI-8.4	Aptitud Protección frente a la corrupción
L6	Recuperación de los datos almacenados	AI-7.2 AI-10.2, AI-10.3, AI-10.4	Aptitud Indicación del resultado
L7	Almacenamiento automático	AI-7.1 AI-8.4	Aptitud Protección frente a la corrupción
L8	Capacidad y continuidad de almacenamiento	AI-7.1	Aptitud
Lx	Todas las extensiones L	AI-11.1	Otros procesamientos de datos para concluir la transacción comercial

	Extensión T		
T1	Completitud de los datos transmitidos	AI-7.1 AI-8.4	Aptitud Protección frente a la corrupción
T2	Protección frente a los cambios accidentales	AI-7.1, AI-7.2 AI-8.4	Aptitud Protección frente a la corrupción
T3	Integridad de los datos	AI-7.1 AI-8.4	Aptitud Protección frente a la corrupción
T4	Autenticidad de los datos transmitidos	AI-7.1 AI-8.4	Aptitud Protección frente a la corrupción
T5	Confidencialidad de las claves	AI-7.1 AI-8.4	Aptitud Protección frente a la corrupción
T6	Gestión de los datos corruptos	AI-7.1 AI-8.4	Aptitud Protección frente a la corrupción
T7	Demora en la transmisión	AI-7.1 AI-8.4	Aptitud Protección frente a la corrupción
T8	Disponibilidad de los servicios de transmisión	AI-7.1 AI-8.4	Aptitud Protección frente a la corrupción
	Extensión S		
S1	Realización de la separación de software	AI-7.6 AI-10.1	Aptitud Indicación del resultado
S2	Indicación mixta	AI-7.1, AI-7.2, AI-7.6 AI-10.2	Aptitud Indicación del resultado
S3	Interfaz protectora del software	AI-7.6	Aptitud
	Extensión D		
D1	Mecanismo de descarga	AI-8.2, AI-8.4	Protección frente a la corrupción
D2	Autenticación del software descargado	AI-7.6 AI-8.3, AI-8.4 AI-12	Aptitud Protección frente a la corrupción Evaluación de la conformidad
D3	Integridad del software descargado	AI-7.1 AI-8.4	Aptitud Protección frente a la corrupción
D4	Trazabilidad de la descarga del software legalmente relevante	AI-7.1, AI-7.6 AI-8.2, AI-8.3 AI-12	Aptitud Protección frente a la corrupción Evaluación de la conformidad

	Extensión I (requisitos de software específicos del instrumento)		
I1-1, I2-1, I3-1, I4-1	Detección de fallos	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Fiabilidad Requisitos específicos para medidores de suministros públicos
I1-2, I2-2, I3-2, I4-2	Funcionalidades para la generación de copias de seguridad	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Fiabilidad Requisitos específicos para medidores de suministros públicos
I1-3, I2-3, I3-3, I4-3	Funcionalidades de restauración y reactivación	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Fiabilidad Requisitos específicos para medidores de suministros públicos
I1-4, I2-4, I3-4, I4-4	Resolución interna	MI-002-5.3, MI-003-5.2	Requisitos específicos para medidores de suministros públicos
I1-5, I2-5, I3-5, I4-5	Evitar la puesta a cero de los valores de medida acumulativos	AI-8.5	Protección frente a la corrupción
I1-6, I2-6, I3-6, I4-6	Indicación para el cliente	AI-7.2 AI-10.5	Aptitud Indicación del resultado
I2-7	Solución aceptable para controlar el periodo de vida de una batería	MI-002-5.2	Requisitos específicos de los contadores de gas
I2-8	Solución aceptable para controlar los convertidores del volumen de un gas	MI-002-9.1	Requisitos específicos de los contadores de gas
I2-9	Elemento de ensayo.	MI-002-5.5	Requisitos específicos de los contadores de gas
I6-1	Detección de fallos	MI-006-IV, MI-006-V	Totalizadores continuos y discontinuos
I6-2	Funcionalidades para la generación de copias de seguridad	MI-006-IV, MI-006-V	Totalizadores continuos y discontinuos

13.2 Interpretación de los artículos y anexos de la MID según los requisitos del software

MID			**Guía de software**
N.º de artículo/anexo (AI = Anexo I)	**Descripción**	**Comentario**	**N.º de requisito**
	Parte del artículo		
1, 2, 3		Irrelevante para el software	
4(b)	Definiciones, disposición de los subconjuntos	Transmisión de información legalmente relevante… Guías básicas aplicables a los subconjuntos	T P, U
Del 5 al 9		Irrelevante para el software	
10	Documentación técnica	Documentación sobre el diseño, la fabricación y el funcionamiento. Que permita la evaluación de la conformidad. Descripción general del instrumento. Descripción de los dispositivos electrónicos con planos, diagramas de flujo de la lógica, información general del software. Ubicación de precintos y marcas. Condiciones de compatibilidad con interfaces y subconjuntos.	P1, U1
Del 11 al 27		Irrelevante para el software	
	Anexo I		
Del AI-1 al AI-5		Irrelevante para el software	
AI-6	Fiabilidad	Detección de fallos, copia de seguridad, restauración, reinicio	Del I1-1 al I1-3, Del I2-1 al I2-3, Del I3-1 al I3-3, Del I4-1 al I4-3, Del I6-1 al I6-2
AI-7	Aptitud	No hay características que faciliten el uso fraudulento; posibilidades mínimas de un uso incorrecto no intencionado.	P3–P7, U3–U8, L1–L5, L7, L8, T1–T8, S2, D3, D4
AI-8	Protección frente a la corrupción		
AI-8.1		La conexión de otros dispositivos no influye.	P4, U4
AI-8.2		Protección; prueba evidente de intervención	P6, P7, U6, U7, D1, D4
AI-8.3		Identificación del software; prueba evidente de intervención	P2, P6, P7, U2, U6, U7, U8, D2, D4
AI-8.4		Protección de los datos almacenados o transmitidos	P5–P7, U5–U7, L1–L5, T1–T8 D1–D3
AI-8.5		No permitir la puesta a cero los registros acumulativos	I1-5, I2-5, I3-5, I4-5

MID			Guía de software
N.º de artículo/anexo (AI = Anexo I)	**Descripción**	**Comentario**	**N.º de requisito**
AI-9	Información que deberá figurar en el instrumento y acompañarlo		
AI-9.1		Alcance máximo (el resto de los elementos son irrelevantes para el software)	L8
AI-9.2		Irrelevante para el software	
AI-9.3		Instrucciones de instalación,…, condiciones de compatibilidad con la interfaz, subconjuntos o instrumentos de medida.	P1, U1
Del AI-9.4 al AI-9.8		Irrelevante para el software	
AI-10	Indicación del resultado		
AI-10.1		Indicación mediante una presentación visual o documento impreso.	U8, L6, S2
AI-10.2		Importancia del resultado, no confusión con indicaciones adicionales.	U8, L1, L4, L6, S2
AI-10.3		Impresión o grabación fácilmente legibles e indelebles.	U8, L6, S2
AI-10.4		Para ventas directas: presentación del resultado a ambas partes.	U8, S2
AI-10.5		Para medidores de suministros públicos: indicador visual para el cliente	I1-6, I2-6, I3-6, I4-6
AI-11	Otros procesamientos de datos para concluir la transacción comercial		
AI-11.1		Grabación de los resultados de la medición en un soporte duradero.	L1 - L8
AI-11.2		Prueba duradera del resultado de la medición e información necesaria para identificar la transacción.	L1, L6
AI-12	Evaluación de conformidad	Evaluación de conformidad fácil con los requisitos de la Directiva.	P1, P2, U1, U2, D2, D4
	Anexos del A1 al H1		
Del A1 al H1		Ningún requisito de las características de los instrumentos	
	Anexo MI-001		
Del MI-001-1 al MI-001-6		Irrelevante para el software	
MI-001-7.1.1, MI-001-7.1.2	Inmunidad electromagnética	Detección de fallos Funcionalidades para la generación de copias de seguridad Funcionalidades de restauración y reactivación	Del I1-1 al I1-3

MID			Guía de software
N.º de artículo/anexo (AI = Anexo I)	**Descripción**	**Comentario**	**N.º de requisito**
Del MI-001-7.1.3 al MI-001-9		Irrelevante para el software	
	Anexo MI-002		
Del MI-002-1 al MI-002-2		Irrelevante para el software	
MI-002-3.1	Inmunidad electromagnética	Detección de fallos Funcionalidades para la generación de copias de seguridad Funcionalidades de restauración y reactivación	Del I2-1 al I2-3
Del MI-002-3.1.3 al MI-002-5.1		Irrelevante para el software	
MI-002-5.2	Aptitud	Solución aceptable para controlar el periodo de vida de una batería	I2-7
MI-002-5.3	Aptitud	Resolución interna	I2-4
Del MI-002-5.4 al MI-002-8		Irrelevante para el software	
MI-002-5.5	Aptitud	Elemento de ensayo.	I2-9
Del MI-002-5.6 al MI-002-8		Irrelevante para el software	
MI-002-9.1	Dispositivos de conversión volumétrica Aptitud	Solución aceptable para controlar el convertidor del volumen de un gas	I2-8
Del MI-002-9.2 al MI-002-10		Irrelevante para el software	
	Anexo MI-003		
Del MI-003-1 al MI-003-4.2		Irrelevante para el software	
MI-003-4.3	Efecto permisible de los fenómenos electromagnéticos transitorios	Detección de fallos Funcionalidades para la generación de copias de seguridad Funcionalidades de restauración y reactivación	Del I3-1 al I3-3
MI-003-5.1		Irrelevante para el software	
MI-003-5.2	Aptitud	Resolución interna	I3-4
Del MI-003-5.3 al MI-003-7		Irrelevante para el software	
	Anexo MI-004		
Del MI-004-1 al MI-004-4.1		Irrelevante para el software	

MID			Guía de software
N.º de artículo/anexo (AI = Anexo I)	**Descripción**	**Comentario**	**N.º de requisito**
MI-004-4.2	Influencias permitidas de las perturbaciones electromagnéticas	Detección de fallos Funcionalidades para la generación de copias de seguridad Funcionalidades de restauración y reactivación	Del I4-1 al I4-3
Del MI-004-4.3 al MI-004-7		Irrelevante para el software	
	Anexo MI-005		
	Anexo MI-006		
MI-006-IV, MI-006-V	Totalizadores continuos y discontinuos	Detección de fallos Funcionalidades para la generación de copias de seguridad	Del I6-1 al I6-2
	Anexo MI-007		
	Anexo MI-008		
	Anexo MI-009		
	Anexo MI-010		

14 Referencias y Bibliografía

[1] Directiva 2004/22/CE del Parlamento Europeo y del Consejo de 31 de marzo de 2004 relativa a los instrumentos de medida Diario oficial de la Unión Europea L 135/1, 30/4/2004.
[2] *Software Requirements and Validation Guide*, versión 1.00, 29 de octubre de 2004, Red de Crecimiento Europeo sobre el software de la MID, número de contrato G7RT-CT-2001-05064, 2004.
[3] Requisitos de software según la MID, WEMEC 7.1, número 2, 2005.

15 Histórico de revisiones

Versión	Fecha	Cambios significativos
1	Mayo 2005	Primera versión de la guía
2	Abril 2007	• Adición y mejora de términos en la sección 2 • Cambios de redacción en secciones 4.1 y 5.1 • Modificación de una aclaración para la identificación del software de en la sección 4.2, requisito P2 y sección 5.2, requisito U2 • Enmienda en requisito L8, especificación de la nota 1 • Añadir una explicación al requisito S1, especificación 1 • Sustitución del requisito D5 por un recordatorio • Cambio de la clase de riesgo para sistemas de medición de líquidos distintos del agua • Cambio de las clases de riesgo para instrumentos de pesaje • Inclusión de varios cambios menores de redacción en el documento • Inclusión de esta tabla de revisiones
3	Marzo 2008	Inclusión de excepciones para la indicación de la identificación del software: nuevos requisitos I1-5, I2-9, I3-6, I4-5 e I5-1
4	Mayo 2009	• Eliminación de los últimos párrafos de la guía de validación de clases B y C de los requisitos P2 y U2 • Inclusión de aclaración para la aplicación de la descarga de software legalmente relevante, capítulo 9 Extensión D • Inclusión del punto 4 en especificaciones del requisito D2

Tabla 15.1 Histórico de revisiones

16 Índice alfabético

DOCUMENTO
INTERNACIONAL

OIML D 31

Edición 2008 (ES)

Requisitos generales para los instrumentos de medida controlados por software

---

OIML D 31 Edición 2008 (ES)

ORGANIZACIÓN INTERNACIONAL DE
METROLOGÍA LEGAL

ÍNDICE

Prólogo

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

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

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

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

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

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

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

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

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

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

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

Bureau International de Métrologie Légale

11, rue Turgot - 75009 París – Francia

Teléfono: 33 (0)1 48 78 12 82

Fax: 33 (0)1 42 82 17 27

E-mail: biml@oiml.org

Internet: www.oiml.org

Requisitos generales para los instrumentos de medida controlados por software

1. Introducción

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

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

2. Ámbito y campo de aplicación

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

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

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

Notas:

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

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

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

3. Terminología

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

3.1 Terminología general

3.1.1 Solución aceptable

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

3.1.2 Registro de actividades

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

3.1.3 Autenticación

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

3.1.4 Autenticidad

Resultado del proceso de autenticación (aceptado o rechazado).

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

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

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

3.1.6 Red cerrada

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

3.1.7 Comandos

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

3.1.8 Comunicación

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

3.1.9 Interfaz de comunicación

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

3.1.10 Certificado criptográfico

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

3.1.11 Métodos criptográficos

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

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

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

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

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

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

3.1.12 Dominio de datos

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

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

3.1.13 Parámetro específico del dispositivo

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

3.1.14 Durabilidad [OIML D 11:2004, 3.17]

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

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

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

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

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

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

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

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

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

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

3.1.18 Registro de errores

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

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

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

3.1.20 Suceso

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

3.1.21 Contador de sucesos

Contador no reiniciable que se incrementa con cada suceso nuevo.

3.1.22 Código ejecutable

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

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

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

3.1.24 Parte fija del software legalmente relevante

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

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

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

3.1.26 Integridad de los programas, los datos o los parámetros

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

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

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

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

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

3.1.29 Legalmente relevante

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

3.1.30 Parámetro legalmente relevante

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

---

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

3.1.31 Parte legalmente relevante del software

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

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

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

3.1.33 Instrumento de medida [VIM:1994, 4.1]

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

3.1.34 Medición continua/ discontinua

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

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

3.1.35 Red abierta

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

3.1.36 Funcionamiento [OIML D 11:2004, 3.16]

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

3.1.37 Código del programa

«Código fuente» o «código ejecutable».

3.1.38 Precintado

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

3.1.39 Protección

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

3.1.40 Software

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

3.1.41 Examen del software

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

3.1.42 Identificación del software

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

3.1.43 Interfaz software

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

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

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

3.1.45 Protección del software

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

3.1.46 Separación del software

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

3.1.47 Código fuente

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

3.1.48 Dispositivo de almacenamiento

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

3.1.49 Subconjunto [OIML D 11:2004, 3.3]

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

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

3.1.50 Ensayo [OIML D 11:2004, 3.20]

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

3.1.51 Registro de fecha y hora

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

3.1.52 Transmisión de datos de medida

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

3.1.53 Parámetro específico del modelo

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

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

3.1.54 Ordenador universal

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

3.1.55 Interfaz de usuario

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

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

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

3.1.57 Verificación [V 1:2000, 2.13]

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

3.2 Listado de siglas

EUT Equipo sometido a ensayo

IEC Comisión Electrotécnica Internacional

E/S Entrada/Salida (puertos)

ISO Organización Internacional de Normalización

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

TIC Tecnologías de la información y de las comunicaciones

EMP Error máximo permitido

OIML Organización Internacional de Metrología Legal

PCB Placa de circuito impreso

PIN Número de identificación personal

TC Comité técnico (OIML)

SC Subcomité (OIML)

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

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

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

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

5. Requisitos de las aplicaciones software de instrumentos de medida

5.1 Requisitos generales

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

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

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

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

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

5.1.1 Identificación del software

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

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

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

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

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

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

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

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

La correspondiente Recomendación OIML debe permitir o desestimar esta excepción.

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

Ejemplo:

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

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

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

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

5.1.2 Adecuación de algoritmos y funciones

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

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

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

5.1.3 Protección del software

5.1.3.1 Prevención del uso incorrecto

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

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

Ejemplo:

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

5.1.3.2 Protección contra el fraude

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

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

Ejemplo:

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

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

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

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

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

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

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

Ejemplo:

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

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

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

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

Ejemplo:

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

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

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

Ejemplo:

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

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

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

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

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

5.1.4 Características de hardware

5.1.4.1 Detección de fallos

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

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

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

Ejemplo:

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

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

El CRC16 constituye un algoritmo de suma de comprobación aceptable.

5.1.4.2 Protección de durabilidad

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

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

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

Ejemplo:

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

5.2 Requisitos específicos para las configuraciones

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

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

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

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

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

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

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

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

5.2.1.1 Separación de dispositivos electrónicos y subconjuntos

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

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

Ejemplo:

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

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

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

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

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

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

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

Ejemplo:

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

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

5.2.1.2. Separación de partes del software

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

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

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

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

Ejemplo:

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

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

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

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

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

Ejemplo:

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

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

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

Ejemplos:

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

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

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

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

5.2.2 Indicaciones compartidas

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

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

Ejemplo:

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

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

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

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

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

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

Ejemplo:

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

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

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

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

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

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

Ejemplo:

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

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

Ejemplo:

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

5.2.3.4 Almacenamiento automático

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

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

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

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

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

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

5.2.3.4.b Se pueden eliminar los datos almacenados si:

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

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

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

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

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

5.2.3.5 Retraso en la transmisión

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

5.2.3.6 Interrupción de la transmisión

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

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

Ejemplo:

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

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

5.2.3.7 Registro de fecha y hora

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

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

Ejemplo:

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

5.2.4 Compatibilidad de los sistemas operativos y del hardware, portabilidad

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

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

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

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

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

5.2.5 Conformidad de los dispositivos fabricados con el modelo aprobado

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

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

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

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

(d) identidad del «código ejecutable íntegro».

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

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

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

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

5.2.6 Mantenimiento y reconfiguración

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

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

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

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

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

5.2.6.2 Actualización verificada

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

5.2.6.3 Actualización rastreada

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

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

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

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

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

Ejemplo:

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

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

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

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

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

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

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

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

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

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

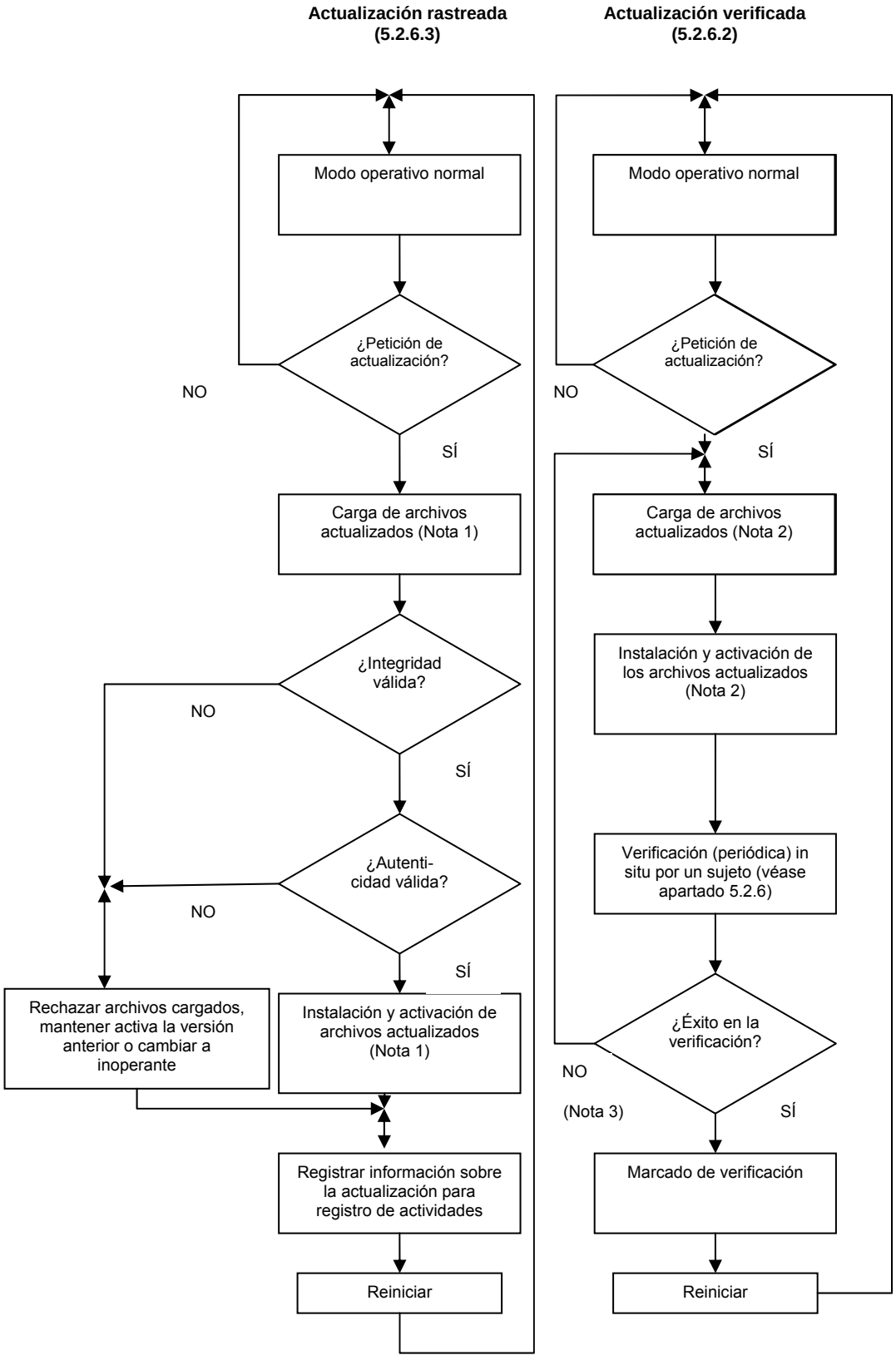

Figura 1 Procedimiento de actualización del software

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

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

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

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

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

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

6 Aprobación de modelo

6.1 Documentación necesaria para la aprobación de modelo

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

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

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

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

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

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

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

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

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

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

- manual de uso.

6.2 Requisitos del procedimiento de aprobación de modelo

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

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

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

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

6.3 Métodos de validación (examen del software)

6.3.1 Visión general de los métodos y su aplicación

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

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

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

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

6.3.2 Descripción de los métodos de validación seleccionados

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

Aplicación:

Se trata del procedimiento básico aplicable en cualquier situación.

Condiciones previas:

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

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

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

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

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

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

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

Descripción:

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

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

Resultado

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

Procedimientos complementarios:

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

Referencias:

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

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

Aplicación:

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

Condiciones previas:

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

Descripción:

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

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

Resultado:

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

Procedimientos complementarios:

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

Referencias:

Varias Recomendaciones OIML específicas.

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

Aplicación:

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

Condiciones previas:

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

Descripción:

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

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

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

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

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

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

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

Resultado:

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

Procedimientos complementarios:

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

Referencia:

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

6.3.2.4 Análisis del flujo de datos metrológicos (DFA)

Aplicación:

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

Condiciones previas:

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

Descripción:

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

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

Resultado:

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

Procedimientos complementarios:

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

Referencia:

IEC 61131-3.

6.3.2.5 Inspección y revisión del código (CIWT)

Aplicación:

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

Condiciones previas:

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

Descripción:

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

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

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

Resultado:

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

Procedimientos complementarios:

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

Referencia:

IEC 61508-7:2000 – 3 [9].

6.3.2.6 Ensayo de módulo del software (SMT)

Aplicación:

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

Condiciones previas:

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

Descripción:

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

Resultado:

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

Procedimientos complementarios:

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

Referencia:

IEC 61508-7:2000 – 3 [9].

6.4 Procedimiento de validación

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

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

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

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

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

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

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

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

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

6.5 Equipo sometido a ensayo (EUT)

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

7 Verificación

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

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

La verificación del software incluirá:

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

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

8. Evaluación de los niveles de (riesgo) severidad

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

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

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

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

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

(a) el riesgo de fraude:

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

(b) la conformidad requerida:

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

(c) la fiabilidad requerida:

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

(d) el interés del defraudador:

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

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

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

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

Anexo A

Bibliografía

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

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

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

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

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

(se pueden descargar archivos PDF gratuitamente).

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

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

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

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

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

Anexo B

Ejemplo de informe de evaluación de un software (Informativo)

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

Informe de ensayo nº XYZ122344

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

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

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

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

Objeto del ensayo

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

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

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

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

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

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

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

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

El código fuente contiene los siguientes archivos legalmente relevantes:

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

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

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

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

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

Realización de la validación

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

Se validaron los siguientes requisitos:

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

Se aplicaron los siguientes métodos de validación:

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

Resultado

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

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

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

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

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

Conclusión

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

National Testing & Measurement Lab.

Software Department

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

Director técnico Responsable técnico

Lista de comprobación

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

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

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

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

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

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

Anexo C

Índice

NIPO 706-10-013-3