WELMEC 7.2

2019

WELMEC

Organizace pro evropskou spolupráci
v legální metrologii

Softwarová příručka

(SMĚRNICE MID 2014/32/EU[1])

WELMEC

Organizace pro evropskou spolupráci
v legální metrologii

WELMEC je organizace zajišťující spolupráci v oblasti legální metrologie mezi členskými státy EU a členy EFTA.

Tento dokument je jedním z řady příruček organizace WELMEC sloužících jako pomůcka pro výrobce měřicích přístrojů a pro notifikované osoby odpovědné za posuzování shody výrobků.

Příručky organizace WELMEC mají pouze doporučující charakter, nepředstavují žádná omezení a nepředepisují žádné technické požadavky nad rámec požadavků stanovených příslušnými normami EU.

Ačkoliv existují i jiné možné přístupy a řešení, doporučení v tomto dokumentu představují stanoviska členů WELMEC jako nejvhodnější přístupy k následování.

This document is a translation of WELMEC Guide 7.2: Software Guide (Measuring Instruments 2014/32/EU) also applicable to 2004/22/EU (Version 2019).
The translation has been prepared by members of the WELMEC Working Group 7.
In case of any inconsistency between the terms of the translation and the terms of the original document the original document shall prevail.

Vydal:
Sekretariát WELMEC

E-mail : secretary@welmec.org
Web: www.welmec.org

Obsah

Předmluva

Tato příručka vychází z dokumentu “Software Requirements and Validation Guide”, verze 1.00 z 29. října 2004, vypracovaného v rámci projektu sítě European Growth Network “*MID-Software”.* Projekt se uskutečnil s podporou Evropské komise pod registračním číslem G7RT-CT-2001-05064 a probíhal od ledna 2002 do prosince 2004.

Příručka má pouze povahu doporučení, nepředstavuje žádná omezení a nepředepisuje žádné technické požadavky nad rámec směrnice MID. Ačkoliv existují i jiné možné přístupy a řešení, doporučení v tomto dokumentu představují osvědčenou praxi, vycházející ze zkušeností WELMEC, kterou je vhodné následovat.

Přestože se příručka zaměřuje na přístroje obsažené ve směrnici MID, doporučení v ní uvedená mají obecnou platnost a lze je aplikovat i v jiných oblastech.

Verze 2015 odpovídá nejnovějším poznatkům, které byly získány při používání předchozích verzí příručky.

[1]**Upozornění**: Toto vydání příručky platí rovněž pro směrnici 2004/22/ES.

Úvod

Tato technická příručka se zabývá aplikací směrnice MID, a to na měřicí přístroje vybavené softwarem. Je určená všem, kteří chtějí porozumět technickým požadavkům směrnice MID na software, především pak základním požadavkům uvedeným v příloze 1 této směrnice. Její míra podrobností je zaměřena na potřeby výrobců měřicí techniky a požadavky notifikovaných osob zabývajících se posouzením shody měřicích přístrojů dle modulu B.

Postupováním podle této příručky splníte požadavky směrnice MID na software měřicích přístrojů. Všechny notifikované osoby tuto příručku přijímají jako vyhovující výklad směrnice MID v otázkách týkajících se softwaru. Provázanost mezi požadavky uvedenými v tomto dokumentu a požadavky směrnice MID je znázorněna v křížových odkazech, které tvoří přílohu tohoto dokumentu (kapitola 12).

Nejnovější informace o příručkách a o činnosti pracovní skupiny WELMEC WG 7 naleznete na adrese www.welmec.org.

1 Terminologie

Níže jsou vysvětleny pojmy ve významu použitém v této příručce. Pokud byly definice či jejich zásadní části převzaty z nějaké normy či z jiného zdroje, je to uvedeno v odkazu.

Přijatelné řešení (Acceptable solution): Návrh nebo princip softwarového modulu nebo hardwarové jednotky nebo jejich prvku, které jsou v souladu s určitým požadavkem. Přijatelné řešení je příkladem, jak je možné vyhovět určitému požadavku. Nevylučuje jiná řešení, jež mohou rovněž danému požadavku vyhovovat.

Prokázání věrohodnosti (Authentication): Ověření a potvrzení deklarované nebo tvrzené identity uživatele, procesu nebo zařízení.

Autentičnost (Authenticity): Pravost a schopnost prokázat pravdivost a důvěryhodnost [4].

Základní konfigurace (Basic configuration): Koncepce *měřicího přístroje* s ohledem na základní architekturu. Rozlišují se dvě základní konfigurace*: jednoúčelové měřicí přístroje a měřicí přístroje využívající počítač.* Tyto pojmy lze použít i pro *podsestavy.*

Jednoúčelový měřicí přístroj (typ P) (Built-for-purpose measuring instrument): *Měřicí přístroj* vyrobený k jednomu konkrétnímu účelu. Celý aplikační software je tedy určen pro účely měření. Podrobnější definici naleznete v podkapitole 4.1.

Uzavřená síť (Closed network): Síť s pevným počtem účastníků, jejichž identita, funkce a umístění jsou známy (viz též *otevřená síť*).

Komunikační rozhraní (Communication interface): Elektronické, optické, radiové nebo jiné technické rozhraní umožňující automatické předávání informací mezi *měřicími přístroji, podsestavami* nebo externími přístroji nebo jejich částmi.

Specifické parametry přístroje (Device-specific parameter): *Legálně relevantní parametry*, jejichž hodnota se liší podle konkrétního přístroje. Mezi specifické parametry přístroje patří kalibrační parametry (např. nastavení rozsahu nebo jiné nastavení či korekce) a konfigurační parametry (např. maximální hodnota, minimální hodnota, jednotky měřené veličiny atd.). Tyto parametry lze nastavit nebo vybrat pouze pokud je přístroj ve speciálním operačním režimu. Specifické parametry přístroje lze rozdělit na parametry, které je nutné zabezpečit (tj. nelze je měnit) a na parametry, které mohou být přístupné (nastavitelné parametry) při provozu přístroje.

Čítač událostí: Čítač událostí zaznamenává každou změnu hodnoty parametru. Slouží jako prostředek kontroly změn.

Záznamník událostí: Záznamník událostí zaznamenává každou změnu softwaru nebo parametru. Slouží jako prostředek kontroly změn. Zaznamenáno je minimálně označení změněné položky.

Integrovaná paměť (Integrated storage): Paměť, která je nedílnou součástí měřicího přístroje, např. RAM, EEPROM, pevný disk.

Integrita dat a softwaru (Integrity of data and software): Ujištění, že v datech ani v softwaru nebyly při užívání, přenosu ani během uložení provedeny žádné změny.

Konfigurace IT (IT configuration): Koncepce *měřicího přístroje* s ohledem na IT funkce a vlastnosti. Tato příručka popisuje čtyři různé IT konfigurace: *dlouhodobé uložení naměřených dat*, *přenos naměřených dat*, *stahování softwaru* a *oddělení softwaru* (viz též *Základní konfigurace*). Tato ustanovení platí rovněž pro podsestavy.

Legálně relevantní parametr (Legally relevant parameter): Parametr *měřicího přístroje* nebo *podsestavy,* který podléhá kontrole z hlediska legální metrologie.

Rozlišují se tyto typy legálně relevantních parametrů: *specifické parametry daného typu a specifické parametry přístroje.*

Legálně relevantní software (Legally relevant software): Část softwaru včetně specifických *parametrů daného* typu, která plní funkce podléhající kontrole z hlediska legální metrologie. Veškerý další software se označuje jako legálně nerelevantní. S naměřenými daty vygenerovanými přístrojem nebo zpracovanými legálně relevantním softwarem se nakládá samostatně a nepovažují se za součást legálně relevantního softwaru.

Označení legálně relevantního softwaru (Legally relevant software identifier): Prvky, které identifikují legálně relevantní software, se nazývají *označení legálně relevantního softwaru.*

Dlouhodobé uložení naměřených dat (Long-term storage of measurement data): Uložení naměřených dat po skončení měření pro jejich pozdější použití k legálně relevantním účelům.

Naměřená data (Measurement data): Naměřené hodnoty vygenerované či zpracované měřicími přístroji s uvedením fyzikálních jednotek a dalších informací (např. časového razítka), které jsou s nimi řádně spojené a charakterizují je z metrologického hlediska.

Měřicí přístroj (Measuring instrument): Jakýkoli přístroj nebo systém, který má funkci měření. Pokud nemůže dojít k záměně, vynechává se v textu přívlastek „měřicí“. [MID, článek 4]

Měřicí přístroje využívající univerzální počítač (typ U) (Measuring instruments using a universal computer): *Měřicí přístroj* založený na víceúčelovém počítači (zpravidla se jedná o systém na bázi PC) určený k zajišťování legálně relevantních funkcí. Přístroj typu U je jakýkoliv přístroj nesplňující podmínky pro *jednoúčelový měřicí přístroj (typ P)*.

Otevřená síť (Open network): Síť libovolných účastníků (zařízení s libovolnými funkcemi). Počet, identita i umístění účastníků se mohou dynamicky měnit a mohou být pro ostatní účastníky neznámé (viz též *Uzavřená síť).*

Operační systém (Operating System): Soubor softwarových a firmwarových prvků řídících fungování počítačových programů a zajišťujících služby jako je alokace zdroje počítače, řízení procesů, vstupů a výstupů a práce se soubory v systému počítače [5].

Ochranné softwarové rozhraní (Protective Software Interface): Rozhraní mezi legálně relevantním a legálně nerelevantním softwarem, podmínky zabezpečení viz rozšíření S3.

Třída rizika (Risk class): Třída typů *měřicích přístrojů* s téměř stejně vyhodnocenými riziky.

Stahování softwaru (Software download): Proces automatického přenosu softwaru do cílového *měřicího přístroje* nebo hardwarové jednotky pomocí jakýchkoli technických prostředků z místního nebo vzdáleného zdroje (např. vyměnitelné paměťové médium, přenosný počítač, vzdálený počítač) přes jakékoliv spojení (např. přímé spojení, sítě apod.)

Označení softwaru (Software identifier): Sekvence znaků, které identifikují software. Toto označení se lokálně považuje za součást softwaru.

Oddělení softwaru (Software separation): Jednoznačné oddělení *legálně relevantního softwaru* od legálně nerelevantního softwaru. Pokud software není takto oddělen, pak je celý software považován za legálně relevantní.

Podsestava (Sub-assembly): Samostatná část měřidla; hardwarové zařízení (hardwarová jednotka), která funguje nezávisle a která tvoří *měřicí přístroj* spolu s dalšími podsestavami (nebo měřicím přístrojem), s nimiž je kompatibilní [MID, článek 4].

Přenos naměřených dat (Transmission of measurement data): Přenos naměřených dat přes komunikační sítě nebo jinými způsoby do vzdáleného zařízení, kde se data dále zpracovávají a/nebo se používají pro účely regulované legislativou.

TEC (TEC): Certifikát schválení typu.

Specifické parametry daného typu (Type-specific parameter): *Legálně relevantní parametry,* jejichž hodnota je stejná u všech přístrojů daného typu. Specifický parametr daného typu se považuje za součást legálně relevantního softwaru.

Uživatelské rozhraní (User interface): Rozhraní tvořící součást měřicího přístroje nebo měřicího systému umožňující předávání informací mezi člověkem a měřicím přístrojem nebo částmi jeho hardwaru či softwaru. Uživatelské rozhraní je např. vypínač, klávesnice, myš, displej, monitor, tiskárna nebo dotyková obrazovka.

Validace (Validation): Potvrzení přezkoušením a poskytnutím objektivního důkazu (např. informace, jejíž pravdivost lze dokázat skutečnostmi získanými pozorováním, měřením, zkouškou apod.), že byly splněny specifické požadavky na zamýšlené použití. V tomto případě jsou to požadavky uvedené ve směrnici MID.

Níže uvedené definice jsou konkrétnější. Tyto termíny jsou použity pouze v některých rozšířeních a u tříd rizika D nebo vyšších.

Hashovací algoritmus (Hash algorithm): Algoritmus, který zkomprimuje obsah bloku dat do hexadecimálního čísla o definované délce (hash kód), takže v praxi se při změně jediného bitu vygeneruje jiný hash kód. Hashovací algoritmy se vybírají tak, aby byla teoreticky nízká pravděpodobnost, že dva různé bloky dat budou míst stejný hash kód.

Algoritmus podpisu (Signature algorithm): Šifrovací algoritmus, který provádí zašifrování (zakódování) pomocí kódovacího *klíče* a který umožňuje dekódování zakódovaného hash kódu, pokud je k dispozici příslušný *dekódovací klíč*.

Klíč: Přidělené číslo nebo sekvence znaků k zakódování anebo dekódování informace.

Systém s veřejným klíčem (PKS) (Public Key System): Dvojice dvou různých *klíčů*, z nichž jeden se nazývá soukromý klíč a druhý veřejný klíč. *Pro ověření integrity a autentičnosti* informace se hash hodnota informace vygenerované *hashovacím algoritmem* zakóduje pomocí soukromého klíče odesílatele, čímž se vytvoří podpis, který následně příjemce dekóduje pomocí veřejného klíče odesílatele.

Infrastruktura s veřejným klíčem (PKI) (Public Key Infrastructure): Organizace garantující důvěryhodnost *systému s veřejným klíčem*. Toto zahrnuje i vystavování a doručování digitálních certifikátů všem členům, kteří se výměny informací účastní.

Certifikace klíčů (Certification of keys): Proces propojení hodnoty veřejného klíče s jednotlivcem, organizací nebo jiným subjektem.

Elektronický podpis (Electronic signature): Krátký kód (podpis), který je jedinečným způsobem přiřazen k textu, bloku dat nebo binárnímu softwarovému souboru, aby byla doložena *integrita* a *autentičnost* uložených nebo přenášených dat. Tento podpis se generuje pomocí *algoritmu podpisu* a soukromého *klíče.* Vytváření elektronického podpisu je zpravidla rozděleno do dvou kroků: (1) nejprve *hashovací algoritmus* zkomprimuje obsah informace k podpisu do krátkého čísla a (2) poté algoritmus podpisu toto číslo zkombinuje se soukromým klíčem pro vytvoření podpisu.

Trust centrum (Trust Centre): Asociace, která důvěryhodným způsobem generuje, uchovává a vydává informace o autentičnosti veřejných klíčů osob nebo jiných subjektů, např. měřicích přístrojů.

2 Jak tuto příručku používat

V této kapitole je popsána struktura příručky a je zde vysvětleno, jak dokument používat.

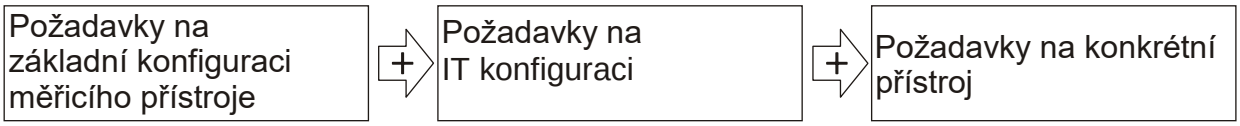
2.1 Celková struktura příručky

Příručka je koncipována jako strukturovaná sada požadavků. Struktura příručky následuje členění měřicích přístrojů podle základních konfigurací a tzv. IT konfigurací. Obecné požadavky jsou doplněny o požadavky na konkrétní přístroje.

Příručka tedy obsahuje tři základní typy požadavků:

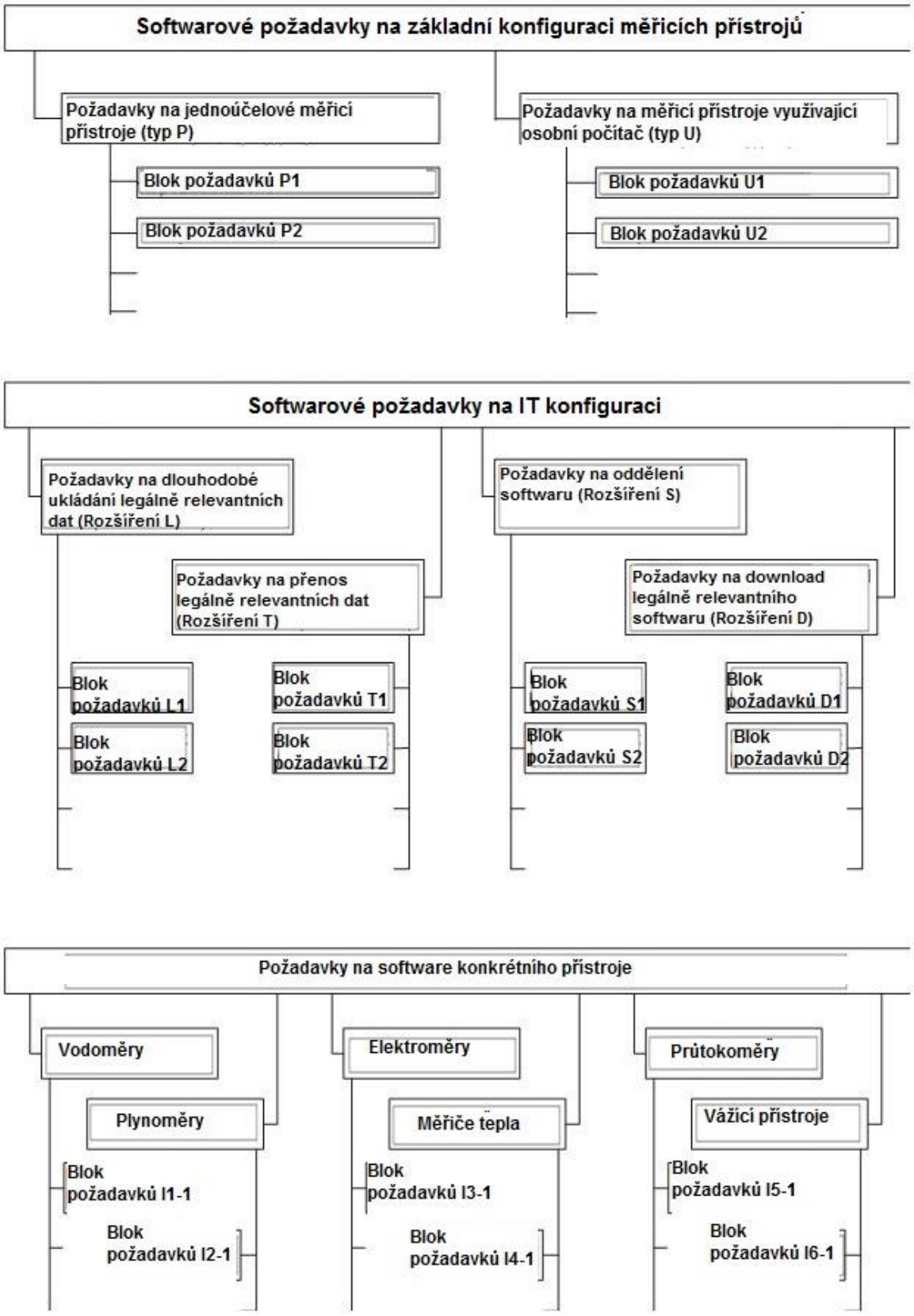
1. požadavky na dvě základní konfigurace měřicích přístrojů (tzv. přístroje typu P a typu U),
2. požadavky na čtyři IT konfigurace (tzv. rozšíření L, T, S a D)
3. požadavky na konkrétní přístroje (tzv. rozšíření I.1, I.2 atd.)

Požadavky prvního typu se vztahují na všechny měřicí přístroje. Požadavky druhého typu se týkají následujících IT funkcí: dlouhodobého uložení naměřených dat (L), přenosu naměřených dat (T), stahování softwaru (D) a oddělení softwaru (S). Každou sadu požadavků je třeba aplikovat pouze tehdy, pokud daná funkce existuje. Posledním typem jsou požadavky na konkrétní přístroje. Jejich číslování je shodné s číslováním příloh s požadavky na jednotlivé přístroje ve směrnici MID. Postup aplikování požadavků vztahujících se na daný měřicí přístroj je schematicky znázorněn na obrázku **2-1**.



Obrázek 2-1: Typy požadavků vztahujících se na konkrétní měřicí přístroj.

Schéma následujícího obrázku **2-2** znázorňuje stávající sady požadavků.



Obrázek 2-2: Schéma skupin požadavků

Kromě výše popsané struktury jsou požadavky v této příručce dále rozděleny podle tříd rizik. Popsáno je šest tříd rizik označených A až F, přičemž A představuje nejnižší předpokládané riziko. Nejnižší třída rizika A a nejvyšší třídy rizika E a F se v současné době pro přístroje regulované směrnicí MID nepoužívají. Byly zavedeny pouze pro případ, že by byly potřebné v budoucnu. Zbývající třídy rizika B až D pokrývají veškeré třídy měřicích přístrojů, na něž se vztahuje směrnice MID. Celá škála tříd rizika (A až F) nicméně poskytuje dostatečný prostor pro případné změny hodnocení rizik. Třídy jsou definovány v kapitole 3 této příručky.

Každý měřicí přístroj bude zařazen do jedné třídy rizika, neboť příslušné specifické požadavky na software jsou určeny třídou rizika daného přístroje.

2.2 Jak se orientovat v této příručce

Tuto přehlednou softwarovou příručku lze použít pro celou řadu měřicích přístrojů. Příručka má modulární podobu. Budete-li postupovat podle níže uvedených pokynů, snadno naleznete příslušné skupiny požadavků vztahující se na konkrétní přístroj.

Krok 1: *Výběr základní konfigurace (P nebo U)*

Na přístroj se v závislosti na základní konfiguraci přístroje bude vztahovat pouze jedna ze dvou sad požadavků. Zvolte tedy typ základní konfigurace odpovídající danému přístroji: jednoúčelový měřicí přístroj se zabudovaným softwarem (typ P, viz podkapitola 4.1), nebo měřicí přístroj využívající univerzální počítač (typ U, viz podkapitola 5.1). Pokud se nejedná o celý přístroj, ale pouze o jeho podsestavu, zvolte konfiguraci pro podsestavu. Použijte úplnou sadu požadavků definovanou pro příslušnou základní konfiguraci.

Krok 2: *Výběr příslušných IT konfigurací (rozšíření L, T, S a D)*

Tyto IT konfigurace zahrnují následující funkce: dlouhodobé uložení naměřených dat (L), přenos naměřených dat (T), oddělení softwaru (S) a stažení legálně relevantního softwaru (D). Příslušné skupiny požadavků (tzv. „rozšíření modulu“) jsou na sobě zcela nezávislé. Skupina požadavků je vybrána pouze na základě IT konfigurace. Skupina požadavků uvedená ve zvoleném rozšíření musí být aplikována v celém rozsahu. Zjistěte, jaká rozšíření jsou pro daný přístroj relevantní a použijte je (viz obr. 2-2).

Krok 3: *Výběr specifických požadavků na konkrétní měřicí přístroj (rozšíření I)*

Za pomoci příslušného rozšíření (I.x) vyberte pro daný druh měřicího přístroje příslušnou skupinu požadavků a aplikujte je (viz Obrázek 2-2).

Krok 4: *Výběr příslušné třídy rizika (rozšíření I)*

Na základě definic uvedených v rozšíření pro konkrétní měřicí přístroje (I.x, podkapitola I.x.6) zvolte třídu rizika. Třídy rizika jsou zde definovány jednotně pro každou třídu měřicích přístrojů, nebo podle dalšího členění do kategorií, rozsahu platnosti apod.

Jakmile určíte příslušnou třídu rizika, je třeba zohledňovat pouze odpovídající požadavky a postup validace.

2.3 Jak pracovat se skupinami požadavků

Každá skupina požadavků obsahuje jeden jasně definovaný požadavek. Tvoří ho text definice, upřesňující vysvětlivky, potřebná dokumentace, postup validace a příklady přijatelných řešení (jsou-li k dispozici). Obsah jednotlivých bloků lze dále rozdělit podle tříd rizika. Na obrázku **2-3** je uvedeno schématické znázornění bloku požadavků.

<table>
<tr><td colspan="3">Název požadavku</td></tr>
<tr><td colspan="3">Hlavní obsah požadavku</td></tr>
<tr><td colspan="3">Doplňující údaje (rozsah platnosti, doplňující vysvětlení, výjimky apod.)</td></tr>
<tr><td colspan="3">Potřebná dokumentace (případně rozdělená na třídy rizika)</td></tr>
<tr><td>Postup validace pro jednu třídu rizika</td><td>Postup validace pro další třídu rizika</td><td>...</td></tr>
<tr><td>Příklad přijatelného řešení pro jednu třídu rizika</td><td>Příklad přijatelného řešení pro další třídu rizika</td><td>...</td></tr>
</table>

Obrázek 2-3: Struktura bloku požadavků

Blok požadavků zahrnuje technický obsah požadavku včetně postupu validace. Je určen jak pro výrobce, tak pro notifikovanou osobu a to ve dvou bodech: (1) zvážit požadavek jako minimální podmínku a (2) neklást další nároky nad tento rámec.

Poznámky pro výrobce:

- Dodržujte hlavní obsah požadavku a další upřesňující údaje.
- Poskytněte požadovanou dokumentaci.
- Přijatelná řešení jsou příklady, jak lze požadavku vyhovět. Není povinné se jimi řídit.
- Postup validace má informativní charakter.

Poznámky pro notifikované osoby:

- Dodržujte hlavní obsah požadavku a další upřesňující údaje.
- Dodržujte postup validace.
- Zkontrolujte, zda je předložená dokumentace úplná.

2.4 Jak pracovat s kontrolními seznamy

Kontrolní seznamy jsou pomůckou, jak se ujistit, že výrobce nebo zkoušející splnili všechny požadavky uvedené v konkrétní kapitole. Jsou součástí protokolu o zkoušce. Upozorňujeme, že tyto kontrolní seznamy představují pouze shrnutí a nerozlišují jednotlivé třídy rizika. Kontrolní seznamy nenahrazují definice požadavků. Úplný popis je uveden u jednotlivých bloků požadavků.

Postup:

- Použijte potřebné kontrolní seznamy podle pokynů uvedených v krokách 1, 2 a 3 podkapitoly 2.2.
- Projděte všechny kontrolní seznamy a zkontrolujte, zda byly veškeré požadavky splněny.
- Vyplňte kontrolní seznamy dle pokynů.

3 Definice tříd rizika

3.1 Obecný princip

Specifické požadavky uvedené v této příručce jsou rozděleny podle tříd rizika (softwaru), přičemž jsou brána v potaz pouze rizika související se softwarem měřicích přístrojů, nikoliv dalších komponent. Z praktických důvodů může být v této příručce používán termín „třída rizika“ i synonymní označení „riziková třída“. Každý měřicí přístroj musí být zařazen do určité třídy rizika, neboť příslušné specifické požadavky na software jsou dané právě třídou rizika, do níž měřicí přístroj spadá.

Rizika softwaru v měřicích přístrojích, jimiž se tato příručka zabývá, jsou zpravidla daná třemi rizikovými faktory, jimiž je: nedostatečné zabezpečení softwaru, nedostatečné přezkoušení softwaru a neshoda s typem. Každý z těchto tří faktorů představuje určitý stupeň rizika, jejichž kombinací pak vzniká třída rizika, ve které je stupeň rizikových faktorů nepřímo definován stupněm nutných bezpečnostních opatření. Ke každému z výše uvedených rizikových faktorů byly vyvinuty tři úrovně ochrany: nízká, střední a vysoká. Čím vyšší je předpokládané riziko, tím vyšší bude i úroveň ochrany.

3.2 Popis úrovní ochrany před rizikovými faktory

Jednotlivé úrovně jsou definovány následujícím způsobem:

Úroveň zabezpečení softwaru

Nízká: Nejsou nutné žádné zvláštní prostředky ochrany proti záměrným změnám.

Střední: Software je chráněný proti záměrným změnám, které by mohly způsobit snadno dostupné a běžné softwarové nástroje (např. textové editory).

Vysoká: Software je chráněný proti záměrným změnám, které by mohly způsobit sofistikované softwarové nástroje (ladicí programy a harddiskové editory, nástroje na vývoj softwaru apod.).

Úroveň přezkoušení softwaru

Nízká: Provádí se standardní přezkoušení typu včetně testu funkčnosti měřicího přístroje. Není požadováno další testování softwaru.

Střední: Oproti nízké úrovni se software testuje na základě dokumentace. Dokumentace obsahuje popis funkcí softwaru, popis parametrů apod. Provádějí se praktické testy (náhodně vybraných) funkcí softwaru pro kontrolu věrohodnosti dokumentace a kontrolu efektivity prostředků ochrany.

Vysoká: Oproti střední úrovni se navíc provádí hloubkový test softwaru, zpravidla na základě zdrojového kódu.

Úroveň shody softwaru

Nízká: Legálně relevantní software jednotlivých přístrojů se považuje za shodný s legálně relevantním softwarem zkoušeného typu, pokud funkce softwaru odpovídají technické dokumentaci daného typu. Binární kód softwaru nemusí být totožný se softwarem daného typu.

Střední: Oproti nízké úrovni shody musí být v tomto případě binární kód legálně relevantního softwaru každého jednotlivého přístroje totožný se softwarem zkoušeného (či přezkušovaného) typu. Oddělení softwaru je povoleno, pokud jsou splněny podmínky uvedené v části S této příručky (kapitola 8).

Vysoká: Binární kód celého softwaru implementovaného do jednotlivých přístrojů je totožný se softwarem zkoušeného typu. Oddělení softwaru již není možné.

3.3 Odvození tříd rizika

Z 27 teoreticky možných kombinací úrovní se v praxi uplatňují pouze tři, nanejvýše 6 kombinací (rizikové třídy B, C, D a případně A, E a F). Pokrývají veškeré třídy přístrojů, na něž se vztahují ustanovení směrnice MID. Navíc poskytují dostatečný prostor v případě změněného posuzování rizik. Třídy jsou definovány v tabulce níže. Tabulku je třeba vykládat tak, že určitá třída rizika odpovídá kombinaci různých úrovní potřebných bezpečnostních opatření.

Třída rizika	Zabezpečení softwaru	Přezkoušení softwaru	Shoda softwaru
A	*nízká*	*nízká*	*nízká*
B	*střední*	*střední*	*nízká*
C	*střední*	*střední*	*střední*
D	*vysoká*	*střední*	*střední*
E	*vysoká*	*vysoká*	*střední*
F	*vysoká*	*vysoká*	*vysoká*

Tabulka 3-1: *Definice tříd rizika*

3.4 Popis jednotlivých tříd rizika

Třída rizika A: Jedná se o nejnižší třídu rizika. Nejsou požadována žádná zvláštní opatření proti záměrným změnám softwaru. Přezkoušení softwaru je součástí testu funkčnosti přístroje. Shoda je požadovaná na úrovni dokumentace. Neočekává se, že bude nějaký přístroj zařazen do třídy rizika A. Třída rizika A nicméně byla zavedena proto, aby i tato možnost zůstala otevřená.

Třída rizika B: Oproti třídě rizika A je u třídy rizika B požadována úroveň zabezpečení softwaru na střední úrovni. Úroveň přezkoušení tedy musí být také na střední úrovni. Shoda zůstává stejná jako u třídy rizika A.

Přezkoušení softwaru se provádí na základě dokumentace. Certifikát o schválení typu proto při uvádění přístrojů na trh připouští různé implementace k jedné dokumentaci [1].

Třída rizika C: V porovnání s třídou rizika B je požadována shoda na „střední“ úrovni. To znamená, že binární kód legálně relevantního softwaru jednotlivých přístrojů je totožný se softwarem zkoušeného typu. Úroveň zabezpečení a úroveň přezkoušení zůstávají stejné jako u třídy rizika B.

Třída rizika D: Podstatný rozdíl oproti třídě rizika C tkví ve zvýšení úrovně zabezpečení na úroveň „vysoká“. Úroveň přezkoušení zůstává stále „střední“, proto musí být poskytnuta dokumentace s dostatečnou vypovídací hodnotou, na základě níž je možné prokázat, že byly implementovány vhodné prostředky zabezpečení. Úroveň shody zůstává stejná jako u třídy rizika C.

Třída rizika E: Oproti třídě rizika D je požadována „vysoká“ úroveň přezkoušení. Úrovně zabezpečení a shody se nemění.

Třída rizika F: Z hlediska všech rizikových faktorů (zabezpečení, přezkoušení a shody softwaru) je požadována úroveň „vysoká“. Rozdíl oproti třídě E spočívá v tom, že software přístroje neobsahuje žádný legálně nerelevantní software.

[1] Po uvedení přístroje na trh se tolerance změny softwaru řídí národními právními předpisy.

4 Základní požadavky na vestavěný software v jednoúčelových měřicích přístrojích (typ P)

Soubor specifických požadavků popsaných v této kapitole se vztahuje na jednoúčelové měřicí přístroje, jakož i na podsestavy a části podle příručky WELMEC 8.8 (Modulární hodnocení měřicích přístrojů) sloužící jednomu účelu. Ustanovení zde uvedená se na takové podsestavy a části vztahují i tehdy, když to v následujícím textu není opakovaně zdůrazněno. Součástí této příručky nicméně nejsou podmínky samostatného přezkušování podsestav a částí ani podmínky akceptace příslušných certifikátů.

Pokud měřicí přístroj využívá univerzální počítač (víceúčelové PC), je třeba se řídit souborem specifických požadavků uvedených v kapitole 5 pro přístroje typu U. Specifické požadavky na přístroje typu U se vztahují i na jednoúčelové měřicí přístroje, které nesplní byť jen jednu z následujících technických vlastností.

4.1 Technický popis

Přístroj typu P je měřicí přístroj s vestavěným IT systémem (např. systémem na bázi mikroprocesoru nebo mikrořadiče). *Všechny komponenty použitého IT systému jsou přístupné k vyhodnocení.*

Vestavěný IT systém konktrétně vystihují následující body:

- Software je určen výhradně pro účely měření. Další funkce pro zabezpečení softwaru a dat, pro přenos dat a pro stahování softwaru jsou rovněž určeny výhradně pro účely měření.
- Uživatelské rozhraní slouží pouze k měření, tj. v běžném provozním režimu podléhá legální kontrole. Lze nicméně přepnout do provozního režimu, který nepodléhá legální kontrole.
- Může obsahovat operační systém (OS) nebo jeho subsystémy, pokud

  - veškerou komunikaci řídí legálně relevantní software,

  - neumožňuje nahrávání nebo pozměňování programů, parametrů nebo dat nebo spuštění programů,

  - jestliže neumožňuje změny prostředí legálně relevantní aplikace apod.

  Měla by být zároveň předem nastavena ochrana přístupu a neměla by vyplývat z dodatečné konfigurace příslušných komponent.
- Softwarové prostředí nelze měnit a neexistují žádné interní ani externí nástroje programování nebo pozměňování softwaru se statutem vestavěného softwaru. Stahování softwaru je možné, pouze pokud jsou dodrženy specifické požadavky rozšíření D (kapitola 9).

4.2 Specifické požadavky na přístroje typu P

Třída rizika B až E
P1: Dokumentace *Základní dokumentace musí kromě specifické dokumentace uvedené v některém z následujících požadavků obsahovat:* *a. Popis legálně relevantního softwaru.* *b. Popis přesnosti výpočetních algoritmů (např. výpočet ceny a principy zaokrouhlování).* *c. Popis uživatelského rozhraní, menu a dialogů.* *d. Označení legálně relevantního softwaru.* *e. Přehledné informace o hardwaru systému, zahrnující např. schéma topologického diagramu, typ počítače (počítačů), typ sítě,* *f.* Operační manuál*.*

Třída rizika B	Třída rizika C	Třída rizika D
P2: Označení softwaru *Legálně relevantní software musí být jasně označen. Označení musí být přístrojem trvale zobrazeno nebo musí být zobrazeno na příkaz nebo během používání.*		
Upřesnění: 1. Označení legálně relevantního softwaru může být samostatné nebo může být součástí strukturovaného označení. V druhém případě musí být možné zřetelně rozlišit označení legálně relevantního softwaru. 2. Pokud jsou různé verze softwaru platnými implementacemi jednoho typu (např. u přístrojů třídy rizika B), potom musí mít každá verze své vlastní unikátní označení legálně relevantního softwaru. 3. Označení legálně relevantního softwaru je specifický parametr daného typu. 4. Zobrazit označení legálně relevantního softwaru musí být snadno proveditelné, bez nutnosti použít další nástroje. 5. Označení je zobrazeno permanentně na zajištěném štítku nebo se zobrazí na příkaz či během spuštění.		
Požadovaná dokumentace: 1. Dokumentace musí obsahovat (úplné) označení softwaru a popis, jak je tvořeno, jak je zabezpečeno, jak je možné označení zobrazit a jak je strukturováno, aby nemohlo dojít k záměně označení legálně relevantního softwaru s jinými označeními a aby bylo možné vyhodnotit jeho jednoznačnost.		
Postup validace: *Ověření na základě dokumentace:* • Zkontrolujte, zda je označení legálně relevantního softwaru v dokumentaci uvedeno. • Zkontrolujte, zda je software provádějící legálně relevantní funkce jasně popsán a umožňuje rozlišit k jaké části legálně relevantního softwaru se konkrétní označení vztahuje. • Ověřte popis zobrazení označení legálně relevantního softwaru. • Zkontrolujte jednoznačnost všech označení legálně relevantního softwaru (zejména v případě opětovného posouzení). *Ověření funkčnosti:* • Zkontrolujte, zda lze označení legálně relevantního softwaru zobrazit tak, jak je popsáno v dokumentaci. • Zkontrolujte, zda je označení legálně relevantního softwaru zobrazené přístrojem shodné s označením uvedeným v dokumentaci. • Zkontrolujte, zda lze jasně rozlišit označení legálně relevantního softwaru od ostatních označení.		
Příklad přijatelného řešení: a) kontrolní součet kódu programu. b) řetězec, vhodně doplněný číslem verze, c) řetězec čísel, písmen, jiných znaků, • Pokud se výrobce rozhodne pro smíšené označení legálně relevantního a legálně nerelevantního softwaru, pak lze označení jednoduše rozlišit zástupnými znaky v certifikátu schválení typu (TEC), např. „abc1.xx“, kde „abc1“ je označení legálně relevantního softwaru a „xx“ jsou zástupné znaky pro legálně nerelevantní software.		

Dodatky pro třídu rizika E
Požadovaná dokumentace Shodná jako u tříd rizika B až D.
Postup validace Shodný jako u tříd rizika B až D.

Třída rizika B	Třída rizika C	Třída rizika D
P3: Vliv uživatelských rozhraní *Příkazy zadané přes uživatelská rozhraní nesmí nepřípustně ovlivňovat legálně relevantní software, specifické parametry přístroje ani naměřená data.*		
Upřesnění: 1. Každý příkaz musí být jednoznačně přiřazen ke spuštění funkce nebo změně dat. 2. Nezdokumentované příkazy nesmí ovlivňovat legálně relevantní funkce, specifické parametry přístroje ani naměřená data. 3. Části softwaru zajišťující interpretaci příkazů jsou považovány za legálně relevantní software.		
Požadovaná dokumentace: Pokud přístroj umí přijímat příkazy, musí dokumentace zahrnovat: • Popis příkazů a jejich vliv na legálně relevantní software, specifické parametry přístroje a naměřená data. • Popis toho, jak jsou legálně relevantní software, specifické parametry přístroje a naměřená data chráněny před ovlivněním jinými vstupy.		
Postup validace: *Ověření na základě dokumentace:* • Zkontrolujte, zda jsou zdokumentované příkazy přípustné, tj. zda jejich vliv na legálně relevantní software, specifické parametry přístroje a naměřená data je povolený. • Zkontrolujte prostředky zabezpečení před ovlivněním jinými vstupy. *Ověření funkčnosti:* • Proveďte praktické testy (namátkovou kontrolu) zadáváním zdokumentovaných příkazů. • Proveďte testy k vyloučení existence nezdokumentovaných příkazů.		
Příklad přijatelného řešení: Softwarový modul, který přijímá a interpretuje příkazy z uživatelského rozhraní. Tento modul patří k legálně relevantnímu softwaru. Dalším modulům legálně relevantního softwaru přeposílá pouze povolené příkazy. Všechny neznámé nebo nepovolené sekvence stisknutí přepínače nebo kláves jsou odmítnuty a nemají žádný vliv na legálně relevantní software, specifické parametry přístroje ani na naměřená data.		

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:** Zdrojový kód legálně relevantního softwaru.
Postup validace (kromě požadavků pro třídy rizika B až D)**:** *Ověření na základě zdrojového kódu:* • Ověřte návrh softwaru, zda je tok dat týkající se příkazů jednoznačně definován a realizován pouze legálně relevantním softwarem. • Pátrejte po nepřípustném toku dat z uživatelského rozhraní do domén, které mají být zabezpečeny. • Ověřte správné dekódování příkazů (pomocí nástrojů nebo manuálně).

Třída rizika B	Třída rizika C	Třída rizika D

P4: Vliv komunikačních rozhraní

Příkazy zadané přes komunikační rozhraní přístroje nesmí nepřípustně ovlivňovat legálně relevantní software, specifické parametry přístroje ani naměřená data.

Upřesnění:

1. Každý příkaz musí být jednoznačně přiřazen ke spuštění funkce nebo přenosu dat.
2. Nezdokumentované příkazy nesmějí ovlivňovat legálně relevantní funkce, specifické parametry přístroje ani naměřená data.
3. Části softwaru zajišťující interpretaci příkazů jsou považovány za legálně relevantní software.
4. Rozhraní umožňující zadávání příkazů, jež mohou nepřípustně ovlivnit legálně relevantní software, specifické parametry přístroje či naměřená data, musí být zaplombována nebo zabezpečena jiným vhodným způsobem. To platí i pro rozhraní, která nelze kompletně posoudit.
5. Tento specifický požadavek se netýká stahování softwaru dle rozšíření D.

Požadovaná dokumentace:

Pokud má přístroj rozhraní, dokumentace musí obsahovat:

- Popis příkazů a jejich vliv na legálně relevantní software, specifické parametry přístroje a naměřená data.
- Popis způsobu zabezpečení legálně relevantního softwaru, specifických parametrů přístroje a naměřených dat proti ovlivnění jinými vstupy.

Postup validace:

Ověření na základě dokumentace:

- Zkontrolujte, zda jsou zdokumentované příkazy přípustné, tj. zda jejich vliv na legálně relevantní software, specifické parametry přístroje a naměřená data je povolený.
- Zkontrolujte prostředky zabezpečení před ovlivněním jinými vstupy.

Ověření funkčnosti:

- Proveďte praktické testy (namátkovou kontrolu) s využitím periferních zařízení.

Příklad přijatelného řešení:

Data z rozhraní přijímá a interpretuje softwarový modul, který je součástí legálně relevantního softwaru. Jiným modulům legálně relevantního softwaru předává pouze povolené příkazy. Všechny neznámé či nepovolené signály nebo sekvence kódů jsou odmítnuty a nemají tedy na legálně relevantní software, specifické parametry přístroje ani na naměřená data žádný vliv.

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:**

Zdrojový kód legálně relevantního softwaru.

Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:**

Ověření na základě zdrojového kódu:

- Ověřte návrh softwaru, zda je tok dat týkající se příkazů legálně relevantního softwaru jednoznačně definován a zda je verifikovatelný.
- Pátrejte po nepřípustném toku dat z rozhraní do domén, které mají být zabezpečeny.
- Ověřte správné dekódování příkazů (pomocí nástrojů nebo manuálně).

Třída rizika B	Třída rizika C	Třída rizika D

P5: Ochrana proti náhodným či neúmyslným změnám

Legálně relevantní software a specifické parametry přístroje musí být zabezpečeny proti náhodným či neúmyslným změnám.

Upřesnění:

1. Software musí být schopný detekovat změny způsobené fyzikálními vlivy (elektromagnetickým rušením, teplotou, vibracemi atd.).
2. Musí být implementovány prostředky ochrany proti neúmyslnému zneužití / nesprávnému použití uživatelskými rozhraními.

Požadovaná dokumentace:

1. Dokumentace musí popisovat způsoby detekce a ochrany legálně relevantního softwaru a specifických parametrů přístroje před neúmyslnými změnami.

Postup validace:

Ověření na základě dokumentace:

- Zkontrolujte, zda jsou popsány způsoby ochrany proti neúmyslným změnám a zda jsou přiměřené.

Ověření funkčnosti:

- Proveďte namátkové kontroly, zda se před vymazáním naměřených dat zobrazí varování (pokud systém mazání dat vůbec umožňuje).

Příklad přijatelného řešení:

- Neúmyslné změny legálně relevantního softwaru a specifických parametrů přístroje jsou kontrolovány pravidelně přepočítávanými kontrolními součty a automatickým porovnáváním těchto součtů s uloženými nominálními hodnotami. Pokud porovnávané hodnoty nesouhlasí, je nutné reagovat způsobem odpovídajícím danému přístroji (např. zastavit měření, vhodně naměřená data označit atd., viz doporučení v kapitole 10).
- Lze použít i alternativní metody, pokud dokáží změnu softwaru odhalit.
- Proces detekce chyb je popsán v rozšíření I (kapitola 10).

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika C a D):
Zdrojový kód legálně relevantního softwaru.

Postup validace (kromě postupu požadovaného pro třídy rizika C a D)**:**

Ověření na základě zdrojového kódu:

- Ověřte, zda jsou způsoby detekce změn dostatečné.
- Ověřte, zda jsou v kontrolním součtu zahrnuty všechny části legálně relevantního softwaru.

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">P6: Ochrana proti nepřípustným záměrným změnám
Legálně relevantní software a naměřená data musí být zabezpečeny proti nepřípustným záměrným modifikacím, nahrávání nebo výměně fyzické paměti.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Ochrana proti manipulaci přes uživatelské rozhraní – viz P3.
2. Ochrana proti manipulaci přes komunikační rozhraní – viz P4.
3. Naměřená data jsou dostatečně zabezpečena tehdy, pokud jsou zpracovávána pouze legálně relevantním softwarem (např. v paměti nebo registrech).</td></tr>
<tr><td></td><td colspan="2">Upřesnění:
4. K detekci změn softwaru je použit kontrolní součet nebo jiná alternativní metoda se stejnou úrovní požadavků.
5. Pro kontrolní účely musí být možno vypočítaný kontrolní součet nebo alternativní indikaci modifikace softwaru na příkaz zobrazit.
6. Kontrolní součet nebo alternativní indikace jsou vypočítávány z legálně relevantního softwaru. Software zajišťující výpočet kontrolních součtů nebo alternativních indikací je součástí legálně relevantního softwaru.
7. V případě aplikace kontrolního součtu, délka klíče tohoto algoritmu musí mít nejméně 4 byty (viz také rozšíření L a T).</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Dokumentace musí obsahovat popis způsobů zabezpečení.</td></tr>
<tr><td colspan="3">• Popis prostředků zabezpečení softwaru a specifických parametrů přístroje, zejména metodu výpočtu kontrolního součtu a odpovídající nominální hodnotu kontrolního součtu nebo alternativní metodu včetně odpovídající nominální hodnoty.</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda jsou zdokumentované prostředky zabezpečení proti nepovolené výměně paměti, na níž je uložen software, dostatečné.
• Ověřte, zda kontrolní součty / alternativní indikace pokrývají celý legálně relevantní software.

Ověření funkčnosti:
• Proveďte test programovacího režimu a zkontrolujte, zda je vstup do něho znepřístupněn.
• Porovnejte vypočítané kontrolní součty / alternativní indikace s nominálními hodnotami.</td></tr>
<tr><td>Příklad přijatelného řešení:
a) Kryt přístroje nebo samotná fyzická paměť jsou zabezpečeny proti nepovolenému odmontování, aby nemohlo dojít k vyjmutí či výměně fyzické paměti.
b) Přístroj je zaplombovaný a jeho rozhraní odpovídají požadavkům P3 a P4.</td><td colspan="2">Příklad přijatelného řešení: (kromě a) a b))
c) Kód programu je chráněn kontrolními součty. Program si vypočítává svůj vlastní kontrolní součet a porovnává ho s očekávanou hodnotou zapsanou ve spustitelném kódu. V případě selhání této kontroly je program zablokován. Je použit kontrolní součet CRC-32 s neveřejným počátečním vektorem (skrytým ve spustitelném kódu).</td></tr>
</table>

<table>
<tr><th>Dodatky pro třídu rizika E</th></tr>
<tr><td>Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D):
Zdrojový kód legálně relevantního softwaru</td></tr>
<tr><td>Postup validace (kromě postupu požadovaného pro třídy rizika B až D):
Ověření na základě zdrojového kódu:
• Ověřte, zda jsou prostředky detekce záměrných změn dostatečné.</td></tr>
</table>

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">P7: Ochrana parametrů
Specifické parametry přístroje musí být po svém nastavení zabezpečeny proti nepřípustným změnám.</td></tr>
<tr><td colspan="3">Upřesnění:
1. V běžném zabezpečeném provozním režimu již nesmí být možné pozměnit specifické parametry přístroje. Jejich případná úprava je možná pouze ve zvláštním provozním režimu přístroje.
2. Mohou existovat některé specifické parametry přístroje, u kterých je dovoleno, aby zůstaly nezabezpečené. Více o specifických parametrech přístroje naleznete v rozšíření I.</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Dokumentace musí popisovat specifické parametry přístroje, zda je lze nastavit, jak se nastavují a jak jsou zabezpečeny.</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda je po zabezpečení znemožněno provádět změny a úpravy specifických parametrů přístroje.
• Ověřte, zda jsou zabezpečeny všechny příslušné parametry (specifikované v rozšíření I, pokud takové existují).
Ověření funkčnosti:
• Proveďte test režimu úprav (konfigurací) a zkontrolujte, zda je vstup do něho po zabezpečení nepřístupněn.
• Ověřte klasifikaci a stav parametrů (chráněný/nastavitelný) na displeji přístroje, pokud je příslušná položka menu k dispozici.</td></tr>
<tr><td colspan="3">Příklad přijatelného řešení:
a) Parametry jsou zabezpečeny jednak zaplombováním přístroje nebo krytu paměti a dále přidružená zaplombovaná propojka nebo přepínač blokuje možnost zápisu do paměťového okruhu.</td></tr>
<tr><td colspan="2">b) Čítač/záznamník událostí:
• Čítač událostí zaznamenává každou změnu hodnoty parametru. Umožňuje zobrazit aktuální počet událostí a porovnat ho s počáteční hodnotou čítače, která byla zaznamenána při uvedení měřicího přístroje do provozu či s hodnotou zaznamenanou při posledním oficiálním ověření. Tato počáteční hodnota čítače je nesmazatelně uvedena na štítku přístroje.
• Změny parametrů zaznamenává záznamník událostí, jež ukládá informace do energeticky nezávislé paměti. Každý vstup je generován automaticky legálně relevantním softwarem a obsahuje:
o označení parametru (např. název)
o hodnotu parametru (aktuální nebo předchozí)
o časový údaj změny (časové razítko)
• Záznamník událostí nelze vymazat nebo měnit, je chráněn bezpečnostní plombou. Obsah záznamníku událostí lze vyčíst na displeji měřidla či na příkaz vytisknout.</td><td>÷</td></tr>
</table>

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:** Zdrojový kód legálně relevantního softwaru, který ukazuje způsob zabezpečení a zobrazování legálně relevantních parametrů.
Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:** *Ověření na základě zdrojového kódu:* • Ověřte kód, zda jsou prostředky na ochranu parametrů dostatečné (např. znepřístupnění režimu úprav po zabezpečení).

Třída rizika C	Třída rizika D
P8: Autentizace prezentovaných naměřených dat *Musí být zaručena autentičnost prezentovaných naměřených dat.*	

Upřesnění:

1. Naměřená data jsou považována za autentická, pokud jsou prezentována legálně relevantním softwarem.
2. Nesmí být možné napodobovat (fingovat) legálně relevantní software za účelem prezentace naměřených dat pomocí snadno dostupných ovládacích nástrojů.
3. Prezentovaná naměřená data musí být srozumitelná a jasně odlišitelná od jiných informací, informací nerelevantních z hlediska legální metrologie. V případě nutnosti musí být poskytnuto detailní označení.
4. Pokud zdroj prezentovaných naměřených dat (např. senzor) není implicitně identifikovatelný či ověřitelný (např. existuje více senzorů či senzor je připojen vzdáleně), měřidlo musí poskytnout identifikaci příslušného zdroje. Jednoznačný identifikátor schváleného zdroje dat je legálně relevantním parametrem, na který se vztahují požadavky P6/U6 či P7/U7. V závislosti na typu datového připojení je nutno aplikovat požadavky rozšíření T.

Požadovaná dokumentace:

Dokumentace musí popisovat, jakým způsobem je zajištěna autentičnost naměřených dat.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda byla prezentovaná naměřená data generována legálně relevantním softwarem.
- Ověřte, zda mohou být naměřená data prezentována pouze legálně relevantním softwarem.
- Pokud zdroj prezentovaných naměřených dat není implicitně identifikovatelný či ověřitelný ověřte, zda zdroj těchto dat je identifikován a indikován legálně relevantním softwarem.

Ověření funkčnosti:

- Ověřte vizuálně, jestli jsou prezentovaná naměřená data snadno odlišitelná od jiných prezentovaných informací, které mohou být též prezentovány.
- Pokud je to relevantní vizuálně zkontrolujte, že prezentovaná naměřená data jsou korektně spjata s příslušným zdrojem.

Příklady přijatelných řešení:

1. Měřicí aplikace je generována legálně relevantním softwarem. Na aplikaci jsou kladeny následující technické požadavky:
   - Legálně nerelevantním programům není umožněn přístup k naměřeným datům, dokud jsou tato data zobrazována.
   - Aplikace je pravidelně obnovována. Asociovaný program kontroluje, zda je aplikace viditelná dokud není měření ukončeno. Zpracovávání naměřených hodnot se zastaví, kdykoliv je tato aplikace zavřená nebo není plně viditelná.

2a Jednotka snímače šifruje naměřené hodnoty klíčem známým autentickému softwaru běžícímu na jednoúčelovým zařízení (číslo jeho verze). Pouze tento věrohodný software dokáže naměřené hodnoty dešifrovat a použít. Neautentické programy běžící v měřidle tento klíč neznají, a proto naměřené hodnoty nedokáží dešifrovat ani použít. Zacházení s klíči je popsáno v rozšíření T.

2b Snímač před posláním hodnot a zahájení komunikace s legálně relevantním softwarem jednoúčelového zařízení provede na základě tajných klíčů „handshake“, tj. proces „potřesení rukou“. Snímač naměřené hodnoty pošle pouze tehdy, když program jednoúčelového zařízení komunikuje správně. Zacházení s klíči je popsáno v rozšíření T.

3. Klíč použitý v bodech 2a / 2b je volitelný a lze ho do snímače a do softwaru jednoúčelového zařízení zapsat bez porušení plomby.	3. Klíč použitý v bodech 2a / 2b je hash kódem programu v jednoúčelovém zařízení. Při každé změně softwaru jednoúčelového zařízení je do senzoru vložen nový klíč, který je zabezpečený tak, aby ho nebylo možné změnit bez porušení plomby.

4. Pokud prezentovaná naměřená data nejsou explicitně spojena se senzorem, primární senzor přenáší data spolu s jednoznačnou identifikací sebe sama. Všechna prezentovaná naměřená data

jsou označena identifikací příslušného senzoru. Identifikace každého senzoru je legálně relevantním parametrem, který lze i vyčíst na krytu senzoru.

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika C až D)**:** Zdrojový kód legálně relevantního softwaru.
Postup validace (kromě postupu požadovaného pro třídy rizika C až D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda prezentovaná naměřená data generuje legálně relevantní software. • Ověřte, zda jsou všechny prostředky garantující prezentaci naměřených dat legálně relevantním softwarem přiměřené a vhodné.

5 Základní požadavky na software měřicích přístrojů využívajících univerzální počítač (typ U)

Soubor specifických požadavků popsaných v této kapitole se vztahuje na měřicí přístroje využívající víceúčelový počítač, ale také na podsestavy a části dle příručky WELMEC 8.8 využívající univerzální počítač. Ustanovení zde uvedená se na takové podsestavy a části vztahují i tehdy, když to v následujícím textu není opakovaně zdůrazněno. Součástí této příručky nicméně nejsou podmínky samostatného přezkušování podsestav a částí ani podmínky akceptace příslušných certifikátů.

5.1 Technický popis

Pro měřicí systém typu U jsou obvykle charakteristické následující konfigurace.

Konfigurace hardwaru

a) Modulární systém založený na univerzálním počítači. Tento počítačový systém může být samostatný nebo může být součástí uzavřené sítě, např. ethernetové sítě, místní sítě LAN postavené na technologii token ring, nebo může být součástí otevřené sítě, např. internetu.

b) Vzhledem k tomu, že se jedná o systém s všeobecným účelem, snímač (který vykonává měření) se obvykle nachází mimo počítačovou jednotku a je k ní připojen přes komunikační linku.

c) Kromě provozního režimu provádějícího konkrétní měření jsou v uživatelském rozhraní k dispozici i další funkce nepodléhající legální kontrole.

d) Paměť může být pevná (např. harddisk), vyjímatelná (např. USB), nebo vzdálená.

Konfigurace softwaru

e) Obvykle je využit operační systém.

f) Kromě aplikace pro měřicí přístroje mohou v systému ve stejný čas běžet i jiné softwarové aplikace.

Za systém typu U se kromě výše popsaných konfigurací považuje i systém, který nesplňuje všechny ustanovení pro přístroje typu P (viz podkapitola 4.1).

Běžně dostupný operační systém a s ním dodávané nízkoúrovňové ovladače, např. video ovladače, ovladače k tiskárnám, diskům, atd., nejsou považovány za legálně relevantní, pokud jejich části nejsou nahrazeny alternativními částmi nebo pokud nejsou speciálně naprogramovány na nějaký specifický měřicí úkol.

Důsledky klasifikace rizik

Software měřicích přístrojů typu U je daleko otevřenější a přístupnější než software měřicích přístrojů typu P, a proto musí být u přístrojů tohoto typu lépe chráněna integrita softwaru. Ke kontrole integrity kódu softwaru je nutné používat zejména kontrolní součty a jiné ekvivalentní metody. Nízká úroveň shody (tj. pouze funkční shoda softwaru a technické dokumentace schvalovaného typu) nepředstavuje

adekvátní způsob zajištění integrity softwaru a tudíž nejnižší možnou třídou, do níž mohou přístroje typu U náležet, je třída rizika C.

5.2 Specifické požadavky na software přístrojů typu U

Třídy rizika C až E
U1: Dokumentace *Základní dokumentace musí kromě specifické dokumentace uvedené v některém z následujících požadavků obsahovat:* a. *Popis funkcí legálně relevantního softwaru, význam dat atd.* b. *Popis přesnosti výpočetních algoritmů (např. výpočet ceny a principy zaokrouhlování).* c. *Popis uživatelského rozhraní, menu a dialogů.* d. *Označení legálně relevantního softwaru.* e. *Přehledné informace o hardwaru systému, zahrnující např. schéma topologického diagramu, typ počítače (počítačů), typ sítě,* f. *Přehled konfigurace použitého operačního systému, uplatněná pravidla bezpečnosti daného operačního systému, např. zabezpečení, uživatelské účty, jejich práva,* g. Operační manuál.

Třída rizika C a D
U2: Označení softwaru *Legálně relevantní software musí být jasně označen. Označení musí být přístrojem trvale zobrazeno nebo musí být zobrazeno na příkazu nebo během používání.*
Upřesnění: 1. Označení legálně relevantního softwaru může být samostatné nebo může být součástí strukturovaného označení. 2. Pokud je označení legálně relevantního softwaru součástí celkového označení, musí být zřetelně rozlišitelné. 3. Označení každého legálně relevantního softwaru, kterým je přístroj vybaven, musí být unikátní. 4. Zobrazit označení legálně relevantního softwaru musí být snadno proveditelné, bez nutnosti použít další nástroje. 5. Označení musí zahrnovat ovladače a komponenty operačního systému, které byly upraveny či speciálně naprogramovány k provádění nějakého legálně relevantního úkolu. Do označení nemusejí být zahrnuty standardní komponenty systému používané beze změn. 6. Budou-li legálně relevantní funkce a záznamy o měření chráněny zvláštní konfigurací operačního systému, musí mít příslušné konfigurační soubory své vlastní označení. 7. Označení legálně relevantního softwaru je považováno za specifický parametr daného typu, který musí být náležitým způsobem zabezpečen (viz požadavky U5 a U6). Není-li označení neoddělitelně spojeno se samotným softwarem, jsou požadovány další prostředky zabezpečení. 8. Označení je (jsou) zobrazeno(a) permanentně nebo se zobrazí po zadání příkazu nebo při spuštění.
Požadovaná dokumentace: Dokumentace musí obsahovat úplné označení softwaru a popis, jak je tvořeno, jak je zabezpečeno, jak je možné označení zobrazit, případně jak je strukturováno, aby bylo možné odlišit označení legálně relevantního softwaru od jiných označení.

Postup validace:

Ověření na základě dokumentace:

- Zkontrolujte, zda dokumentace obsahuje označení legálně relevantního softwaru.
- Zkontrolujte, zda je software provádějící legálně relevantní úkoly jasně popsán a umožňuje rozlišit k jaké části legálně relevantního softwaru se konkrétní označení vztahuje.
- Ověřte popis generování a zobrazení označení.
- Zkontrolujte, zda operační systém obsahuje nějaké modifikované či samostatně vyvinuté komponenty. Pokud ano, zkontroluje, zda jsou zahrnuty do označení.
- Pokud je software pro funkce měření chráněn speciální konfigurací operačního systému, zkontrolujte, zda mají relevantní konfigurační soubory své vlastní označení.
- Zkontrolujte jednoznačnost všech označení legálně relevantního softwaru.

Ověření funkčnosti:

- Označení softwaru lze zobrazit dle popisu v dokumentaci.
- Předložená označení jsou identická s označeními uvedenými v dokumentaci.
- Označení legálně relevantního softwaru je odlišitelné od jiných označení.

Příklad přijatelného řešení:

a) kontrolní součet kódu programu.
b) řetězec doplněný číslem verze,
c) řetězec čísel, písmen, jiných znaků,

Pokud se výrobce rozhodne pro smíšené označení legálně relevantního a legálně nerelevantního softwaru, pak lze označení jednoduše rozlišit zástupnými znaky v certifikátu schválení typu (TEC), např. „abc1.xx“, kde „abc1“ je označení legálně relevantního softwaru a „xx“ jsou zástupné znaky pro legálně nerelevantní software.

Dodatky pro třídu rizika E
Požadovaná dokumentace Shodná jako u tříd rizika C a D.
Postup validace Shodná jako u tříd rizika C a D.

Třída rizika C	**Třída rizika D**
U3: Vliv uživatelských rozhraní *Příkazy zadané přes uživatelská rozhraní nesmí nepřípustně ovlivňovat legálně relevantní software, specifické parametry přístroje ani naměřená data.*	
Upřesnění: 1. Každý příkaz musí být jednoznačně přiřazen ke spuštění funkce nebo změně dat. 2. Nezdokumentované příkazy nesmí ovlivňovat legálně relevantní funkce, specifické parametry přístroje ani naměřená data. 3. Části softwaru zajišťující interpretaci příkazů jsou považovány za legálně relevantní software. 4. Zvláště funkce operačního systému nabízené v uživatelském rozhraní nesmějí ovlivňovat legálně relevantní software, specifické parametry přístroje ani naměřená data (včetně konfigurace operačního systému a dalších prostředků jejich zabezpečení).	
÷	5. Uživatelské rozhraní musí být uzavřené, tj. uživatel nesmí mít možnost nahrávat programy, psát programy nebo zadávat příkazy operačnímu systému.

Požadovaná dokumentace: Pokud přístroj dokáže přijímat příkazy, dokumentace musí zahrnovat: • Popis příkazů a jejich vliv na legálně relevantní software, specifické parametry přístroje a naměřená data. • Popis toho, jak jsou legálně relevantní software, specifické parametry přístroje a naměřená data zabezpečeny před ovlivněním jinými vstupy. • Především popis toho, jak jsou legálně relevantní software, specifické parametry přístroje a naměřená data zabezpečeny proti funkcím operačního systému nabízeným uživateli.	**Požadovaná dokumentace** (kromě dokumentace pro třídu rizika C)**:** • Popis způsobů zabezpečení proti jiným vstupům včetně funkcí operačního systému, které jsou nabízené uživateli.
Postup validace: *Ověření na základě dokumentace:* • Zkontrolujte, zda jsou zdokumentované příkazy přípustné, tj. zda jejich vliv na legálně relevantní software, specifické parametry přístroje a naměřená data je povolený. • Zkontrolujte prostředky zabezpečení před ovlivněním jinými příkazy. • Zvláště zkontrolujte prostředky zabezpečení proti ovlivnění funkcemi operačního systému, které jsou nabízené uživateli. *Ověření funkčnosti:* • Proveďte praktické testy (namátkovou kontrolu) zadáváním zdokumentovaných příkazů. • Proveďte testy k vyloučení existence nezdokumentovaných příkazů.	**Postup validace** (kromě požadavků pro třídu rizika C)**:** *Ověření na základě dokumentace:* • Ověřte, zda použité prostředky a testovací protokoly odpovídají vysoké úrovni zabezpečení.
Příklad přijatelného řešení: • Modul v legálně relevantním softwaru odfiltrovává nepřípustné příkazy. Pouze tento modul přijímá příkazy a nelze ho obejít. Jakýkoliv falešný vstup je blokován.	**Příklad přijatelného řešení:** • K používání měřicího systému jsou zřízeny pouze účty s omezenými oprávněními. Přístup k účtu administrátora je blokován dle požadavku U6.

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídu rizika D)**:** Zdrojový kód legálně relevantního softwaru.
Postup validace (kromě požadavků pro třídu rizika D)**:** *Ověření na základě zdrojového kódu:* • Ověřte návrh softwaru, zda je tok dat týkající se příkazů legálně relevantního softwaru jednoznačně definován a zda je verifikovatelný. • Pátrejte po nepřípustném toku dat z uživatelského rozhraní do domén, které mají být zabezpečeny. • Ověřte správné dekódování příkazů (pomocí nástrojů nebo manuálně).

Třída rizika C	Třída rizika D

U4: Vliv komunikačních rozhraní

Příkazy zadané přes komunikační rozhraní přístroje nesmí nepřípustně ovlivňovat legálně relevantní software, specifické parametry přístroje ani naměřená data.

Upřesnění:

1. Každý příkaz musí být jednoznačně přiřazen ke spuštění funkce nebo přenosu dat.
2. Nezdokumentované příkazy nesmějí ovlivňovat legálně relevantní funkce, specifické parametry přístroje ani naměřená data.
3. Části softwaru zajišťující interpretaci příkazů jsou považovány za legálně relevantní software.
4. Rozhraní umožňující zadávání příkazů, jež mohou nepřípustně ovlivnit legálně relevantní software, specifické parametry přístroje či naměřená data, musí být zaplombována nebo zabezpečena jiným vhodným způsobem. To platí i pro rozhraní, která nelze kompletně posoudit.
5. Tento specifický požadavek se netýká stahování softwaru dle rozšíření D.

Upozornění: Pokud operační systém umožňuje vzdálenou kontrolu nebo vzdálený přístup, pak se požadavky U3 vztahují obdobně na komunikační rozhraní a připojený vzdálený terminál.

Požadovaná dokumentace:

Pokud má přístroj rozhraní, dokumentace musí obsahovat:

- Popis příkazů a jejich vliv na legálně relevantní software, specifické parametry přístroje a naměřená data.
- Popis způsobu zabezpečení legálně relevantního softwaru, specifických parametrů přístroje a naměřených dat před ovlivněním jinými vstupy.

Postup validace:

Ověření na základě dokumentace:

- Zkontrolujte, zda jsou zdokumentované příkazy přípustné, tj. zda jejich vliv na legálně relevantní software, specifické parametry přístroje a naměřená data je povolený..
- Zkontrolujte prostředky zabezpečení před ovlivněním jinými příkazy.

Ověření funkčnosti:

- Proveďte praktické testy (namátkovou kontrolu) s využitím periferních zařízení.

Příklad přijatelného řešení:

Data z rozhraní přijímá a interpretuje softwarový modul, který je součástí legálně relevantního softwaru. Jiným modulům legálně relevantního softwaru předává pouze povolené příkazy. Všechny neznámé či nepovolené příkazy jsou odmítnuty, a nemají tedy na legálně relevantní software, specifické parametry přístroje ani na naměřená data žádný vliv.

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika C až D)**:**

Zdrojový kód legálně relevantního softwaru.

Postup validace (kromě postupu požadovaného pro třídy rizika C až D)**:**

Ověření na základě zdrojového kódu:

- Ověřte návrh softwaru, zda je tok dat týkající se příkazů legálně relevantního softwaru jednoznačně definován a zda je verifikovatelný.
- Pátrejte po nepřípustném toku dat z uživatelského rozhraní do domén, které mají být zabezpečeny.
- Ověřte správné dekódování příkazů (pomocí nástrojů nebo manuálně).

Třída rizika C	Třída rizika D

U5: Ochrana proti náhodným či neúmyslným změnám
Legálně relevantní software a specifické parametry přístroje musí být zabezpečeny proti náhodným či neúmyslným změnám.

Upřesnění:

1. Software musí být schopný detekovat změny způsobené fyzikálními vlivy (elektromagnetickým rušením, teplotou, vibracemi atd.).
2. Musí být implementovány prostředky ochrany proti neúmyslnému zneužití / nesprávnému použití uživatelskými rozhraními.
3. Náhodná modifikace legálně relevantního softwaru a specifických parametrů přístroje musí být pravidelně kontrolována kontrolními součty a jejich automatickým porovnáváním s uloženými nominálními hodnotami. Pokud porovnávané hodnoty nesouhlasí, je nutné reagovat způsobem odpovídajícím danému přístroji (např. zastavit měření, vhodně naměřená data označit; viz doporučení v kapitole 10)
   K odhalení změny stavu softwaru lze použít i alternativní metody.
4. Pokud to operační systém umožňuje, doporučuje se odstranit všechna uživatelská práva na vymazání, přesun či úpravy legálně relevantního softwaru. Přístup pak řídí obslužné programy.
5. Doporučuje se zabezpečit přístup k legálně relevantnímu softwaru hesly a rovněž používat mechanismy pouze pro čtení. Osoba dohlížející na systém povoluje práva pouze na žádost.

Požadovaná dokumentace:

- Popis prostředků detekce a zabezpečení legálně relevantního softwaru a specifických parametrů přístroje proti neúmyslným změnám.
- Popis metody kontrolního součtu a opatření při nesouladu porovnávaných hodnot.
- Popis toho, jak a kde je uložena nominální hodnota kontrolního součtu, nebo alternativní údaje o stavu změny.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda jsou popsány prostředky ochrany proti neúmyslným změnám a zda jsou tyto prostředky dostatečné.
- Ověřte, zda kontrolní součet pokrývá celý legálně relevantní software.
- Ověřte, zda jsou metody výpočtu kontrolního součtu, porovnávání a opatření v případě nesouhlasu údajů správné.

Příklad přijatelného řešení:

- Zneužití operačního systému, přepsání nebo vymazání dat a programů: Je využito všech prostředků ochrany a práv na soukromí, které poskytuje operační systém nebo programovací jazyk.
- Náhodná změna legálně relevantního softwaru je kontrolována prostřednictvím kontrolního součtu příslušného kódu a jeho porovnáním s nominální hodnotou. Pokud se při kontrole zjistí, že byl kód změněn, jsou podniknuty odpovídající kroky.

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika C to D)**:**
Zdrojový kód legálně relevantního softwaru.

Postup validace (kromě postupu požadovaného pro třídy rizika C až D)**:**

Ověření na základě zdrojového kódu:

- Ověřte, zda jsou prostředky detekce změn (chyb) dostatečné.
- Ověřte, zda jsou v kontrolním součtu zahrnuty všechny části legálně relevantního softwaru.

<table>
<tr><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="2">U6: Ochrana proti nepřípustným záměrným změnám
Legálně relevantní software a naměřená data musí být zabezpečeny proti nepřípustným záměrným modifikacím nebo nahrazení.</td></tr>
<tr><td colspan="2">Upřesnění:
1. Velkokapacitní paměťové zařízení, v němž je uložen legálně relevantní software, konfigurační soubory a specifické parametry přístroje, musí být chráněno proti fyzické výměně.
2. K detekci změn softwaru je použit kontrolní součet nebo jiná alternativní metoda se stejnou úrovní požadavků. Vypočítaný kontrolní součet nebo alternativní indikace modifikace softwaru musí být možno zobrazit na příkaz pro kontrolní účely.
3. Kontrolní součet nebo alternativní indikace se vypočítává z legálně relevantního softwaru. Software zajišťující výpočet kontrolních součtů nebo alternativních indikací je součástí legálně relevantního softwaru.
4. Legálně relevantní software musí být zabezpečen proti změnám či nahrazení jiným softwarem. Jeho ochranu musí zajišťovat prostředky operačního systému.
5. Části a prvky operačního systému zajišťující ochranu legálně relevantního softwaru musí být rovněž považovány za legálně relevantní software, a jako takové musí být odpovídajícím způsobem zabezpečeny. Tento specifický požadavek se nevztahuje na stahování softwaru dle rozšíření D.
6. V případě aplikace kontrolního součtu, délka klíče tohoto algoritmu musí mít nejméně 4 byty.</td></tr>
<tr><td></td><td>7. Univerzální počítač lze obecně použít pouze tehdy, pokud je možné použít doplňkový hardware zajišťující dodatečné zabezpečení.
8. Při výběru vhodného algoritmu a minimální délky klíče musí být vzaty v úvahu požadavky a doporučení národních a mezinárodních institutů zodpovědných za bezpečnost dat.</td></tr>
<tr><td colspan="2">Požadovaná dokumentace:
• Popis prostředků zabezpečení softwaru a specifických parametrů přístroje, zejména popis metody výpočtu kontrolního součtu a nominálních hodnot nebo alternativní metody s odpovídajícím nominálním údajem.
• Popis metod zabezpečení velkokapacitních pamětí proti jejich výměně (pokud je tento požadavek relevantní).
• Popis použitých prvků zabezpečení operačního systému.
• Popis zobrazení kontrolních součtů nebo alternativních indikací.</td></tr>
<tr><td colspan="2">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda kontrolní součty nebo alternativní údaje pokrývají celý legálně relevantní software.
• Ověřte, zda jsou prostředky operačního systému zabraňující modifikaci či výměně legálně relevantního softwaru dostatečné.
• Ověřte, zda jsou prvky operačního systému zajišťující ochranu legálně relevantního softwaru součástí legálně relevantního softwaru a zda jsou jako takové náležitě zabezpečeny.
• Ověřte, zda jsou velkokapacitní paměťová zařízení zabezpečena proti fyzické výměně (je-li tento požadavek relevantní).

Ověření funkčnosti:
• Zajistěte výpočet kontrolních součtů nebo alternativních indikací a porovnejte výsledky s nominálními hodnotami.</td></tr>
<tr><td></td><td>Ověření na základě dokumentace:
• Ověřte, zda přijatá opatření odpovídají nejnovějším požadavkům na vysoký stupeň ochrany.</td></tr>
</table>

Příklady přijatelného řešení:	**Příklad přijatelného řešení:**
1. Kód programu je chráněn výpočtem kontrolních součtů. Program vypočítává svůj vlastní kontrolní součet a porovnává ho s požadovanou hodnotou zapsanou ve spustitelném kódu. V případě selhání této kontroly je program zablokován. Je použit kontrolní součet CRC-32 s neveřejným počátečním vektorem (skrytým ve spustitelném kódu). Přístup k účtu administrátora je blokován pomocí náhodného hesla, které je generováno automaticky a nikdo ho nezná. Změna konfigurace legálně relevantního softwaru je možná pouze při nové instalaci operačního systému. Obejít prostředky zabezpečení operačního systému přímým zápisem do velkokapacitní paměti nebo její fyzické výměně je zabráněno zapečetěním. 2. Nepovolené manipulaci s legálně relevantním softwarem je zabráněno kontrolou přístupu nebo využitím prvků ochrany soukromí poskytovaných operačním systémem. Administrace operačního systému musí být chráněna plombou nebo ekvivalentními prostředky.	• Kód programu je zabezpečen uložením legálně relevantního softwaru na jednoúčelovou přídavnou jednotku, která je zajištěna plombou. Tato jednotka je tvořena pamětí chráněnou proti zápisu a mikroprocesorem.

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika C až D)**:** Zdrojový kód legálně relevantního softwaru.
Postup validace (kromě směrnic požadovaných pro třídu rizika D)**:** *Ověření na základě zdrojového kódu:* • Ověřte komunikaci s hardwarem zajišťujícím dodatečnou ochranu. • Ověřte, zda sou změny legálně relevantního softwaru detekovány.

Třída rizika C	**Třída rizika D**
U7: Ochrana parametrů *Specifické parametry přístroje musí být zabezpečeny proti nepřípustným změnám.*	
Upřesnění: 1. Vzhledem k tomu, že pomocí jednoduchých nástrojů univerzálních počítačů lze snadno manipulovat specifickými parametry přístroje, musí být tyto parametry uloženy v zabezpečeném hardwaru, např. v příslušném snímači.	
Požadovaná dokumentace: Dokumentace musí popisovat specifické parametry přístroje, zda je lze nastavit, jak se nastavují a jak jsou zabezpečeny.	
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda je po nastavení znemožněno provádět změny a úpravy specifických parametrů přístroje. • Ověřte, zda jsou zabezpečeny všechny příslušné parametry.	
Příklad přijatelného řešení: • Specifické parametry přístroje, které mají být zabezpečeny, jsou uloženy na jednoúčelovou přídavnou jednotku, jež je zajištěna proti vyjmutí plombou, nebo jsou uloženy přímo v jednotce snímače. Přepsání parametrů je blokováno hardwarovým přepínačem, který je zaplombován. • Nechráněné nastavitelné parametry jsou uloženy do standardní paměti univerzálního počítače.	

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika C až D)**:** Zdrojový kód legálně relevantního softwaru.
Postup validace (kromě postupu požadovaného pro třídy rizika C až D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda jsou prostředky na ochranu parametrů dostatečné.

Třída rizika C	Třída rizika D
U8: Autentizace prezentovaných naměřených dat *Musí být zaručena autentičnost prezentovaných naměřených dat.*	

Upřesnění:

1. Naměřená data jsou považována za autentická, pokud jsou prezentována legálně relevantním softwarem.
2. Nesmí být možné napodobovat (fingovat) legálně relevantní software za účelem prezentace naměřených dat pomocí nástrojů operačního systému nebo jiných snadno dostupných ovládacích nástrojů.
3. Prezentovaná naměřená data musí být srozumitelná a jasně odlišitelná od jiných informací, informací nerelevantních z hlediska legální metrologie. V případě nutnosti musí být poskytnuto detailní označení.
4. Nelze-li plného zabezpečení dosáhnout prostředky operačního systému, musí být zajištěno technickými prostředky, že pouze legálně relevatní software provádí funkce relevantní z hlediska legální metrologie (např. snímač bude na univerzálním počítači pracovat pouze s příslušným legálně relevantním programem).
5. Pokud zdroj prezentovaných naměřených dat (např. senzor) není implicitně identifikovatelný či ověřitelný (např. existuje více senzorů či senzor je připojen vzdáleně), měřidlo musí poskytnout identifikaci příslušného zdroje. Jednoznačný identifikátor schváleného zdroje dat je legálně relevantním parametrem, na který se vztahují požadavky P6/U6 či P7/U7. V závislosti na typu datového připojení je nutno aplikovat požadavky rozšíření T.

Požadovaná dokumentace:

Dokumentace musí popisovat, jakým způsobem je zajištěna autentičnost naměřených dat.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda byla prezentovaná naměřená data generována legálně relevantním softwarem.
- Ověřte, zda mohou být naměřená data prezentována pouze legálně relevantním softwarem.
- Pokud zdroj prezentovaných naměřených dat není implicitně identifikovatelný či ověřitelný ověřte, zda zdroj těchto dat je identifikován a indikován legálně relevantním softwarem.

Ověření funkčnosti:

- Ověřte vizuálně, jestli jsou prezentovaná naměřená data snadno odlišitelná od jiných prezentovaných informací, které mohou být též prezentovány.
- Pokud je to relevantní vizuálně zkontrolujte, že prezentovaná naměřená data jsou korektně spjata s příslušným zdrojem.

Příklady přijatelných řešení:

1. Legálně relevantní software zobrazuje naměřená data v okně, které je vždy navrchu. Dokud jsou naměřená data zobrazována, legálně nerelevantní software k nim nemá přístup.

2a Jednotka snímače šifruje naměřené hodnoty klíčem známým autentickému softwaru běžícímu na univerzálním počítači (např. číslo jeho verze). Pouze tento věrohodný software dokáže naměřené hodnoty dešifrovat a použít. Neautentické programy běžící v počítači tento klíč neznají, a proto naměřené hodnoty nedokáží dešifrovat ani použít. Zacházení s klíči je popsáno v rozšíření T.

2b Snímač před posláním hodnot a zahájení komunikace s legálně relevantním softwarem univerzálního počítače provede na základě tajných klíčů „handshake“, tj. proces „potřesení rukou“. Snímač naměřené hodnoty pošle pouze tehdy, když program v univerzálním počítači komunikuje správně. Zacházení s klíči je popsáno v rozšíření T.

3. Klíč použitý v bodech 2a / 2b je volitelný a lze ho do snímače a do softwaru univerzálního počítače zapsat bez porušení plomby.	3. Klíč použitý v bodech 2a / 2b je hash kódem programu v univerzálním počítači. Při každé změně softwaru v univerzálním počítači je do senzoru vložen nový klíč, který je zabezpečený tak, aby ho nebylo možné změnit bez porušení plomby.
4. Pokud prezentovaná naměřená data nejsou explicitně spojena se senzorem, primární senzor přenáší data spolu s jednoznačnou identifikací sebe sama. Všechna prezentovaná naměřená data jsou označena identifikací příslušného senzoru. Identifikace každého senzoru je legálně relevantním parametrem, který lze i vyčíst na krytu senzoru.	

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika C až D)**:** Zdrojový kód legálně relevantního softwaru.
Postup validace (kromě postupu požadovaného pro třídy rizika C až D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda prezentovaná naměřená data generuje legálně relevantní software. • Ověřte, zda jsou všechny prostředky garantující prezentaci naměřených dat legálně relevantním softwarem přiměřené a vhodné.

Třídy rizika C až E
U9: Vliv jiného softwaru *Legálně relevantní software musí být navržen tak, aby ho nebylo možné nepřípustně ovlivnit jiným softwarem.*
Upřesnění: 1. Tento požadavek s sebou nese rozdělení softwaru na legálně relevantní a legálně nerelevantní software s ohledem na nejnovější poznatky softwarového inženýrství v oblasti modulárních či objektově orientovaných konceptů. Je nutné se řídit rozšířením S. U univerzálních počítačů se jedná o standardní záležitost.
Požadovaná dokumentace: Viz rozšíření S.
Postup validace: Viz rozšíření S.
Příklad přijatelného řešení: Viz rozšíření S.

6 Rozšíření L: Dlouhodobé uložení naměřených dat

Specifické požadavky této kapitoly se aplikují pouze když je navrženo dlouhodobé uložení naměřených dat. Doplňují specifické požadavky na vestavěný software jednoúčelových měřicích přístrojů (požadavky na přístroje typu P) a na software měřicích přístrojů využívajících univerzální počítač (požadavky na přístroje typu U).

Termín „dlouhodobé uložení“ označuje úsek od chvíle, kdy je měření fyzicky dokončeno, až do okamžiku ukončení všech procesů, jež mají být *legálně relevantním softwarem* provedeny. Tento termín může být rovněž použit k označení dlouhodobého uložení dat po takovém časovém úseku.

6.1 Technický popis

V následující tabulce jsou popsány tři různé technické konfigurace pro dlouhodobé uložení dat.

Pro jednoúčelové přístroje je typickým řešením integrovaná paměť, tato paměť je součástí metrologicky nezbytného hardwaru a softwaru.

Měřicí přístroje využívající univerzální počítač obvykle využívají již existující zdroje, např. harddisky.

Třetí variantou je vyjímatelná paměťová jednotka umožňující vyjmutí paměti z přístroje (ať již z jednoúčelového přístroje nebo z univerzálního počítače). Takovou paměťovou jednotku lze kamkoliv přenášet. Přístroj, který načte data z této výměnné paměťové jednotky (např. za účelem zobrazení, tisku stvrzenek, atd.) musí být předmětem legální kontroly.

A) Integrovaná paměť
Jednoduché zařízení, jednoúčelové, bez možnosti externích nástrojů či prostředků na editaci nebo změnu dat, integrovaná paměť pro naměřená data nebo parametry, např. RAM, flesh paměť, harddisk.
B) Paměť univerzálního počítače
Univerzální počítač, grafické uživatelské rozhraní, operační systém umožňující souběžné zpracování úloh, paralelní existence úloh, jež jsou/nejsou předmětem legální kontroly; paměť lze ze zařízení vyjmout, obsah lze kopírovat kdekoliv v počítači i mimo něj.
C) Vyjímatelná paměť nebo vzdálené (externí) úložiště
Libovolné základní zařízení (jednoúčelové nebo využívající univerzální počítač); paměť lze ze zařízení vyjmout. Může se jednat např. o paměť USB, paměťovou kartu, nebo vzdálené databáze připojené přes síť.

Tabulka 6-1: Technický popis pamětí pro dlouhodobé uložení dat

Na základě rozhodnutí příslušných pracovních skupin WELMEC může být u vybraných typů měřicích přístrojů členění omezeno, viz kapitola 10.

6.2 Specifické požadavky na software pro dlouhodobé uložení dat

Třída rizika B	Třída rizika C	Třída rizika D

L1 Úplnost uložených naměřených dat

Ukládaná naměřená data musí být doplněna všemi náležitými informacemi potřebnými pro legální účely.

Upřesnění:

1. Musí být možné zpětně dohledat měření, při němž uložená naměřená data vznikla.
2. Uložená naměřená data musejí být dostačující pro kontrolu faktur.
3. Druh požadované informace se může odvíjet od typu přístroje.
4. Předpokladem splnění tohoto specifického požadavku je označení každého jednotlivého uloženého bloku dat.

Požadovaná dokumentace:

Popis všech položek bloku dat.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda blok dat obsahuje všechny informace potřebné pro legálně relevantní účely.

Příklad přijatelného řešení:

- Blok dat, který je z legálního a metrologického hlediska úplný, musí být tvořen následujícími položkami:
  - naměřené hodnoty s dostatečným rozlišením
  - jednotka měření
  - cena za jednotku nebo cena k zaplacení (je-li relevantní)
  - datum a čas měření (je-li relevantní)
  - označení přístroje
  - místo měření (je-li relevantní)
- Data jsou uložena ve stejném rozlišení, hodnotách, jednotkách atd., jako je indikováno při měření nebo je vytištěno na dodacím dokladu.

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:**

Zdrojový kód legálně relevantního softwaru generujícího bloky dat, které mají být uloženy.

Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:**

Ověření na základě zdrojového kódu:

- Ověřte, zda jsou bloky dat správně sestavené.

Třída rizika B	Třída rizika C	Třída rizika D

L2: Ochrana proti náhodným či neúmyslným změnám
Uložená naměřená data musí být chráněna proti náhodným a neúmyslným změnám.

Upřesnění:

1. Uložená data musí být schopna detekovat náhodné změny dat způsobené fyzikálními vlivy (elektromagnetickým rušením, teplotou, vibracemi, atd.).
2. Musí být implementovány prostředky zabezpečení proti neúmyslným změnám nebo proti vymazání naměřených dat.

Požadovaná dokumentace:

Popis prostředků zabezpečení.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda je implementována metoda na detekci náhodných změn dat.
- Ověřte, zda tato metoda pokrývá všechna data.
- Ověřte, zda nemůže dojít k přepsání dat před koncem předpokládané doby jejich uložení.
- Ověřte, zda uživatel dostane upozornění, když chce změnit či vymazat naměřená data.

Ověření funkčnosti:

- Proveďte praktické namátkové testy, které ověří, zda uživatel před změnou/vymazáním naměřených dat dostane upozornění (pokud je vůbec možné provádět změny/smazání).

Příklad přijatelného řešení:

- Ukládaná naměřená data jsou doplněna dalšími kontrolními informacemi umožňujícími softwaru data načíst, vyhodnotit a zobrazit (viz L6)
- Pro detekci změny dat v důsledku fyzikálních vlivů je počítán kontrolní součet CRC-16 uloženého bloku dat a jeho hodnota je zapsána k ukládanému bloku dat.
  Poznámka: Algoritmus není tajný. Na rozdíl od požadavku L3 není utajen ani počáteční vektor CRC registru, ani generující polynom (tj. dělitel algoritmu). Počáteční vektor a generující polynom jsou známy jak programu, který vytváří kontrolní součty, tak programu, který je verifikuje.
- Naměřená data/faktury jsou chráněny připojeným časovým razítkem generovaným automaticky při jejich vytvoření a dále značkou nebo informací, zda faktury byly či nebyly zaplaceny. Obslužný program přesune/vymaže data pouze pokud faktury již byly zaplaceny, nebo se jedná o zastaralé faktury.
- Naměřená data nelze mazat bez předchozí autorizace, např. prostřednictvím dotazu v dialogovém okně nebo zprávou požadující potvrzení vymazání.
- Automatické přepisování naměřených dat je možné jen tehdy, když jsou záznamy, které jsou uloženy, odpovídajícím způsobem zabezpečeny. Parametr určující počet dní do data, kdy bude možné naměřená data vymazat, je nastaven a zabezpečen při uvedení do provozu dle potřeb uživatele a velikosti datového úložiště. Pokud je paměť plná a neobsahuje žádné dostatečně staré záznamy, které by mohly být přepsány, měření se zastaví. V takovém případě lze provést manuální mazání (s předchozí autorizací).

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:**
Zdrojový kód legálně relevantního softwaru zajišťující zabezpečení uložených dat.

Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:**

Ověření na základě zdrojového kódu:

- Ověřte, zda jsou prostředky zabezpečení uložených dat dostatečné a zda jsou správně implementované.

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">L3: Integrita dat
Uložená naměřená data musí být chráněna proti záměrným změnám.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Data uložená v integrovaných pamětech jsou obecně chráněna hardwarovými prostředky. Není nutné chránit je dalšími prostředky.
2. Musí být aplikovány prostředky ochrany proti záměrným změnám, které lze provést snadno dostupnými ovládacími softwarovými nástroji.
3. Uložená data musí být doplněna dalšími kontrolními informacemi umožňujícími ověření jejich integrity, a to při jejich vyčtení, vyhodnocení, zobrazení či jiném zpracování.</td></tr>
<tr><td colspan="2"></td><td>4. Prostředky zabezpečení musí rovněž zabránit záměrným změnám, které lze provést speciálními sofistikovanými softwarovými nástroji.
5. Při výběru vhodného algoritmu a minimální délky klíče musí být vzaty v úvahu požadavky a doporučení národních a mezinárodních institutů zodpovědných za bezpečnost dat.
6. I když bude algoritmus a klíč splňovat vysokou úroveň ochrany, technické řešení standardního osobního počítače tento stupeň ochrany nebude naplňovat, pokud nebudou existovat dostatečné prostředky ochrany pro programy, které podepisují nebo verifikují přenášená data (viz základní požadavky U pro univerzální počítače – poznámka k požadavku U6 - třída rizika D).</td></tr>
<tr><td colspan="2"></td><td></td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Je nutné zdokumentovat způsob realizace ochrany dat a označení poškozených dat.</td></tr>
<tr><td colspan="2">Postup validace:
Ověření na základě dokumentace:
• V případě použití kontrolního součtu nebo podpisu:
Ověřte, zda je kontrolní součet nebo podpis generován z celého bloku dat.
Ověřte, zda legálně relevantní software, který čte data a vypočítává kontrolní součet nebo dešifruje podpis, skutečně porovnává vypočtené hodnoty s nominálními.
• Ověřte, zda jsou neveřejné údaje (např. počáteční hodnota klíče, pokud je použita) zabezpečeny proti odhalení jednoduchými nástroji.</td><td>Postup validace (kromě postupu požadovaného pro třídy rizika B a C):
Ověření na základě dokumentace:
• Ověřte, zda přijatá opatření odpovídají nejnovějším požadavkům na vysoký stupeň ochrany.</td></tr>
<tr><td colspan="2">Příklad přijatelného řešení:
Uložená data jsou chráněna pomocí CRC-16.</td><td>Příklad přijatelného řešení:
Uložená data jsou chráněna pomocí kryptografického podpisu.</td></tr>
<tr><td colspan="3">Dodatky pro třídu rizika E</td></tr>
<tr><td colspan="3">Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D):
Zdrojový kód legálně relevantního softwaru, který zajišťuje integritu uložených dat.</td></tr>
</table>

Postup validace (kromě postupu požadovaného pro třídu rizika D)**:**

Ověření na základě zdrojového kódu:

- Ověřte, zda jsou prostředky zajištění integrity dostatečné a zda jsou správně implementovány.

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">L4 Dohledatelnost uložených naměřených dat
Musí být možné zpětně dohledat příslušné měření a měřicí přístroj, při němž uložená naměřená data vznikla.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Dohledatelnost vyžaduje vhodné přiřazení (prolinkování) naměřených dat s měřením, které data vygenerovalo.
2. Dohledatelnost vyžaduje vhodné přiřazení (prolinkování) naměřených dat s měřicím přístrojem, který data vygeneroval.
3. Předpokladem dohledatelnosti ke konkrétnímu měření je identifikace měření.
4. Předpokladem dohledatelnosti k měřicímu přístroji je identifikace měřicího přístroje.</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Popis metody zajišťující autentičnost dat.</td></tr>
<tr><td colspan="2">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda je každá naměřená hodnota správně přiřazena k příslušnému měření.
• V případě použití kontrolního součtu nebo podpisu ověřte, zda se kontrolní součet či podpis počítá z celého bloku dat.
• Ověřte, zda jsou neveřejné údaje (např. počáteční hodnota klíče, pokud je použita) zabezpečena proti odhalení jednoduchými nástroji.
Ověření funkčnosti:
• Ověřte, zda se příslušná uložená data shodují s daty vytištěnými na stvrzence nebo na faktuře.
• Ověřte, zda je na stvrzence znak, dle kterého je možné naměřená data porovnat s referenčními daty uloženými v paměti podléhající legální kontrole.</td><td>Postup validace (kromě postupu požadovaného pro třídy rizika B a C):
Ověření na základě dokumentace:
• Ověřte, zda přijatá opatření odpovídají nejnovějším požadavkům na vysoký stupeň ochrany.</td></tr>
<tr><td colspan="2">Příklad přijatelného řešení:
Uložený blok dat obsahuje následující prvky:
• Unikátní (pořadové) identifikační číslo a identifikaci měřicího přístroje, který hodnotu vygeneroval. Podpis, který je použit pro zajištění integrity dat, může být zároveň použit pro zajištění dohledatelnosti.
• Čas, kdy bylo měření provedeno (časové razítko) a identifikaci měřicího přístroje, který hodnotu vygeneroval.
Poznámka: Na stvrzence může být uvedeno, že naměřené hodnoty lze porovnat s referenčními hodnotami uloženými v paměti podléhající legální kontrole. Přiřazení je provedeno porovnáním identifikačního čísla nebo časového razítka na dodacím dokladu s údaji v uloženém bloku dat.</td><td>Příklad přijatelného řešení:
Kromě přijatelného řešení pro rizikové třídy B a C původ certifikátů používaných k podepsání naměřených dat je verifikován PKI.</td></tr>
</table>

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:** Zdrojový kód generující bloky dat určené k uložení a provádějící ověření.
Postup validace (kromě postupu požadovaného pro třídu rizika D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda jsou bloky dat správně sestaveny a spolehlivě ověřeny.

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">L5: Utajení klíčů
S klíči a s informacemi s nimi souvisejícími musí být nakládáno jako s naměřenými daty. Musí zůstat v tajnosti a musí být chráněny proti odhalení.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Tento požadavek je platný pouze v případě, že je tajný klíč použit.
2. Tento požadavek se vztahuje pouze na uchovávání naměřených dat v externí paměti (tj. paměti umístněné mimo přístroj, který měření provedl) nebo v paměti univerzálního počítače.
3. Pokud je přístup ke klíčům chráněn hardwarovými prostředky, nejsou nutné žádné další softwarové prostředky.
4. Musí být aplikovány prostředky ochrany proti záměrným změnám, které lze provést snadno dostupnými ovládacími softwarovými nástroji.
5. Pokud je místo algoritmu podpisu použit algoritmus kontrolního součtu, úlohu klíče zastává počáteční vektor nebo generující polynom.</td></tr>
<tr><td colspan="2"></td><td>6. Prostředky zabezpečení musí rovněž zabránit záměrným změnám, které lze provést speciálními sofistikovanými softwarovými nástroji.
7. Při výběru vhodného algoritmu a minimální délky klíče musí být vzaty v úvahu požadavky a doporučení národních a mezinárodních institutů zodpovědných za bezpečnost dat.
8. Technické řešení na bázi standardního osobního počítače není pro zajištění vysokého stupně ochrany dostatečné bez odpovídajících hardwarových prostředků ochrany klíče a dalších tajných údajů (viz základní požadavky pro univerzální počítače, U6).</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Popis správy klíčů a popis prostředků na uchování klíčů a s nimi souvisejících informací v tajnosti.</td></tr>
<tr><td>Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda nelze tajné informace odhalit.</td><td colspan="2">Postup validace (kromě postupu požadovaného pro třídy rizika B a C):
Ověření na základě dokumentace:
• Ověřte, zda přijatá opatření odpovídají nejnovějším požadavkům na vysoký stupeň ochrany.</td></tr>
<tr><td>Příklad přijatelného řešení:
Tajný klíč a s ním související informace jsou uloženy v binární podobě ve spustitelném kódu legálně relevantního softwaru. Software systému nenabízí žádné nástroje k zobrazení nebo editaci těchto údajů.</td><td colspan="2">Příklad přijatelného řešení:
Tajný klíč je uložen v části hardwaru, kterou lze fyzicky zaplombovat. Software nemá žádné nástroje umožňující zobrazení či editaci těchto údajů.
• Veřejný klíč k uchovávaným údajům, které jsou předmětem legální kontroly, byl autorizován v akreditovaném Trust centru.
• Veřejný klíč je možné číst přímo z přístroje, který je předmětem legální kontroly a který vyprodukoval příslušná data.</td></tr>
</table>

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:** Zdrojový kód zajišťující správu klíče.

Postup validace (kromě postupu požadovaného pro třídu rizika D)**:**

Ověření na základě zdrojového kódu:

- Ověřte, zda jsou prostředky pro správu klíčů dostatečné.

Třída rizika B	Třída rizika C	Třída rizika D

L6: Načtení, verifikace a zobrazení uložených dat
Načíst, verifikace či zobrazit uložená naměřená data může pouze legálně relevantní software.

Upřesnění:
1. Software musí být schopen zobrazit uložená naměřená data spolu s příslušnými informacemi (viz L1).
2. Vyvolaná data musí být verifikována.
3. Zobrazená nebo vytištěná naměřená data musí indikovat případné porušení dohledatelnosti či integrity.

Požadovaná dokumentace:
- Popis funkcí softwaru načítajícího data.
- Popis jak jsou označena poškozená data.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda je software načítající data schopen data správně zobrazit.

Ověření funkčnosti:

- Proveďte praktické namátkové testy k ověření, zda jsou při načtení zobrazeny všechny potřebné informace.

Příklad přijatelného řešení:
Integrita a dohledatelnost uložených naměřených dat jsou zajištěny podpisem celého datového bloku. Pokud verifikace podpisu selže, jsou naměřená data označena jako chybná, v opačném případě jsou vytištěna.

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:**
Zdrojový kód softwaru zajišťující načtení dat.

Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:**

Ověření na základě zdrojového kódu:

- Ověřte, zda jsou prostředky načítání, ověřování podpisů atd., dostatečné a zda jsou správně implementované.

Třída rizika B	Třída rizika C	Třída rizika D
L7: Automatické uložení *Naměřená data musí být po skončení měření uložena automaticky.*		
Upřesnění: 1. Funkce uložení nesmí být závislá na rozhodnutí operátora. 2. Pokud je na operátorovi požadováno rozhodnutí, zda přijmout či nepřijmout výsledek měření, musí být naměřená data uložena automaticky poté, co operátor takové rozhodnutí učiní.		
Požadovaná dokumentace: Popis automatického uložení. V případě, že o uložení rozhoduje operátor, pak také popis grafického uživatelského rozhraní.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda je proces uložení automatický. *Ověření funkčnosti:* • Proveďte praktické namátkové testy, zda se naměřené hodnoty po měření nebo po akceptaci výsledků měření automaticky uloží. Ověřte, zda menu neobsahuje žádná tlačítka či příkazy, které by automatické uložení přerušily či vypnuly.		
Příklad přijatelného řešení: V menu grafického uživatelského rozhraní není žádná položka či tlačítko, kterým by bylo možné manuálně spustit uložení naměřených výsledků. Naměřené hodnoty jsou společně s doplňujícími informacemi (jako jsou časové razítko, podpis) zabaleny do datového bloku, který je uložen automaticky ihned po měření či akceptaci výsledků měření.		

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:** Zdrojový kód legálně relevantního softwaru.
Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda jsou prostředky automatického uložení dostatečné a zda jsou správně implementovány.

Třída rizika B	Třída rizika C	Třída rizika D

L8: Kapacita paměti a kontinuita

Kapacita paměti pro dlouhodobé uložení dat musí být pro zamýšlené účely dostatečná.

Upřesnění:

1. Pokud je paměť plná nebo je-li paměť z přístroje vyjmuta či odpojena, operátor je o tom informován prostřednictvím výstrahy.
2. Musí být zajištěno, že lze přepsat pouze zastaralá data.
3. Minimální doba uložení naměřených dat a požadovaných informací se řídí národní legislativou, a proto se jimi tato příručka nezabývá.
4. Musí být zpřístupněny informace o kapacitě paměti.

Požadovaná dokumentace:

Kapacita paměti, popis správy uložených naměřených dat.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda dokumentace obsahuje údaje o kapacitě paměti nebo formulaci jejího výpočtu.
- Ověřte, zda před koncem doby uložení dat stanovené a zdokumentované výrobcem nemůže dojít k přepsání dat.

Ověření funkčnosti:

- Ověřte, zda se zobrazí varování, že je paměť plná nebo že byla odejmuta, pokud je to relevantní.

Příklad přijatelného řešení:

- Měření, která lze snadno a rychle přerušit: Když je paměť nedostupná před dokončením měření: Měřicí přístroj disponuje dostatečně velkou dočasnou pamětí pro uložení aktuální operace. Nelze následně zahájit další měření a hodnoty uložené v dočasné paměti jsou uchovány do chvíle, než mohou být přeneseny do archivní paměti.
- Měření, která nelze přerušit: Kumulativní údaje jsou vyčteny a přeneseny do paměti později, když je tato paměť opět k dispozici.
- Naměřená data jsou po prověření jejich stáří (příslušná doba uložení se řídí národní legislativou) automaticky přepsána. Před přepsáním dat je uživatel vyzván o povolení data vymazat a data jsou mazána počínaje nejstaršími.

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:**

Zdrojový kód legálně relevantního softwaru zajišťující uložení dat.

Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:**

Ověření na základě zdrojového kódu:

- Ověřte, zda jsou prostředky uložení dostatečné a zda jsou správně implementované.

7 Rozšíření T: Přenos naměřených dat komunikačními sítěmi

Specifické požadavky této kapitoly se aplikují pouze, když jsou naměřená data přenášena přes komunikační sítě do vzdáleného zařízení, kde jsou dále použita k legálně relevantním účelům příjemce. Tyto požadavky doplňují specifické požadavky na software jednoúčelových měřicích přístrojů (požadavky na přístroje typu P) a software měřicích přístrojů využívajících univerzální počítač (požadavky na přístroje typu U).

Toto rozšíření se nevztahuje na případy, kdy naměřená data nejsou následně zpracovávána k legálně relevantním účelům. Pokud je software stažen a nahrán do zařízení podléhajícího legální kontrole, vztahují se na něj požadavky rozšíření D.

7.1 Technický popis

V následující tabulce jsou popsány dvě síťové konfigurace.

Popis konfigurací
A) Uzavřená síť K síti je připojen pouze pevně daný počet účastníků s jednoznačnou identitou, funkcí a umístěním. Všechna zařízení v síti podléhají legální kontrole.
B) Otevřená síť K síti se může připojit libovolný počet účastníků (zařízení s libovolnými funkcemi). Ostatní účastníci nemusejí znát identitu, funkci a umístění připojených zařízení. Za otevřenou síť jsou považovány jakékoliv sítě se zařízeními podléhajícími legální kontrole, které mezi sebou komunikují přes infračervené komunikační rozhraní nebo bezdrátově.

Tabulka 7-1: Technický popis komunikačních sítí.

7.2 Specifické požadavky na software pro přenos dat

Třída rizika B	Třída rizika C	Třída rizika D
T1: Úplnost přenesených dat *Přenesená data musí obsahovat všechny odpovídající informace nutné k zobrazení či k dalšímu zpracování naměřených hodnot v přijímací jednotce.*		
Upřesnění: 1. Úplnost dat je individuální. Závisí na typu měření.		
Požadovaná dokumentace: Dokumentace všech položek bloku dat.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda blok dat obsahuje všechny informace potřebné pro další zpracování naměřených hodnot přijímací jednotkou.		
Příklad přijatelného řešení: Blok dat se skládá z následujících položek: • naměřené hodnoty ve správném rozlišení • správná jednotka míry (z legálního hlediska) • jednotková cena nebo celková cena k zaplacení (je-li relevantní) • datum a čas měření (je-li relevantní) • označení přístroje, je-li to relevantní (přenos dat) • místo měření (je-li relevantní)		

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:** Zdrojový kód generující bloky dat, které mají být přeneseny.
Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda jsou bloky dat správně sestaveny.

Třída rizika B	Třída rizika C	Třída rizika D

T2: Ochrana proti náhodným či neúmyslným změnám
Data musí být při přenosu chráněna proti náhodným a neúmyslným změnám.

Upřesnění:
1. Musí být implementovány prostředky na ochranu dat před jejich neúmyslnými změnami či smazáním.

Požadovaná dokumentace:
Popis použitých metod na detekci chyb během přenosu.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda je implementována metoda na detekci chyb během přenosu.

Příklad přijatelného řešení:

- Přenášená data jsou doplněna další kontrolní informací, tak aby mohl software přijímací jednotky detekovat náhodné chyby během přenosu.
- Detekce změn dat se provádí kontrolním součtem (algoritmem **CRC-16)** všech bytů datového bloku. Tento kontrolní součet se přiloží k přenášeným datům. Předtím než jsou data použita, přijímač znovu vypočítá hodnotu kontrolního součtu a porovná ji s přenesenou nominální hodnotou. Pokud se tyto hodnoty shodují, jsou data validní a mohou být použita. V opačném případě musí být vymazána nebo označena za neplatná.

  Poznámka: Algoritmus není tajný a na rozdíl od požadavku T3 není tajný ani počáteční vektor CRC registru, ani generující polynom, tj. dělitel algoritmu. Počáteční vektor a generující polynom jsou známy jak programu, který vytváří kontrolní součty, tak programu, který je verifikuje.
- Využití prostředků přenosových protokolů, např. TCP/IP, IFSF.

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:**
Zdrojový kód legálně relevantního softwaru zajišťující ochranu dat při přenosu.

Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:**

Ověření na základě zdrojového kódu:

- Ověřte, zda jsou prostředky ochrany dat při přenosu dostatečné a zda jsou správně implementovány.

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">T3: Integrita dat
Naměřená data musí být při přenosu chráněna proti záměrným změnám.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Tento požadavek se vztahuje pouze na otevřené sítě, nikoliv na sítě uzavřené.
2. Musí být aplikovány prostředky ochrany proti záměrným změnám, které lze provést snadno dostupnými ovládacími softwarovými nástroji.</td></tr>
<tr><td colspan="2"></td><td>3. Prostředky zabezpečení musí rovněž zabránit záměrným změnám, které lze provést speciálními sofistikovanými softwarovými nástroji.
4. Při výběru vhodného algoritmu a minimální délky klíče musí být vzaty v úvahu požadavky a doporučení národních a mezinárodních institutů zodpovědných za bezpečnost dat.
5. Aby byla zajištěna vysoká úroveň zabezpečení, je nutné aplikovat odpovídající prostředky ochrany softwaru, který podepisuje či verifikuje přenášená data (např. prostředky hardwarové) (viz také kapitola 5 pro software univerzálních počítačů, požadavek U6, upřesňující poznámka 6 pro třídu rizika D).</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Popis metody zabezpečení.</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
Zkontrolujte, zda byla zvolena vhodná metoda.</td></tr>
<tr><td colspan="2">Příklad přijatelného řešení:
• Přenášená data jsou doplněna další kontrolní informací, tak aby mohl software přijímací jednotky detekovat náhodné chyby během přenosu.
• Z dat, která mají být přenesena, je vygenerován kontrolní součet. Předtím než jsou data použita, je znovu vypočtena hodnota kontrolního součtu a porovnána s přenesenou nominální hodnotou. Pokud se tyto hodnoty shodují, jsou data validní a mohou být použita. V opačném případě musí být vymazána nebo označena za neplatná.
• Přijatelným řešením je algoritmus CRC-16.

<u>Poznámka:</u> Algoritmus není tajný, ale na rozdíl od požadavku T2 je tajný počáteční vektor CRC registru nebo generující polynom (tj. dělitel algoritmu). Počáteční vektor a generující polynom jsou známy pouze programům vytvářejícím a verifikujícím kontrolní součty. Je třeba k nim přistupovat jako ke klíčům (viz T5).</td><td>Příklad přijatelného řešení:
• Přenášená data jsou doplněna další kontrolní informací, tak aby mohl software přijímací jednotky detekovat náhodné chyby během přenosu.
• Namísto CRC se generuje podpis.
• Ochranu zajišťuje přenosový protokol, např. HTTPS, TLS.</td></tr>
<tr><td colspan="3">Dodatky pro třídu rizika E</td></tr>
<tr><td colspan="3">Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D):
Zdrojový kód legálně relevantního softwaru zajišťující integritu ochrany dat při přenosu.</td></tr>
<tr><td colspan="3">Postup validace (kromě postupu požadovaného pro třídy rizika B až D):
Ověření na základě zdrojového kódu:
• Ověřte, zda jsou prostředky zajišťující integritu dat při přenosu dostatečné.</td></tr>
</table>

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">T4: Dohledatelnost přenesených naměřených dat
Musí být možné zpětně dohledat příslušné měření a měřicí přístroj, při němž přenesená naměřená data vznikla.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Tento požadavek se vztahuje pouze na otevřené sítě, nikoliv na uzavřené sítě.
2. Dohledatelnost vyžaduje vhodné přiřazení (prolinkování) naměřených dat s měřením, které data vygenerovalo.
3. Dohledatelnost vyžaduje vhodné přiřazení (prolinkování) naměřených dat s měřicím přístrojem, který data vygeneroval.
4. Předpokladem dohledatelnosti ke konkrétnímu měření je identifikace měření.
5. Předpokladem dohledatelnosti k měřicímu přístroji je identifikace měřicího přístroje.
6. Musí být aplikovány prostředky ochrany proti záměrným změnám, které lze provést snadno dostupnými ovládacími softwarovými nástroji.</td></tr>
<tr><td colspan="2"></td><td>7. Prostředky zabezpečení musí rovněž zabránit záměrným změnám, které lze provést speciálními sofistikovanými softwarovými nástroji.
8. Při výběru vhodného algoritmu a minimální délky klíče musí být vzaty v úvahu požadavky a doporučení národních a mezinárodních institutů zodpovědných za bezpečnost dat.</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
• Popis způsobu prokázání věrohodnosti.</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
Zkontrolujte, zda jsou metody prokázání věrohodnosti dostatečné.</td></tr>
<tr><td colspan="3">Příklad přijatelného řešení:
• Každý blok dat má unikátní (pořadové) identifikační číslo, které obsahuje datum, kdy měření proběhlo (časové razítko).
• Každý blok dat obsahuje informace o původu naměřených dat, tj. sériové číslo nebo označení měřicího přístroje, který měření uskutečnil.
• V otevřených sítích je autentičnost dat zaručena tehdy, když je blok dat opatřen jednoznačným podpisem, který se vztahuje na všechny položky přenášených dat.
• Při příjmu dat je kontrolována jejich věrohodnost.</td></tr>
<tr><td colspan="2"></td><td></td></tr>
</table>

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:** Zdrojový kód legálně relevantního softwaru vysílacího a přijímacího zařízení.
Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:** *Ověření na základě zdrojového kódu:* • Ověření, zda jsou prostředky zaručující autentičnost dat při přenosu dostatečné.

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">T5: Utajení klíčů
S klíči a s informacemi s nimi souvisejícími musí být nakládáno jako s naměřenými daty. Musí zůstat v tajnosti a musí být chráněny proti odhalení.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Tento požadavek je platný pouze v případě, že je tajný klíč použit.
2. Musí být aplikovány prostředky ochrany proti záměrným změnám, které lze provést snadno dostupnými ovládacími softwarovými nástroji.
3. Pokud je přístup ke klíčům chráněn hardwarovými prostředky, nejsou nutné žádné další softwarové prostředky.</td></tr>
<tr><td colspan="2"></td><td>4. Prostředky zabezpečení musí rovněž zabránit záměrným změnám, které lze provést speciálními sofistikovanými softwarovými nástroji.
5. Při výběru vhodného algoritmu a minimální délky klíče musí být vzaty v úvahu požadavky a doporučení národních a mezinárodních institutů zodpovědných za bezpečnost dat.
6. Technické řešení na bázi standardního osobního počítače není pro zajištění vysokého stupně ochrany dostatečné bez odpovídajících hardwarových prostředků ochrany klíče a dalších tajných údajů (viz základní požadavky pro univerzální počítače U6).</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Popis správy klíčů a popis prostředků na uchování klíčů a s nimi souvisejících informací v tajnosti.</td></tr>
<tr><td colspan="2">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda nelze tajné informace odhalit.</td><td>Postup validace (kromě postupu požadovaného pro třídy rizika B a C):
Ověření na základě dokumentace:
• Ověřte, zda přijatá opatření odpovídají nejnovějším požadavkům na vysoký stupeň ochrany.</td></tr>
<tr><td colspan="2">Příklad přijatelného řešení:
Tajný klíč a s ním související informace jsou uloženy v binární podobě ve spustitelném kódu legálně relevantního softwaru. Tudíž není známa adresa, kde jsou tyto informace uloženy. Software systému nenabízí žádné nástroje k zobrazení nebo editaci těchto údajů. Pokud je místo algoritmu podpisu použit algoritmus kontrolního součtu, úlohu klíče zastává počáteční vektor nebo generující polynom.</td><td>Příklad přijatelného řešení:
Tajný klíč je uložen v části hardwaru, kterou lze fyzicky zaplombovat. Software nemá žádné nástroje umožňující zobrazení či editaci těchto údajů.
• Veřejný klíč k uchovávaným údajům, které jsou předmětem legální kontroly, byl autorizován v akreditovaném Trust centru.
• Veřejný klíč je možné číst přímo z přístroje, který je předmětem legální kontroly a který vyprodukoval příslušná data.</td></tr>
</table>

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:** Zdrojový kód legálně relevantního softwaru zajišťující nakládání s klíči.
Postup validace (kromě postupu požadovaného pro třídu rizika D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda jsou prostředky pro správu klíčů dostatečné.

Třída rizika B	Třída rizika C	Třída rizika D
T6: Příjem, verifikace a zacházení s přenesenými naměřenými daty *Příjem naměřených dat, jejich verifikaci a zacházení musí provádět legálně relevantní software.*		
Upřesnění: 1. Komunikační protokoly obvykle opakují přenos dat tak dlouho, dokud neproběhne bez chyby. Přesto je však možné, že přijatý blok dat bude poškozený. 2. Přijatá naměřená data musí indikovat případnou odchylku v dohledatelnosti či integritě.		
Požadovaná dokumentace: Popis detekce chybných dat.		
Postup validace: *Ověření na základě dokumentace a ověření funkčnosti:* • Ověřte, zda jsou poškozená data detekována a označena.		
Příklad přijatelného řešení: Když program, který přijímá data, verifikuje je a dále s nimi zachází, zjistí nesoulad při ověření podpisu, nejprve se, pokud má k dispozici redundantní informace, pokusí obnovit původní hodnotu. Pokud obnova selže, program vygeneruje upozornění pro uživatele, nezveřejní naměřenou hodnotu a označí poškozený blok dat značkou ve speciálním poli (stavovém poli) jako „neplatný“.		

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:** Zdrojový kód legálně relevantního softwaru přijímacího zařízení.
Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda jsou prostředky zacházení s poškozenými daty dostatečné.

Třída rizika B	Třída rizika C	Třída rizika D
T7: Zpoždění při přenosu *Měření nesmí být nepřípustně ovlivněno zpožděním při přenosu.*		
Upřesnění: 1. Načasování přenosu dat musí být takové, aby ani v nehorším případě nedošlo k nepřípustnému ovlivnění měření.		
Požadovaná dokumentace: Popis způsobu, jak je měření chráněno proti zpožděním při přenosu.		
Postup validace: • Ověřte koncept ochrany, zda není měření ovlivněno zpožděním při přenosu.		
Příklad přijatelného řešení: Implementace komunikačních protokolů pro sběrnice „field bus“.		

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B, C a D)**:** Zdrojový kód legálně relevantního softwaru zajišťující přenos dat.
Postup validace (kromě postupu požadovaného pro třídy rizika B, C a D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda jsou prostředky přijaté pro zacházení se zpožděním při přenosu dostatečné.

Třída rizika B	Třída rizika C	Třída rizika D
T8: Dostupnost přenosových služeb *V případě nedostupnosti služeb sítě nesmí dojít ke ztrátě naměřených dat.* **Upřesnění:** 1. Naměřená data se odložením přenosu nebo potlačením přenosu nesmí poškodit. 2. Přístroj vysílající data musí být schopen zvládat náhodné poruchy přenosu. 3. Reakce měřicího přístroje na výpadek přenosových služeb závisí na principu měření (viz Rozšíření I).		
Požadovaná dokumentace: Popis prostředků zabezpečení při rušení přenosu nebo jiných výpadcích.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte přijaté prostředky ochrany naměřených dat před rušením a výpadky během přenosu. *Ověření funkčnosti:* • Namátkovými kontrolami ověřte, že v důsledku přerušení přenosu nedojde ke ztrátě relevantních dat.		
Příklad přijatelného řešení: 1) Měření, která lze snadno a rychle přerušit: Měření lze dokončit i v případě výpadku přenosu. Nicméně měřicí přístroj nebo zařízení, které přenáší naměřená data, má dostatečně velkou dočasnou paměť pro uložení aktuální operace. Nelze následně zahájit další měření a hodnoty uložené v dočasné paměti jsou uchovány do chvíle, než mohou být přeneseny. Více příkladů naleznete v části I. 2) Měření, která nelze přerušit: Kumulativní údaje jsou vyčteny a přeneseny později, když je toto spojení opět obnoveno.		

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:** Zdrojový kód legálně relevantního softwaru zajišťující přenos dat.
Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda jsou prostředky reakce na přerušení přenosu dostatečné.

8 Rozšíření S: Oddělení softwaru

Oddělení softwaru je volitelný způsob umožňující rozlišit legálně relevantní software od legálně nerelevantního softwaru. Komunikaci mezi těmito oddělenými částmi softwaru zajišťují ochranná rozhraní. Pokud výrobce splní podmínky oddělení softwaru, nemusí při změně legálně nerelevantního softwaru podstupovat procedury schvalování typu.

Pokud se na přístroj vztahují specifické požadavky této kapitoly, jsou považovány za doplněk k základním požadavkům na typy přístrojů P a U uvedených v kapitolách 4 a 5 této příručky.

8.1 Technický popis

Měřicí přístroje či systémy řízené softwarem jsou obecně komplexní a jsou tvořeny legálně relevantními i legálně nerelevantními moduly. Je výhodné (nikoliv však povinné) tyto typy softwarových modulů oddělit.

8.2 Specifické požadavky na software v případě oddělení softwaru

Třída rizika B	Třída rizika C	Třída rizika D

S1: Realizace oddělení softwaru

Část softwaru obsahující legálně relevantní software a parametry musí být jednoznačně oddělena od ostatních částí softwaru.

Upřesnění:

1. Do legálně relevantního softwaru náleží všechny *části softwaru* (programové jednotky, podprogramy, procesy, funkce, třídy, programy, knihovny atd.), které se
   - podílejí na kalkulaci naměřených hodnot nebo ji ovlivňují,
   - podílejí na pomocných funkcích, jako je např. zobrazování dat, zabezpečení dat, uložení dat, označení softwaru, provádění stahování softwaru, přenos nebo uložení dat, verifikace přijatých nebo uložených dat atd.

   Všechny *proměnné, dočasné soubory a parametry,* které mají vliv na naměřená data nebo na legálně relevantní software, rovněž patří do legálně relevantního softwaru.
2. Součástí legálně relevantního softwaru je i samotné ochranné rozhraní softwaru (viz S3).
3. Ostatní jednotky programu, data nebo parametry, které nejsou uvedeny výše, představují legálně nerelevantní software.

Požadovaná dokumentace:

Pojmenování všech komponent, které tvoří legálně relevantní software.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda je pojmenování správné a seznam komponent kompletní.

Příklad přijatelného řešení:

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:**

Zdrojový kód legálně relevantního softwaru.

Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:**

Ověření na základě zdrojového kódu:

- Proveďte kontrolu (např. analýzou toku dat pomocí nástrojů nebo manuálně), zda jsou všechny jednotky programu, programy nebo knihovny podílející se na zpracování naměřených hodnot kvalifikovány do legálně relevantního softwaru.

Třída rizika B	Třída rizika C	Třída rizika D
S2: Smíšená indikace *Informace generované legálně nerelevantním softwarem musí být na displeji nebo tištěném výstupu zobrazeny či uvedeny tak, aby nemohlo dojít k jejich záměně s informacemi generovanými legálně relevantním softwarem.*		
Upřesnění: ---		
Požadovaná dokumentace: Popis legálně relevantního softwaru, který zajišťuje indikaci. Popis toho, jak je indikace legálně relevantních informací chráněna před záměnou s informacemi generovanými legálně nerelevantním softwarem.		
Postup validace: *Ověření funkčnosti:* • Vizuálně ověřte, zda nelze zaměnit doplňující informace generované legálně nerelevantním softwarem a prezentované na displeji nebo tištěném výstupu s informacemi generovanými legálně relevantním softwarem.		
Příklad přijatelného řešení: • Pokud mají být legálně relevantní informace doplněny dalšími informacemi, jejichž část je legálně nerelevantní (např. označení produktu), musí být definováno schéma indikace, které bude kontrolováno legálně relevantním softwarem. Aby blo zajištěno, že všechny legálně relevantní informace jsou ze vstupu extrahovány, musí legálně relevantní informace procházet filtrem, který je součástí legálně relevantního softwaru a detekuje nepřípustné informace, např. jednotky měření. Přípustné informace jsou pak vloženy do schématu indikací, který je kontrolován legálně relevantním softwarem.		

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:** Zdrojový kód legálně relevantního softwaru.
Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda legálně relevantní software generuje indikaci naměřených hodnot. • Ověřte, zda je realizovaná implementace smíšené indikace správná. • Ověřte, zda indikace nemůže být měněna či potlačena legálně nerelevantními programy.

Třída rizika B	Třída rizika C	Třída rizika D

S3: Ochranné rozhraní softwaru

Výměna dat mezi legálně relevantním softwarem a legálně nerelevantním softwarem musí probíhat výhradně přes ochranné rozhraní.

Upřesnění:

1. Tento požadavek se vztahuje na všechny typy interakcí a výměn dat mezi legálně relevantním a legálně nerelevantním softwarem.
2. Veškerá komunikace musí být výhradně realizována přes definované ochranné rozhraní.
3. Přípustné jsou pouze takové interakce a toky dat, které nemají nepřípustný vliv na proces měření, zejména na legálně relevantní software, specifické parametry přístroje a naměřená data.
4. Legálně nerelevantní software nesmí ovlivňovat řád a průběh procesu měření.

Požadovaná dokumentace: Popis softwarového rozhraní

- Popis ochranného rozhraní včetně popisu povolených interakcí a toků dat.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda jsou definovány a popsány všechny funkce legálně relevantního softwaru a úkony procesu měření, které lze spustit přes ochranné rozhraní.
- Ověřte, zda jsou definována a popsána data, která lze přes toto rozhraní posílat.
- Proveďte kontrolu věrohodnosti, zda je popis interakcí a výměn dat kompletní.

Příklad přijatelného řešení:

- Datové domény legálně relevantní části softwaru jsou „zapouzdřené“ a to tak, že jsou v této části programu deklarovnány pouze lokálních proměnné.
- Rozhraní je realizováno jako podprogram legálně relevantního softwaru, který je vyvolán legálně nerelevantním softwarem. Data, která mají být přenesena do legálně relevantního softwaru, jsou předávána jako parametry podprogramu.
- Legálně relevantní software odfiltrovává nepřípustné příkazy rozhraní.

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:**

Zdrojový kód legálně relevantního softwaru.

Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:**

Ověření na základě zdrojového kódu:

- Zkontrolujte návrh softwaru. Jestli je tok dat jednoznačně definován legálně relevantním softwarem a zda je možné ho ověřit.
- Ověřte tok dat přes ochranné rozhraní s použitím odpovídajících nástrojů příp. manuálně. Ověřte, zda je zdokumentován veškerý tok dat mezi jednotlivými částmi softwaru. Pátrejte po nepřípustném toku dat.
- Ověřte, zda jsou zdokumentovány interakce vyvolané legálně nerelevantním softwarem. Pátrejte po nepřípustných interakcích.

9 Rozšíření D: Stahování legálně relevantního softwaru

Toto rozšíření je nutné aplikovat na přístroje vybavené nástroji na stahování softwaru bez porušení plomby. Požadavky zde uvedené jsou pouze doplněním základních požadavků na přístroje typu P nebo U popsaných v kapitolách 4 a 5 této příručky.

Tato příručka nezavádí žádná nařízení s ohledem na povolení či omezení stahovat software do měřicích přístrojů v provozu bez nutnosti porušení plomby. Pokud je nicméně stahování softwaru do přístroje bez porušení plomby povoleno, pak je nutné zohlednit specifické požadavky tohoto rozšíření.

9.1 Technický popis

Rozsah konfigurací, které jsou pro stahování softwaru obecně možné, je rozsáhlý. Viz popis v následující tabulce.

Konfigurace hardwaru Přístroje s nástroji na stahování softwaru mohou být buď jednoúčelové (typ P), nebo se může jednat o přístroje využívající univerzální počítač (typ U). Spojení pro přenos softwaru může být přímé (např. RS 232, USB), nebo může využívat uzavřenou síť (např. ethernet, síť LAN postavenou na technologii Token ring) či otevřenou síť (např. internet).
Konfigurace softwaru Celý software, který má být stažen, může být legálně relevantní nebo může být legálně relevantní software oddělen od legálně nerelevantního softwaru. V případě oddělení softwaru bude předmětem níže uvedených požadavků pouze stahování legálně relevantního softwaru. Pokud bylo oddělení softwaru certifikováno, lze legálně nerelevantní software stahovat bez jakéhokoliv omezení.

Tabulka 9-1: Technický popis konfigurací pro automatické stahování softwaru.

Stahování softwaru tvoří dvě (logické) etapy: (1) Proces přenosu na měřicí přístroj a (2) instalace přeneseného softwaru.

9.2 Specifické požadavky na software

Třída rizika B	Třída rizika C	Třída rizika D

D1: Mechanismus stahování
Obě etapy stahování softwaru, přenos i následná instalace softwaru, musí probíhat automaticky a bez vlivu na zabezpečení legálně relevantního softwaru

Upřesnění:

1. Přístroj musí být vybaven legálně relevantním softwarem, který provádí kontrolu funkcí dle požadavků D2 až D4.
2. Přístroj musí být schopen detekovat selhání přenosu softwaru nebo následné instalace. Musí být zobrazeno upozornění. Neúspěšný přenos nebo instalace nebo přerušení přenosu či instalace nesmí ovlivnit původní stav měřicího přístroje. Jinak musí být na přístroji trvale zobrazeno chybové hlášení a dokud nebude chyba odstraněna, nebude možné přístroj použít k dalšímu měření.
3. Po úspěšném dokončení instalace musí být aktivovány všechny prostředky zabezpečení.
4. Při přenosu a následné instalaci softwaru musí být pozastaven proces měření nebo musí být odpovídajícím způsobem zajištěna správnost měření.
5. Počet opakovaných pokusů o přenos a instalaci musí být přiměřeně omezen.

Požadovaná dokumentace:

Dokumentace musí popisovat způsob implementace podmínek uvedených v části „Upřesnění“.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda jsou splněny podmínky uvedené v části „Upřesnění“.

Ověření funkčnosti:

- Proveďte alespoň jedno stažení softwaru z důvodu kontroly, zda proběhlo správně.

Příklad přijatelného řešení:

Celá část tvořená legálně relevantním softwarem je neměnná, tj. nedovoluje stahování či změny bez porušení plomby.

Pomocný program trvale uložený v legálně relevantní části softwaru, který:

a. navazuje spojení s vysílatelem a kontroluje povolení
b. automaticky zamezuje měření při přenosu a instalaci
c. automaticky přenáší legálně relevantní software do zabezpečené dočasné oblasti
d. automaticky provádí kontroly požadované dle D2 až D4
e. automaticky instaluje software do správného umístění
f. provádí interní organizaci, tj. maže záložní soubory atd.
g. zajišťuje, aby bezpečnostní prvky, které byly kvůli usnadnění přenosu a instalace vyřazeny, byly po dokončení těchto operací zase automaticky nastaveny na požadovanou úroveň
h. zahajuje odpovídající procesy oprav, pokud dojde k poruše.

V členských státech, v nichž není povoleno stahování softwaru do přístrojů v provozu, musí existovat možnost zablokovat funkci stahování softwaru a to zabezpečovacími prostředky (přepínač, zabezpečený parametr). V tomto případě nesmí být možno legálně relevantní software stáhnout bez porušení plomby/zabezpečení.

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:**
Část zdrojového kódu legálně relevantního softwaru zajišťující řízení procesu stahování.

Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:**

Ověření na základě zdrojového kódu:

- Ověřte, zda jsou prostředky pro řízení procesu stahování dostatečné.

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">D2: Prokázání věrohodnosti přeneseného softwaru
Je třeba implementovat prostředky zaručující autentičnost přeneseného softwaru.
Upřesnění:
1. Před instalací přeneseného softwaru musí proběhnout následující kontroly:
a. kontrola autentičnosti softwaru,
b. kontrola, zda software patří k měřicímu přístroji, na nějž má být nainstalován.
2. Přinese-li tato kontrola negativní výsledek, bude to považováno za chybu přenosu a dále je nutné postupovat dle požadavků D1.</td></tr>
<tr><td colspan="2"></td><td>3. Při výběru vhodného algoritmu a minimální délky klíče musí být vzaty v úvahu požadavky a doporučení národních a mezinárodních institutů zodpovědných za bezpečnost dat.</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Dokumentace musí popisovat způsob provádění kontrol uvedených v části „Upřesnění“.</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda jsou popisované kontroly dostatečné.
Ověření funkčnosti:
• Ověřte, zda je zamezeno instalaci neautentického softwaru nebo softwaru, který nepatří k danému měřicímu přístroji.</td></tr>
<tr><td colspan="3">Příklad přijatelného řešení:
1. Autentičnost: Z důvodu ochrany integrity softwaru (viz D3) je generován elektronický podpis části softwaru, která má být stažena. Autentičnost je zaručena tehdy, když klíč uložený v legálně relevantním softwaru přístroje potvrdí, že podpis byl vytvořen autorizovaným orgánem. Kontrola podpisu probíhá automaticky. Klíč může být změněn pouze po porušení plomby.
2. Správný typ měřicího přístroje
Kontrola typu přístroje se provádí automatickým porovnáním označení typu přístroje uloženého v legálně relevantním softwaru přístroje se seznamem kompatibilních přístrojů, který je součástí softwaru.</td></tr>
<tr><td colspan="2"></td><td></td></tr>
</table>

<table>
<tr><th>Dodatky pro třídu rizika E</th></tr>
<tr><td>Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D):
Zdrojový kód legálně relevantní části softwaru zajišťující ověření autentičnosti.</td></tr>
<tr><td>Postup validace (kromě postupu požadovaného pro třídy rizika B až D):
Ověření na základě zdrojového kódu:
• Ověřte, zda jsou implementovány prostředky kontroly podmínek uvedených v části „Upřesnění“.</td></tr>
</table>

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">D3: Integrita stahovaného softwaru
Je třeba použít prostředky zabraňující změně softwaru při přenosu.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Před instalací přeneseného softwaru je nutné zkontrolovat, zda nebyl software při přenosu změněn.
2. Přinese-li tato kontrola negativní výsledek, bude to považováno za chybu přenosu a dále je nutné postupovat dle požadavků D1.</td></tr>
<tr><td colspan="2"></td><td>3. Při výběru vhodného algoritmu a minimální délky klíče musí být vzaty v úvahu požadavky a doporučení národních a mezinárodních institutů zodpovědných za bezpečnost dat.</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Dokumentace musí popisovat způsob provádění kontrol.</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda je popsaná kontrola dostatečná.
Ověření funkčnosti:
• Ověřte, zda je zamezeno instalaci změněného softwaru.</td></tr>
<tr><td colspan="2">Příklad přijatelného řešení:
• Integritu softwaru lze ověřit přepočtem kontrolního součtu legálně relevantního softwaru a porovnáním příslušného výsledku s kontrolním součtem skrytým v softwaru.
• Přijatelný algoritmus: CRC, tajný počáteční vektor, délka 32 bitů. Počáteční vektor je uložen v legálně relevantní části softwaru.</td><td>Příklad přijatelného řešení:
• Jako podpis je použit algoritmus SHA s RSA. Dešifrovací klíč je uložen v legálně relevantní části softwaru a nelze ho změnit nebo vyčíst bez porušení plomby.</td></tr>
</table>

<table>
<tr><th>Dodatky pro třídu rizika E</th></tr>
<tr><td>Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D):
Zdrojový kód legálně relevantní části softwaru zajišťující kontrolu integrity softwaru.</td></tr>
<tr><td>Postup validace (kromě postupu požadovaného pro třídy rizika B až D):
Ověření na základě zdrojového kódu:
• Ověřte, zda jsou prostředky kontroly integrity dostatečné.</td></tr>
</table>

Třída rizika B	Třída rizika C	Třída rizika D

D4: Dohledatelnost stahovaného legálně relevantního softwaru
Za účelem následných kontrol musí být v přístroji zajištěna odpovídajícími technickými prostředky zpětná návaznost a dohledatelnost stahovaných legálně relevantních softwarů.

Upřesnění:
1. Musí být zaznamenána a zabezpečena všechna relevantní data umožňující dohledat stahování nebo pokus o stahování softwaru. Patří k nim např. datum a čas stahování, označení softwaru, původce přenosu, oznámení o úspěšnosti přenosu a instalace.
2. Zaznamenaná data musejí být dostupná po adekvátní dobu (délka této doby je určena nařízeními mimo rámec MID).
3. Zaznamenaná data musí být na vyžádání zobrazena.
4. Prostředky a záznamy sloužící k dohledatelnosti jsou součástí legálně relevantního softwaru, a jako takové musejí být náležitým způsobem chráněny.

Požadovaná dokumentace:
Dokumentace musí popisovat:
- způsob implementace a zabezpečení prostředků návaznosti a dohledatelnosti,
- strukturu záznamů,
- způsob, jak lze zaznamenané informace zobrazit

Postup validace:

Ověření na základě dokumentace:
- Ověřte, zda implementované prostředky dohledatelnosti splňují podmínky uvedené v části „Upřesnění“.

Ověření funkčnosti:
- Ověřte funkčnosti prostředků při stahování softwaru.

Postup validace (kromě postupu požadovaného pro třídy rizika B a C)**:**

Ověření na základě dokumentace:
- Ověřte, zda přijatá opatření odpovídají nejnovějším požadavkům na vysoký stupeň ochrany.

Příklad přijatelného řešení:
- Záznam událostí: Měřicí přístroj je vybaven záznamníkem událostí, který automaticky zaznamenává minimálně datum a čas stahování, označení stahovaného legálně relevantního softwaru, označení vysílací strany a záznam o úspěšnosti procesu. Záznam o úspěšnosti stahování se vytvoří při každém pokusu o stažení softwaru bez ohledu na jeho výsledek.
- Po dosažení limitu kapacity záznamíku událostí musí technologické prostředky zabránit dalšímu stahování softwaru. Záznamník událostí lze vymazat pouze po porušení plomby. Umístit novou plombu je oprávněn pouze kontrolní úřad.

Dodatky pro třídu rizika E

Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D)**:**
Zdrojový kód legálně relevantní části softwaru zajišťující sledování procesů stahování.

Postup validace (kromě postupu požadovaného pro třídu rizika D)**:**

Ověření na základě zdrojového kódu:
- Ověřte, zda jsou prostředky sledování procesů stahování dostatečné.
- Ověřte, zda jsou prostředky zabezpečení uložených dat dostatečné.

10 Rozšíření I: Požadavky na software přístrojů konkrétního typu

Toto rozšíření pouze doplňuje obecné požadavky na software uvedené v předchozích kapitolách a nelze jej tedy vnímat odděleně od částí P nebo U či od ostatních rozšíření (viz kapitola 2). Je obdobou příloh MI-x směrnice MID určených pro konkrétní typy přístrojů. Věnuje se specifickým vlastnostem měřicích přístrojů nebo systémů (či podsestav) a požadavkům na ně. Žádné z těchto požadavků nicméně nepřesahují rámec směrnice MID. Na doporučení organizace OIML nebo na normy ISO/IEC je v následujícím textu odkazováno pouze tehdy, když jsou v souladu se směrnicí MID a výkladem jejích požadavků.

Rozšíření I se zabývá vlastnostmi softwaru daných měřicích přístrojů a uvádí, jaké jsou na něj kladeny požadavky. Kromě toho měřicím přístrojům přiřazuje určitou třídu rizika dle typu (kategorie) přístroje. Tím je zajištěna harmonizace na rovině zkoušení, zabezpečení a shody daného softwaru.

Rozšíření I by v tuto chvíli mělo představovat první návrh, jenž bude příslušnými odbornými pracovními skupinami WELMEC v budoucnu dále doplňován. Má proto otevřenou strukturu - vytváří jakousi kostru, která je s výjimkou přiřazení tříd rizika vyplněna pouze částečně (např. u měřičů spotřeby a automatických vážicích přístrojů). Na základě zkušeností a rozhodnutí příslušných pracovních skupin WELMEC může být toto rozšíření použito i pro jiné přístroje MID (a také pro přístroje, které v této směrnici nejsou zahrnuté). Číslování „x“ podkapitol (10.x) se řídí číslováním specifických příloh směrnice MID (MI-x). Přístroje nezahrnuté do směrnice MID lze přidávat od kapitoly 10.11 dále.

Software každého přístroje má určité specifické vlastnosti, které u určitého typu „x“ měřicího přístroje musí být zohledněny. O těchto vlastnostech by mělo být systematicky pojednáno následujícím způsobem: každá podkapitola 10.x by měla být dále rozdělena do podkapitol 10.x.y, kde se bude část „y“ zabývat následujícími vlastnostmi:

10.x.1 Zvláštní předpisy, normy a jiné normativní dokumenty

V tomto oddílu by měly být uvedeny zvláštní předpisy, normy a jiné normativní dokumenty vztahující se ke konkrétnímu přístroji (nebo kategorii přístrojů), např. doporučení organizace OIML nebo směrnice WELMEC, které mohou být užitečné při vývoji zvláštních požadavků na software pro příslušný přístroj (či kategorii přístrojů) s ohledem na interpretaci požadavků uvedených v Příloze 1 směrnice MID a specifických příloh MI-x.

Specifické požadavky na software obvykle doplňují obecné požadavky uvedené v předchozích kapitolách. Pokud tomu tak není, mělo by být jednoznačně uvedeno, zda specifický požadavek na software nahrazuje jeden (či více) obecných požadavků na software, nebo zda se jeden (či více) obecných požadavků v konkrétním případě na software přístroje nevztahují a proč.

10.x.2 Technický popis

V tomto oddílu mohou být uvedeny následující informace:

- příklady nejčastějších specifických technických konfigurací,
- jak jsou na těchto příkladech použity požadavky P, U a rozšíření a
- užitečné kontrolní seznamy (dle přístroje) pro výrobce i zkoušejícího

Popis by měl zahrnovat:

- princip měření (kumulativní měření nebo jednotlivé, nezávislé měřicí úkoly; opakovatelné nebo neopakovatelné měření; statické nebo dynamické měření),
- popis detekce chyb a reakce na ně; jsou možné dvě situace:
  a) existence chyby je zřejmá, nebo ji lze snadno odhalit, nebo ji dokáží detekovat hardwarové prostředky,
  b) existence chyby není zřejmá a nelze ji snadno odhalit, nejsou dostupné hardwarové prostředky na její detekci.

  V druhém případě (b) se detekce chyb a reakce na ně neobejde bez odpovídajících softwarových prostředků, na něž se vztahují příslušné požadavky.
- konfiguraci hardwaru; měly by být zahrnuty alespoň následující body:
  a) jedná se o modulární systém založený na víceúčelovém počítači, nebo o jednoúčelový přístroj s integrovaným systémem podléhajícím legální kontrole?
  b) je počítačový systém samostatný, nebo je součástí uzavřené sítě (např. ethernet, LAN s technologií token ring), nebo otevřené sítě (např. internet)?
  c) je snímač přístroje oddělený (tj. je v samostatném krytu a má samostatné napájení) od systému typu U, nebo je do něho částečně či zcela integrovaný?
  d) podléhá uživatelské rozhraní vždy legální kontrole (platí pro typ přístrojů P i U), nebo může být přepnuto do jiného provozního režimu, jenž legální kontrole nepodléhá?
  e) předpokládá se dlouhodobé uložení dat? Pokud ano, bude využita lokální paměť (např. harddisk), nebo vzdálená paměť (např. server)?
  f) jedná se o pevnou paměť (např. vnitřní ROM), nebo výměnnou (např. disketa, CD-RW, paměťová karta smart-media, nebo flash disk)?
- konfiguraci softwaru a prostředí; měly by být zahrnuty alespoň následující body:
  a) jaký operační systém je použit nebo může být použit??
  b) jsou v systému kromě legálně relevantního softwaru i jiné softwarové aplikace?
  c) obsahuje systém nějaký software nepodléhající legální kontrole, který má být na základě schválení volně měněn?

10.x.3 Specifické požadavky na software

Tento oddíl by měl obsahovat seznam specifických požadavků na software a komentáře k nim. Formou by se měl podobat předchozím kapitolám.

10.x.4 Příklady legálně relevantních parametrů, funkcí a dat

V tomto oddílu mohou být uvedeny příklady

- specifických parametrů přístroje (např. jednotlivé konfigurační a kalibrační parametry konkrétního měřicího přístroje),
- specifických parametrů daného typu přístroje (např. specifické parametry, které jsou určeny při zkoušce typu), nebo
- legálně relevantní, specifické funkce.

10.x.5 Další vlastnosti

V tomto oddílu mohou být zmíněny další vlastnosti, např. konkrétní dokumentace požadovaná pro zkoušení daného typu (softwaru), specifické popisy a pokyny, které mají být dodány k certifikátům schválení typu (TEC), nebo další informace (např. požadavky týkající se testovatelnosti).

10.x.6 Přiřazení třídy rizika

V tomto oddílu by měla být definována příslušná třída rizika pro přístroje typu x. To lze provést dvěma způsoby:

- obecně (s platností pro všechny kategorie příslušného typu), nebo
- podle oblasti použití, kategorie, nebo jiných vlastností, pokud nějaké existují.

10.1 Vodoměry

10.1.1 Zvláštní předpisy, normy a jiné normativní dokumenty

V souladu s článkem 2 směrnice MID mohou členské státy nařídit, aby vodoměry používané v domácnostech, obchodech a lehkém průmyslu podléhaly směrnici MID. Specifické požadavky uvedené v této kapitole vycházejí pouze z přílohy MI-001.

Doporučení a normy organizace OIML nebyly zohledněny.

10.1.2 Technický popis

10.1.2.1 Konfigurace hardwaru

Vodoměry jsou obvykle jednoúčelové přístroje (v tomto dokumentu označované jako typ P).

10.1.2.2 Konfigurace softwaru

Konfigurace softwaru se liší podle výrobce, ale obvykle se předpokládá, že je v souladu s doporučeními uvedenými v hlavní části této příručky.

10.1.2.3 Princip měření

Vodoměry průběžně kumulativně měří objem spotřebované vody. Zobrazují celkový objem spotřebované vody. Při měření se využívají různé principy.

Měření objemu nelze opakovat.

10.1.2.4 Detekce a řešení chyb

Požadavek směrnice MI-001, 7.1.2 se zabývá elektromagnetickým rušením. Tento požadavek je nutné interpretovat v souvislosti s přístroji ovládanými softwarem, jelikož detekce rušení a náprava chyb se neobejdou bez součinnosti specifických částí hardwaru a softwaru. Z hlediska softwaru nezáleží na typu rušení (tj. zda se jedná o elektromagnetické, elektrické či mechanické rušení), jelikož postupy obnovy jsou vždy stejné.

10.1.3 Specifické požadavky na software (vodoměry)

Třída rizika B	Třída rizika C	Třída rizika D
I1-1: Obnova po chybě *Software se musí po chybě v důsledku rušení dokázat vrátit do běžného provozu.*		
Upřesnění: Úseky chybného provozu by měly být pro lepší evidenci označeny datovým razítkem.		
Požadovaná dokumentace: Stručný popis mechanismu obnovy po chybě a kdy je tento mechanismus spuštěn.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda realizace obnovy po chybě probíhá náležitým způsobem. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Cyklicky vykonávaný podprogram mikroprocesoru nuluje hlídací mechanismus hardwaru, a brání tak jeho spuštění. Pokud některá funkce nebyla vykonána nebo pokud dokonce dojde k uvíznutí mikroprocesoru v jakékoliv nekonečné smyčce, nedojde k vynulování hlídacího mechanismu a hlídací mechanismus se tedy po určité době spustí.		

Třída rizika B	Třída rizika C	Třída rizika D
I1-2: Prostředky zálohování *Musí existovat prostředky zajišťující pravidelnou zálohu naměřených dat, jako jsou naměřené hodnoty a současný stav procesu. Tato data musejí být uložena v energeticky nezávislé paměti.*		
Upřesnění: Intervaly uložení musí být dostatečně krátké, aby byl rozdíl mezi aktuálními a uloženými kumulativními hodnotami malý.		
Požadovaná dokumentace: Stručný popis toho, jaká data jsou zálohována a kdy se zálohování provádí. Výpočet maximální chyby, k níž může při zálohování kumulativních hodnot dojít.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda jsou naměřená data uložena v energeticky nezávislé paměti a zda je lze obnovit. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Naměřená data jsou zálohována dle potřeby (např. každých 60 minut).		

Třída rizika B	Třída rizika C	Třída rizika D
I1-3: MID Příloha I, 8.5 (zamezení vynulování naměřených kumulativních hodnot) *Údaje o celkovém spotřebovaném objemu nebo údaje, z nichž lze celkový spotřebovaný objem odvodit, které se částečně či plně využívají k výpočtu ceny k zaplacení, musí být u přístrojů na měření spotřeby chráněny proti vynulování během provozu.*		
Upřesnění: Kumulativní čítače měřicího přístroje lze vynulovat před uvedením do provozu.		
Požadovaná dokumentace: Dokumentace prostředků zabezpečení proti vynulování ukazatelů objemu.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda legálně relevantní hodnoty kumulativního měření nelze vynulovat, aniž by o to byl záznam. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Čítače objemu jsou chráněny proti změnám a vynulování stejnými prostředky jako parametry přístroje (viz P7).		

Třída rizika B	Třída rizika C	Třída rizika D
I1-4: Dynamické chování *Legálně nerelevantní software nesmí nežádoucím způsobem ovlivňovat dynamiku procesu měření.*		
Upřesnění: • Tento požadavek aplikujte jako doplnění požadavků S-1, S-2 a S-3 v případě, že bylo provedeno oddělení softwaru dle rozšíření S. • Tento doplňující požadavek má zajistit, že při použití měřicích přístrojů v reálném čase nedojde k nežádoucímu ovlivnění dynamického chování legálně relevantního softwaru legálně nerelevantním softwarem, tj. že zdroje legálně relevantního softwaru nebudou nežádoucím způsobem omezeny legálně nerelevantním softwarem.		
Požadovaná dokumentace: • Popis hierarchie přerušení. • Časové schéma úkolů softwaru. Limity a poměrné časy pro legálně nerelevantní úkoly.		
Postup validace: *Ověření na základě dokumentace:* • Programátor legálně nerelevantní části softwaru má k dispozici dokumentaci s limity poměrných časů pro legálně nerelevantní úkoly. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Návrh hierarchie přerušení musí zamezit nežádoucím vlivům.		

Třída rizika B	Třída rizika C	Třída rizika D
I1-5: Vytištěné označení softwaru *Označení softwaru je obvykle zobrazeno na displeji. U vodoměrů může být označení softwaru uvedeno rovněž na tištěném štítku s názvem přístroje. Takové řešení je přijatelné, pokud jsou splněny následující podmínky A, B a C:* *A. Uživatelské rozhraní nenabízí nástroj k aktivaci zobrazení označení softwaru na displeji, nebo displej přístroje technicky neumožňuje zobrazit označení softwaru (mechanický čítač).* *B. Přístroj nemá žádné rozhraní, kterým by označení softwaru mohl sdělit.* *C. Na vyrobeném přístroji již není možné software měnit, nebo je změna softwaru možná pouze v kombinaci s výměnou hardwaru nebo jeho části.*		
Upřesnění: • Výrobce hardwaru nebo příslušné hardwarové části zodpovídá za to, že je označení softwaru správně uvedeno na příslušném hardwaru. • Dále platí všechna další upřesnění požadavků P2/U2.		
Požadovaná dokumentace: • Viz P2/U2.		
Postup validace: *Ověření na základě dokumentace:* • Viz P2/U2. *Ověření funkčnosti:* • Viz P2/U2.		
Příklad přijatelného řešení: Vytištěné označení softwaru na štítku přístroje.		

10.1.4 Příklady legálně relevantních parametrů, funkcí a dat

Parametry vodoměrů zahrnují např. konstanty pro přepočty, konfiguraci, atd., ale také parametry pro nastavení funkcí přístroje. Označení a zabezpečení parametrů a skupin parametrů je popsáno v požadavcích P2 a P7 u přístrojů typu P.

V následující tabulce jsou uvedeny některé z typických parametrů vodoměrů. (Tabulka bude doplněna, jakmile pracovní skupina WELMEC WG 11 rozhodne o její finální podobě.)

Parametr	Chráněný	Nastavitelný	Poznámka
Kalibrační faktor	x		
Linearizační faktor	x		

10.1.5 Další vlastnosti

Neočekává se, že stahování softwaru bude mít při použití přístrojů v domácnostech (rozšíření D, kapitola 9) velký význam.

Kumulativní čítač energie nebo objemu, jímž jsou vybaveny domácí přístroje, není považován za zařízení k dlouhodobému uložení dat ve smyslu rozšíření L (kapitol 6). U přístroje, který měří pouze kumulovanou energii/objem, proto není použití rozšíření L nutné.

10.1.6 Přiřazení třídy rizika

V současnou chvíli je dle rozhodnutí příslušné pracovní skupiny WELMEC WG 11 považována za odpovídající následující třída rizika. Měla by být použita při zkouškách softwaru vodoměrů (řízených softwarem) dle této příručky:

- **Třída rizika C pro přístroje typu P**

Konečné rozhodnutí nicméně dosud nebylo přijato a pracovní skupina WG 11 tuto záležitost znovu zváží v souvislosti s rozhodováním o odpovídající třídě či třídách rizika pro přístroje typu U.

10.2 Plynoměry a přepočítávače množství plynu

10.2.1 Zvláštní předpisy, normy a jiné normativní dokumenty

Specifické požadavky této kapitoly jsou založeny na příloze IV směrnice MID, Plynoměry a přepočítávače množství plynu (MI-002).

Pokud jde o zabezpečení plynoměrů a přepočítávačů množství plynu, lze se řídit i příručkou WELMEC 11.3.

Zvláštní návod ve vztahu k plynovému chromatografu připojenému jako živé čidlo EVCD lze najít v příručce WELMEC 11.1.

Další pokyny nebo aktualizace týkající se konkrétních pokynů pro plynoměry a přepočítávače množství plynu lze najít na webu WELMEC.

Národní právní předpisy týkající se doplňkových funkcí, doporučení OIML, (EN) harmonizované normy a (IEC) normy nebyly brány v úvahu.

10.2.2 Technický popis

10.2.2.1 Konfigurace hardwaru

Plynoměry a přepočítávací zařízení jsou obvykle samostatné hardwarové jednotky. Indikátory nebo kalkulátory plynoměrů a přepočítávačů množství plynu mohou mít jedno nebo více rozhraní pro připojení externích senzorů.

V případě, že je plynový chromatograf připojen jako živé čidlo k EVCD, GC ovlivňuje výsledek měření EVCD (základní objem), a proto by mělo být součástí procesu posuzování shody.

10.2.2.2 Konfigurace softwaru

Konfigurace softwaru se liší podle výrobce, ale obvykle se předpokládá, že je v souladu s doporučeními uvedenými v hlavní části této příručky.

10.2.2.3 Princip měření

Plynoměry průběžně kumulativně měří objem či hmotnost proteklé měřidlem. Přepočítávače množství plynu mohou být použity k přepočtu objemu na základní podmínky.

Měření objemu je neopakovatelné.

10.2.2.4 Detekce a řešení chyb

Požadavek směrnice MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002), článek 3.1 se zabývá přípustným rušením. Z hlediska softwaru nezáleží na typu rušení (tj. zda se jedná o elektromagnetické, elektrické či mechanické rušení atd.): postupy obnovy jsou vždy stejné.

- Po prodělaném rušení musí být plynoměr opět:
  - navrácen do provozu v mezích MPE a
  - mít zabezpečeny všechny měřicí funkce a
  - musí umožnit obnovu všech hodnot naměřených bezprostředně před rušením.

  Viz článek 3.1.2 směrnice MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002).

- Elektronické přepočítávací zařízení musí být schopno detekovat, že pracuje mimo provozní rozsah(y) uvedený výrobcem pro parametry, které jsou relevantní pro přesnost měření. V takovém případě přepočítávací zařízení musí zastavit načítání přepočítaného množství a může sčítat separátně přepočítané množství za dobu, kdy zařízení pracuje mimo provozní rozsah(y).
  Viz článek 9.1 směrnice MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002).

10.2.3 Specifické požadavky na software

10.2.3.1 Plynoměry a přepočítávače objemu

Třída rizika B	Třída rizika C	Třída rizika D
I2-1: Směrnice MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002), článek 3.1, obnova po chybě *Software se musí po chybě v důsledku rušení dokázat vrátit do běžného provozu.*		
Upřesnění: Úseky chybného provozu by měly být pro lepší evidenci označeny datovým razítkem.		
Požadovaná dokumentace: Stručný popis mechanismu obnovy po chybě a vysvětlení jak a kdy je tento mechanismus spuštěn.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda realizace obnovy po chybě probíhá náležitým způsobem. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Hlídací mechanismus hardwaru je vynulován cyklicky vykonávaným podprogramem mikroprocesoru, aby zablokoval spuštění hlídacího mechanismu.		

Třída rizika B	Třída rizika C	Třída rizika D
I2-2: Legálně nerelevantní software a dynamické chování *Legálně nerelevantní software nesmí nežádoucím způsobem ovlivňovat dynamiku procesu měření.*		
Upřesnění: Tento doplňující požadavek má zajistit, že při použití měřicích přístrojů v reálném čase nedojde k nežádoucímu ovlivnění dynamického chování legálně relevantního softwaru legálně nerelevantním softwarem, tj. že zdroje legálně relevantního softwaru nebudou nežádoucím způsobem omezeny legálně nerelevantním softwarem.		
Požadovaná dokumentace: • Popis hierarchie přerušení. • Časové schéma úkolů softwaru. Limity a poměrné časy pro legálně nerelevantní úkoly.		
Postup validace: *Ověření na základě dokumentace:* • Programátor legálně nerelevantní části softwaru má k dispozici dokumentaci s limity poměrných časů pro legálně nerelevantní úkoly. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Návrh hierarchie přerušení musí zamezit nežádoucím vlivům.		

Třída rizika B	Třída rizika C	Třída rizika D
I2-3: Směrnice MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002), článek 3.1.2, Prostředky zálohování *Mohou existovat prostředky zajišťující pravidelnou zálohu naměřených dat, jako jsou naměřené hodnoty a současný stav procesu. Tato data musí být uložena v energeticky nezávislé paměti.*		
Upřesnění: Pokud jsou pro zajištění obnovy po chybě použity prostředky zálohování, musí být vypočten takový minimální interval ukládání dat, který zajistí, že nebude překročena kritická hodnota.		
Požadovaná dokumentace: Stručný popis toho, jaká data jsou zálohována a kdy se zálohování provádí. Výpočet takového minimálního intervalu pro ukládání dat, že není překročena kritická hodnota změny.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda jsou naměřená data uložena v energeticky nezávislé paměti a zda je lze obnovit. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Naměřená data jsou zálohována dle potřeby.		

Třída rizika B	Třída rizika C	Třída rizika D
I2-4: Doplňkové funkce[2] *Doplňkové funkce, např. předplatné nebo intervalové měření[3], by neměly ovlivnit legálně relevantní měřicí funkce specifikované v MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002).*		
Upřesnění: • Doplňkové funkce jsou povoleny za předpokladu, že neovlivňují legálně relevantní měřicí funkce specifikované v MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002).		
Požadovaná dokumentace: Viz S1 až S3.		
Postup validace: Viz S1 až S3.		
Příklad přijatelného řešení: Viz S1 až S3.		

Třída rizika B	Třída rizika C	Třída rizika D
I2-5: Stahování softwaru *Během instalace softwaru nesmí být měřicí proces celkově pozastaven na déle než na 1 minutu. V případě, že proces instalace zabírá více než 1 minutu, musí být přijata další opatření (např. instalace probíhá v režimu minimálního odběru).*		
Upřesnění: • Pokud je realizováno stahování softwaru kromě požadavků D1, D2, D3 a D4 aplikujte i tento požadavek. • Tento dodatečný požadavek přináší ujištění, že aplikace běžící v reálném čase nejsou přerušeny moc dlouho.		
Požadovaná dokumentace: Viz D1.		
Postup validace: Viz D1.		
Příklad přijatelného řešení: Viz D1.		

[2] Vždy by měl vzít výrobce v úvahu národní požadavky týkající se doplňkových funkcí.
[3] Další doporučení k intervalovému měření poskytuje WELMEC Guide 11.2.

Třída rizika B	Třída rizika C	Třída rizika D
I2-6: MID Příloha I, 8.5 (Zamezení vynulování naměřených kumulativních hodnot) *Údaje o celkovém spotřebovaném objemu nebo údaje, z nichž lze celkový spotřebovaný objem odvodit, které se částečně či plně využívají k výpočtu ceny k zaplacení, musí být u přístrojů na měření spotřeby chráněny proti vynulování během provozu.*		
Upřesnění: Během procesu schvalování typu dle příloh D, F či H1 musí být měřidla spotřeby zabezpečena všemi zajištěními, jak je specifikováno výrobcem a je specifikováno v TEC. Tato zajištění musí být takového rázu, že není možno vynulovat naměřené kumulativní hodnoty bez evidence tohoto zásahu. U plynoměrů musí být registr celkového naměřeného objemu chráněn hardwarovou metrologickou plombou. U přepočítávačů množství plynu musí být objem při základních podmínkách chráněn hardwarovou metrologickou plombou.		
Požadovaná dokumentace: Dokumentace prostředků zabezpečení proti vynulování ukazatelů objemu.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda je operace vynulování kumulativních legálně relevantních naměřených hodnot zajištěna a že očekávaná zabezpečení poskytují záznam o intervenci. *Ověření funkčnosti:* • Ověřte správnou funkci aplikovaných zabezpečení.		
Příklad přijatelného řešení: U plynoměrů musí být registr pro celkový naměřený objem chráněn hardwarovou metrologickou plombou. Ostatní registry, např. pro denní či noční tarif, mohou být chráněny stejnými prostředky jako parametry (viz P7/U7), přičemž musí být dostupný celkový (úhrnný kumulativní) registr chráněný hardwarovou plombou. Pro další informace viz WELMEC guide 11.1 a 11.3. U přepočítávačů musí být hardwarovou metrologickou plombou chráněn objem při základních podmínkách. Registr indikující objem při podmínkách měření může být též chráněn stejnými prostředky jako parametry (viz P7/U7). Poznámka: Objem při podmínkách měření může být synchronizován s indikací připojeného plynoměru. Národní legislativa může vyžadovat další opatření, např. reverifikace.		

Třída rizika B	Třída rizika C	Třída rizika D

I2-7: MID-Příloha I, článek 10.5 (Čtení naměřených hodnot)

A. Naměřené hodnoty, které slouží jako základ pro stanovení ceny, mohou pocházet z různých registrů, které jsou aktivovány dálkově, dle času či jinými způsoby. Každý registr reprezentuje celkové množství odpovídající jedné fakturovací sazbě. Je třeba, aby měřidlo zobrazovalo hodnoty každého registru periodicky či na požádání přes uživatelské rozhraní.

Upřesnění:

Kumulativní registry měřidla mohou být vynulovány před provedením posouzení shody. Během procesu posouzení shody dle příloh D, F či H1 musí být měřidla spotřeby vybavena všemi zajištěními, jak je specifikováno výrobcem a je specifikováno v TEC. Tato zajištění musí být takového rázu, že není možno vynulovat naměřené kumulativní hodnoty bez evidence tohoto zásahu.

Požadovaná dokumentace:

Dokumentace popisující jak je možno získat naměřené hodnoty, které slouží jako základ pro stanovení ceny.

Postup validace:

Ověření na základě dokumentace:

- Ověřte správné zacházení s naměřenými hodnotami.

Ověření funkčnosti:

- Potvrďte správnou funkci zacházení s naměřenými hodnotami.

Příklad přijatelného řešení:

Pokud je měřidlo navrženo tak, že počítá množství definovaná v MID, Příloze IV Plynoměry a přepočítávače množství plynu (MI-002) v různých registrech, musí být možné zobrazit celkové množství každého registru na displeji pomocí uživatelského rozhraní (viz tento dokument, např. tlačítek měřidla) a stejně tak i zobrazit právě aktuální registr.

Akceptovatelné je též zobrazení výsledků rozdílných registrů na několika displejích, periodicky či na požádání přes uživatelské rozhraní. Avšak při zobrazení těchto hodnot musí být jasné, který registr se jak zobrazuje (na kterém displeji), v tomto ohlednu nesmí dojít k nejednoznačnosti.

Třída rizika B	Třída rizika C	Třída rizika D

I2-8: Ochrana proti záměrným změnám u plynoměrů typu P s mechanickým čítačem

Vypočítanou hodnotu kontrolního součtu či alternativní indikace sloužící k detekci modifikace softwaru musí být možné pro kontrolní účely na příkaz zobrazit, viz P6, třída rizika C.

Jako vyjímka pro plynoměry a přepočítavače množství plynu typu P s mechanickým čítačem je akceptovatelné, aby hodnota kontrolního součtu či alternativní indikace byla uvedena na štítku měřidla, a to pokud jsou splněny následující podmínky A, B a C:

A. Uživatelské rozhraní nenabízí prostředek k aktivaci zobrazení hodnoty kontrolního součtu či alternativní indikace modifikace softwaru na displeji nebo displej přístroje technicky neumožňuje zobrazit označení softwaru (mechanický čítač).

B. Přístroj nemá žádné rozhraní, kterým by identifikaci softwaru mohl sdělit.

C. Na vyrobeném přístroji již není možné software měnit nebo je změna softwaru možná pouze v kombinaci s výměnou hardwaru nebo jeho části.

Upřesnění:

- Výrobce zodpovídá za to, že hodnota kontrolního součtu či alternativní indikace modifikace softwaru je na příslušném hardwaru správně uvedena.
- Dále aplikujte všechna další upřesnění požadavků P6.

Požadovaná dokumentace:
Viz P6.

Postup validace:

Ověření na základě dokumentace:

- Viz P6.

Ověření funkčnosti:

- Viz P6.

Příklad přijatelného řešení:
Hodnota kontrolního součtu či alternativní indikace sloužící k detekci modifikace softwaru vytištěná na štítku přístroje.

Třída rizika B	Třída rizika C	Třída rizika D

I2-9: MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002), článek 5.3 počet míst (Plynoměry a přepočítávače množství plynu)

Čítač zobrazující celkové množství musí být tvořen takovou dostatečně dlouhou řadou číslic, aby se nemohl vrátit na původní hodnotu dříve než po 8000 hodinách provozu přístroje při maximálním průtoku Q_{max}.

Upřesnění:

Požadovaná dokumentace:
Dokumentace vnitřní reprezentace čítače.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, že je řada číslic dostatečná – že po uplnynutí 8000 hodin provozu při průtoku Q_{max} se čítač nevrátí na svou počáteční hodnotu.

Příklad přijatelného řešení:
Typické hodnoty plynoměrů používaných v domácnostech jsou: Q_{max} = 6 m³/h. Požadovaný rozsah je tedy 48 000 m³, tedy zobrazení 5 číslic (současné mechanické i elektronické plynoměry jsou schopny zobrazit až 99 999 m³, což je pro tento typ měřidla více než adekvátní).

Třída rizika B	Třída rizika C	Třída rizika D
I2-10: MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002), článek 5.2 Životnost zdroje napájení *Zdroj napájení vyhrazený pro konkrétní měřicí přístroj musí mít životnost alespoň pět let. Poté, co tato doba životnosti z 90 % uplyne, se musí na přístroji zobrazit varovné hlášení.*		
Upřesnění: Termín „životnost“ se zde používá k označení dostupné kapacity zdroje napájení. Pokud je možné zdroj energie na místě vyměnit, nesmí při výměně zdroje energie dojít k poškození parametrů přístroje a naměřených dat. Je možné zobrazit varovné hlášení i před uplynutím 90% kapacity za předpokladu, že toto hlášení není zavádějící.		
Požadovaná dokumentace: Dokumentace popisující kapacitu zdroje napájení, maximální životnost (nezávisle na spotřebě), způsob zjištění spotřebované čizbývající kapacity, popis způsobu podávání varovného hlášení o nízké zbývající kapacitě zdroje a popis výměny baterie.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda jsou prostředky sledování dostupné energie zdroje dostatečné.		
Příklad přijatelného řešení: Počítá se doba provozu přístroje nebo počet událostí probouzejících přístroj ze spánku. Tyto údaje jsou uloženy do energeticky nezávislé paměti a porovnány s nominální hodnotou životnosti baterie. Po uplynutí 90 % doby životnosti se zobrazí příslušné varovné hlášení. Software detekuje výměnu zdroje napájení a vynuluje čítač. Jiným řešením může být nepřetržité sledování stavu zdroje napájení. Varovné hlášení je považováno za přiměřené pokud je zobrazeno jako vzkaz na displeji přístroje nebo je zobrazena indikace chyby. Dále elektronické rozhraní může poslat hlášení operátorovi sítě/měřidla. Pouze odeslání skrytého hlášení (přes elektronické rozhraní) operátorovi sítě/měřidla není dostatečné.		

10.2.3.2 Plynoměry

Třída rizika B	Třída rizika C	Třída rizika D
I2-11: MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002), článek 5.5 Testovací prvek plynoměru *Plynoměr musí být vybaven testovacím prvkem umožňujícím provádění testů v přiměřeném čase.*		
Upřesnění: Testovací prvek urychlující časově náročné procesy testování se obvykle používá k testování před instalací a běžným provozem. V testovacím režimu se musí používat stejné čítače a stejné části softwaru, které budou použity v běžném režimu provozu.		
Požadovaná dokumentace: Dokumentace testovacího prvku a návod na spuštění testovacího režimu.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda lze všechny časově náročné procesy testování plynoměru provést prostřednictvím testovacího prvku.		
Příklad přijatelného řešení: Pro testovací účely musí přírůstek testovacího prvku či pulzu nastat nejméně každých 60 sekund při Q_{min}, viz WELMEC Příručka 11.1, odstavec 2.4.4. Časovou základnu vnitřních hodin lze zrychlit. Procesy, které trvají např. týden, měsíc nebo dokonce rok a způsobují přetečení čítačů, lze otestovat v testovacím režimu za pouhé minuty až hodiny.		

10.2.3.3 Elektronický přepočítávač

Třída rizika B	Třída rizika C	Třída rizika D
I2-12: MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002), článek 9.1 Elektronický přepočítávač *U parametrů relevantních z hlediska přesnosti měření musí být elektronický přepočítávač schopen rozpoznat, kdy je přístroj mimo rozsah měření definovaný výrobcem. V takovém případě přepočítávač nesmí přepočítanou hodnotu integrovat, ale může vypočítat přepočítanou hodnotu odděleně za dobu, kdy přístroj pracoval mimo definovaný rozsah provozu.*		
Upřesnění: Na displeji se musí zobrazit hlášení o chybě.		
Požadovaná dokumentace: Dokumentace různých čítačů přepočítaného množství a chybného množství.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda jsou prostředky zvládání neobvyklých podmínek provozu dostatečné.		
Příklad přijatelného řešení: Software sleduje relevantní vstupní hodnoty a porovnává je s předem definovanými limity. Pokud všechny hodnoty vyhovují stanoveným limitům, potom je přepočítané množství integrováno do běžného čítače (dedikovaná proměnná). V opačném případě se množství sečte do jiné proměnné. Dalším možným řešením by mohlo být použít pouze jeden kumulativní čítač a zaznamenávat do zapisovače událostí datum začátku a konce, čas a hodnoty naměřené při provozu, jehož rozsah nevyhovoval definovaným limitům (viz P7). Mohou být uvedeny oba údaje o množství. Uživatel dokáže jasně poznat a odlišit běžný režim od chybového podle informací o stavu.		

Třída rizika B	Třída rizika C	Třída rizika D
I2-13: Přepočet konverzního faktoru (tzv. přepočítávacího čísla) *V elektronických přepočítávačích množství plynu musí být přepočítávací číslo přepočítáváno v intervalu, který nepřekračuje 1 min u teplotního přepočítávače, a v intervalu nepřekračujícím 30 s u ostatních typů přepočítávačů.* *Avšak pokud z plynoměru nepřijde žádný signál objemu* *- po dobu delší než 1 min pro teplotní přepočítávače; nebo* *- po dobu delší než 30 s pro ostatní typy;* *přepočet není až do dalšího obdržení signálu vyžadován.*		
Upřesnění:		
Požadovaná dokumentace: Dokumentace sekvence přepočtu.		
Postup validace: *Ověření na základě dokumentace:* Ověřte, zda jsou přijatá opatření přiměřená.		
Příklad přijatelného řešení:		

10.2.4 Příklady legálně relevantních parametrů, funkcí a dat

Přístup k prostředkům pro modifikaci legálně relevantního softwaru, nastavení a/nebo parametrům majícími vliv na výsledky měření musí být zabezpečen[4].

U plynoměrů například ale nejenom:

Parametr	Chráněný	Nastavitelný	Poznámka
Kalibrační faktor	X		
Linearizační faktor	X		
Legálně relevantní konfigurace registrů	X		
Nastavení např.: • korekce • interpolace křivky • pulzního číslo • hranice minimálního průtoku • ultrasonických senzorů • převodník geometrie ultrasonických plynoměrů	X		
Další relevantní parametry, které ovlivňují či by mohly ovlivnit výsledek měření	X		
Stahování legálně relevantního softwaru	X		

U přepočítávačů například ale nejenom:

Parametr	Chráněný	Nastavitelný	Poznámka
Kalibrační faktor	X		
Linearizační faktor	X		
Legálně relevantní konfigurace registrů	X		
Nastavení např.: • legálně relevantní parametry korekčního zařízení, jako jsou parametry vycházející z chybové křivky plynoměru • pulzního číslo plynoměru • složení plynu a parametry podílející se na výpočtu kompresibility	X		
Další relevantní parametry, které ovlivňují či by mohly ovlivnit výsledek měření	X		
Stahování legálně relevantního softwaru	X		

[4] Vždy by měl vzít výrobce v úvahu národní požadavky týkající se doplňkových funkcí.
Další doporučení k intervalovému měření poskytuje WELMEC Guide 11.2.

10.2.5 Přiřazení třídy rizika

Následující třída rizika je považována za odpovídající a měla by být použita při zkouškách softwaru plynoměrů a přepočítávačů množství plynu (řízených softwarem) dle této příručky:

- **Třída rizika C pro přístroje typu P a U**

10.3 Elektroměry k měření činné energie

10.3.1 Zvláštní předpisy, normy a jiné normativní dokumenty

Specifické požadavky této kapitoly jsou založeny na příloze V směrnice MID, Elektroměry k měření činné energie (MI-003).

Pokud jde o zabezpečení elektroměrů k měření činné energie, lze se řídit i příručkou WELMEC 11.3.

Další pokyny nebo aktualizace týkající se konkrétních pokynů pro elektroměry k měření činné energie lze najít na webu WELMEC.

Národní právní předpisy týkající se doplňkových funkcí, doporučení OIML, (EN) harmonizované normy a (IEC) normy nebyly brány v úvahu.

10.3.2 Technický popis

10.3.2.1 Konfigurace hardwaru

Do elektroměrů činné energie vstupuje napětí a proud, na jejichž základě přístroj stanoví celkový výkon v čase, a stanoví tak celkové množství spotřebované elektrické energie.
Elektroměry k měření činné energie mohou být používány v kombinaci s externími transformátory.

10.3.2.2 Konfigurace softwaru

Konfigurace softwaru se liší podle typu měřidla, ale předpokládá se, že je v souladu s doporučeními uvedenými v hlavní části této příručky.

10.3.2.3 Princip měření

Elektroměry k měření činné energie průběžně kumulativně měří objem spotřebované energie. Přístroj zobrazuje celkové množství spotřebované energie.
Měření je neopakovatelné.

10.3.2.4 Detekce a řešení chyb

Požadavek směrnice MID, Příloha V Elektroměry k měření činné energie (MI-003), článek 4.3.1 se zabývá přípustným rušením. Z hlediska softwaru nezáleží na typu rušení (tj. zda se jedná o elektromagnetické, elektrické či mechanické rušení atd.), jelikož postupy obnovy jsou vždy stejné.

- Po prodělaném rušení musí být plynoměr opět:
  - navrácen do provozu v mezích MPE a
  - mít zabezpečeny všechny měřicí funkce a
  - musí umožnit obnovu všech hodnot naměřených bezprostředně před rušením a
  - nesmí indikovat změnu zaznamenané energie větší než je hodnota kritické změny.

10.3.3 Specifické požadavky na software

Třída rizika B	Třída rizika C	Třída rizika D
I3-1: Obnova po chybě *Software se musí po chybě v důsledku rušení dokázat vrátit do běžného provozu.*		
Upřesnění: Úseky chybného provozu by měly být pro lepší evidenci označeny datovým razítkem.		
Požadovaná dokumentace: Stručný popis mechanismu obnovy po chybě a vysvětlení jak a kdy je tento mechanismus spuštěn. Krátký popis souvisejících testů provedených výrobcem.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda realizace obnovy po chybě probíhá náležitým způsobem. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Cyklicky vykonávaný podprogram mikroprocesoru nuluje hlídací mechanismus hardwaru, a brání tak jeho spuštění. Pokud některá funkce nebyla vykonána nebo pokud dokonce dojde k uvíznutí mikroprocesoru v jakékoliv nekonečné smyčce, nedojde k vynulování hlídacího mechanismu a hlídací mechanismus se tedy po určité době spustí.		

Třída rizika B	Třída rizika C	Třída rizika D
I3-2: Legálně nerelevantní software a dynamické chování *Legálně nerelevantní software nesmí nežádoucím způsobem ovlivňovat dynamiku procesu měření.*		
Upřesnění: Tento doplňující požadavek má zajistit, že při použití měřicích přístrojů v reálném čase nedojde k nežádoucímu ovlivnění dynamického chování legálně relevantního softwaru legálně nerelevantním softwarem, tj. že zdroje legálně relevantního softwaru nebudou nežádoucím způsobem omezeny legálně nerelevantním softwarem.		
Požadovaná dokumentace: • Popis hierarchie přerušení. • Časové schéma úkolů softwaru. Limity a poměrné časy pro legálně nerelevantní úkoly.		
Postup validace: *Ověření na základě dokumentace:* • Programátor legálně nerelevantní části softwaru má k dispozici dokumentaci s limity poměrných časů pro legálně nerelevantní úkoly. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Návrh hierarchie přerušení musí zamezit nežádoucím vlivům.		

Třída rizika B	Třída rizika C	Třída rizika D
I3-3: Doplňkové funkce[5] *Doplňkové funkce, např. předplatné nebo intervalové měření[6], by neměly ovlivnit legálně relevantní měřicí funkce specifikované v MID, Příloha V* Elektroměry k měření činné energie *(MI-003).*		
Upřesnění: • Doplňkové funkce jsou povoleny za předpokladu, že neovlivňují legálně relevantní měřicí funkce specifikované v MID, Příloha V Elektroměry k měření činné energie (MI-003).		
Požadovaná dokumentace: Viz S1 až S3.		
Postup validace: Viz S1 až S3.		
Příklad přijatelného řešení: Viz S1 až S3.		

[5] Vždy by měl vzít výrobce v úvahu národní požadavky týkající se doplňkových funkcí.
[6] Další doporučení k intervalovému měření poskytuje WELMEC Guide 11.2.

Třída rizika B	Třída rizika C	Třída rizika D
I3-4: Směrnice MID, Příloha V Elektroměry k měření činné energie (MI-003), článek 4.3.1, Prostředky zálohování *Mohou existovat prostředky zajišťující pravidelnou zálohu naměřených dat, jako jsou naměřené hodnoty a současný stav procesu. Tato data musí být uložena v energeticky nezávislé paměti.*		
Upřesnění: Pokud jsou pro zajištění obnovy po chybě použity prostředky zálohování, musí být vypočten takový minimální interval ukládání dat, který zajistí, že nebude překročena kritická hodnota.		
Požadovaná dokumentace: Stručný popis toho, jaká data jsou zálohována a kdy se zálohování provádí. Výpočet takového minimálního intervalu pro ukládání dat, že není překročena kritická hodnota změny.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda jsou naměřená data uložena v energeticky nezávislé paměti a zda je lze obnovit. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Naměřená data jsou zálohována dle potřeby.		

Třída rizika B	Třída rizika C	Třída rizika D
I3-5: Stahování softwaru *Během instalace softwaru nesmí být měřicí proces celkově znemožněn déle než na 1 minutu.* *V případě, že proces instalace zabírá více než 1 minutu, musí být přijata další opatření (např. instalace probíhá v režimu nízké spotřeby energie).*		
Upřesnění: • Pokud je realizováno stahování softwaru kromě požadavků D1, D2, D3 a D4 aplikujte i tento požadavek. • Tento dodatečný požadavek přináší ujištění, že aplikace běžící v reálném čase nejsou přerušeny moc dlouho.		
Požadovaná dokumentace: Viz D1.		
Postup validace: Viz D1.		
Příklad přijatelného řešení: Viz D1.		

Třída rizika B	Třída rizika C	Třída rizika D
I3-6: MID Příloha I, 8.5 (Zamezení vynulování naměřených kumulativních hodnot) *Údaje o celkovém spotřebovaném objemu nebo údaje, z nichž lze celkový spotřebovaný objem odvodit, které se částečně či plně využívají k výpočtu ceny k zaplacení, musí být u přístrojů na měření spotřeby chráněny proti vynulování během provozu.*		
Upřesnění: Kumulativní registry měřicího přístroje lze vynulovat před provedením procedury posouzení shody. Během procesu schvalování typu dle příloh D, F či H1 musí být měřidla spotřeby zabezpečena všemi zajištěními, jak je specifikováno výrobcem a je specifikováno v TEC. Tato zajištění musí být takového rázu, že není možno vynulovat naměřené kumulativní hodnoty bez evidence tohoto zásahu.		
Požadovaná dokumentace: Dokumentace prostředků zabezpečení proti vynulování ukazatelů objemu.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda je operace vynulování kumulativních legálně relevantních naměřených hodnot zajištěna a že očekávaná zabezpečení poskytují záznam o intervenci. *Ověření funkčnosti:* • Ověřte správnou funkci aplikovaných zabezpečení, viz také P3/U3 a P4/U4.		
Příklad přijatelného řešení: Registr pro celkové naměřené množství musí být chráněn hardwarovou plombou. Ostatní registry, např. pro denní či noční tarif, mohou být chráněny stejnými prostředky jako parametry (viz P7/U7), přičemž musí být dostupný celkový (úhrnný kumulativní) registr chráněný hardwarovou plombou. Pro další informace viz WELMEC guide 11.1.		

Třída rizika B	Třída rizika C	Třída rizika D

I3-7: MID-Příloha I, článek 10.5 (Čtení naměřených hodnot)

Naměřené hodnoty, které slouží jako základ pro stanovení ceny, mohou pocházet z různých registrů, které jsou aktivovány dálkově, dle času či jinými způsoby. Každý registr reprezentuje celkové množství odpovídající jedné fakturovací sazbě. Musí být možné zobrazit hodnoty na displeji periodicky či na požádání přes uživatelské rozhraní.

Upřesnění:

Kumulativní registry měřidla mohou být vynulovány před provedením posouzení shody. Během procesu posouzení shody dle příloh D, F či H1 musí být měřidla spotřeby vybavena všemi zajištěními, jak je specifikováno výrobcem a je specifikováno v TEC. Tato zajištění musí být takového rázu, že není možno vynulovat naměřené kumulativní hodnoty bez evidence tohoto zásahu.

Požadovaná dokumentace:

Dokumentace popisující jak je možno získat naměřené hodnoty, které slouží jako základ pro stanovení ceny.

Postup validace:

Ověření na základě dokumentace:

- Ověřte správné zacházení s naměřenými hodnotami.

Ověření funkčnosti:

- Potvrďte správnou funkci zacházení s naměřenými hodnotami.

Příklad přijatelného řešení:

Pokud je měřidlo navrženo tak, že načítá množství definovaná v MID, Příloze V Elektroměry k měření činné energie (MI-003) v různých registrech, musí být možné zobrazit celkové množství každého registru na displeji pomocí uživatelského rozhraní (viz tento dokument, např. tlačítek měřidla) a stejně tak i zobrazit právě aktuální registr.

Je též možné zobrazit výsledky na několika displejích, periodicky či na požádání přes uživatelské rozhraní. Avšak při zobrazení těchto hodnot musí být jasné, který registr se jak zobrazuje (na kterém displeji), v tomto ohlednu nesmí dojít k nejednoznačnosti.

Třída rizika B	Třída rizika C	Třída rizika D

I3-8: Ochrana proti záměrným změnám u elektroměrů k měření činné energie typu P s mechanickým čítačem

Vypočítanou hodnotu kontrolního součtu či alternativní indikace sloužící k detekci modifikace softwaru musí být možné pro kontrolní účely na příkaz zobrazit, viz P6. Jako vyjímka pro elektroměry k měření činné energie typu P s mechanickým čítačem je akceptovatelné, aby hodnota kontrolního součtu či alternativní indikace byla uvedena na štítku měřidla, a to pokud jsou splněny následující podmínky A, B a C:

A. Uživatelské rozhraní nenabízí prostředek k aktivaci zobrazení hodnoty kontrolního součtu či alternativní indikace modifikace softwaru na displeji nebo displej přístroje technicky neumožňuje tyto hodnoty zobrazit (mechanický čítač).

B. Přístroj nemá žádné rozhraní, kterým by identifikaci softwaru mohl sdělit.

C. Na vyrobeném přístroji již není možné software měnit nebo je změna softwaru možná pouze v kombinaci s výměnou hardwaru nebo jeho části.

Upřesnění:

- Výrobce zodpovídá za to, že hodnota kontrolního součtu či alternativní indikace modifikace softwaru je na příslušném hardwaru správně uvedena.
- Dále aplikujte všechna další upřesnění požadavků P6.

Požadovaná dokumentace:
Viz P6.

Postup validace:

Ověření na základě dokumentace:

- Viz P6.

Ověření funkčnosti:

- Viz P6.

Příklad přijatelného řešení:
Hodnota kontrolního součtu či alternativní indikace sloužící k detekci modifikace softwaru vytištěná na štítku přístroje.

Třída rizika B	Třída rizika C	Třída rizika D
I3-9: MID, Příloha V Elektroměry k měření činné energie (MI-003), článek 5.2 počet míst *Čítač zobrazující celkové množství energie musí být tvořen takovou dostatečně dlouhou řadou číslic, aby se nemohl vrátit na původní hodnotu dříve než po 4000 hodinách provozu elektroměru při maximální kapacitě ($I = I_{max}$, $U = U_n$ and $PF = 1$).*		
Upřesnění:		
Požadovaná dokumentace: Dokumentace vnitřní reprezentace čítače elektrické energie a pomocných veličin.		
Postup validace: *Ověření na základě dokumentace:* Ověřte, zda je řada číslic dostatečně dlouhá (vnitřní a na displeji).		
Příklad přijatelného řešení: Typické hodnoty třífázových elektroměrů jsou: P_{max} (4000h) = 3*60 A * 230 V * 4000h / 1000 = 165600 kWh. To vyžaduje zobrazení přinejmenším 6 číslic.		

10.3.4 Příklady legálně relevantních parametrů, funkcí a dat

Přístup k prostředkům pro modifikaci legálně relevantního softwaru, nastavení a/nebo parametrům majícími vliv na výsledky měření musí být zabezpečen[7].

Parametr	Chráněný	Nastavitelný	Poznámka
Kalibrační faktor	X		
Linearizační faktor	X		
Legálně relevantní konfigurace registrů	X		
Nastavení např.: • legálně relevantní parametry korekčního zařízení, jako jsou parametry vycházející z interpolace křivky elektroměru k měření činné energie • transformační poměr	X		
Další relevantní parametry, které ovlivňují či by mohly ovlivnit výsledek měření	X		
Stahování legálně relevantního softwaru	X		

10.3.5 Přiřazení třídy rizika

Následující třída rizika je považována za odpovídající a měla by být použita při zkouškách softwaru elektroměrů k měření činné energie (řízených softwarem) dle této příručky:

- **Třída rizika C pro přístroje typu P a U**

[7] Vždy by měl vzít výrobce v úvahu národní požadavky týkající se doplňkových funkcí.
Další doporučení k intervalovému měření poskytuje WELMEC Guide 11.2.

10.4 Měřidla tepelné energie

10.4.1 Zvláštní předpisy, normy a jiné normativní dokumenty

V souladu s článkem 2 směrnice MID mohou členské státy nařídit, aby měřidla tepelné energie používaná v domácnostech, obchodech a lehkém průmyslu podléhaly směrnici MID. Specifické požadavky uvedené v této kapitole vycházejí pouze z přílohy MI-004.

Doporučení a normy organizace OIML nebyly zohledněny.

10.4.2 Technický popis

10.4.2.1 Konfigurace hardwaru

Měřidla tepelné energie jsou obvykle jednoúčelové přístroje (v tomto dokumentu označované jako typ P). Jedná se buď o samostatný přístroj, nebo přístroj tvořený několika podsestavami, např. snímače spotřeby, dvojice tepelných čidel a přepočítávací jednotky tak, jak je uvedeno ve směrnici MID, odst. 4(b). Měřič tepla může být rovněž kombinací těchto dvou typů.

10.4.2.2 Konfigurace softwaru

Konfigurace softwaru se liší podle výrobce, ale obvykle se předpokládá, že je v souladu s doporučeními uvedenými v hlavní části této příručky.

10.4.2.3 Princip měření

Měřidla tepelné energie průběžně kumulativně měří objem energie spotřebované v topném obvodu. Přístroj zobrazuje celkový objem spotřebované tepelné energie. Při měření se využívají různé principy.

Měření energie nelze opakovat.

10.4.2.4 Detekce a řešení chyb

Požadavek směrnice MI-004, 4.1 a 4.2 se zabývá elektromagnetickým rušením. Tento požadavek je nutné interpretovat v souvislosti s přístroji ovládanými softwarem, jelikož detekce rušení a náprava chyb se neobejdou bez součinnosti specifických částí hardwaru a softwaru. Z hlediska softwaru nezáleží na typu rušení (tj. zda se jedná o elektromagnetické, elektrické či mechanické rušení), jelikož postupy obnovy jsou vždy stejné.

10.4.3 Specifické požadavky na software (měřidla tepelné energie)

Třída rizika B	Třída rizika C	Třída rizika D
I4-1: Obnova po chybě *Software se musí po chybě v důsledku rušení dokázat vrátit do běžného provozu.*		
Upřesnění: Úseky chybného provozu by měly být pro lepší evidenci označeny datovým razítkem.		
Požadovaná dokumentace: Stručný popis mechanismu obnovy po chybě a kdy je tento mechanismus spuštěn.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda realizace obnovy po chybě probíhá náležitým způsobem. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Cyklicky vykonávaný podprogram mikroprocesoru nuluje hlídací mechanismus hardwaru, a brání tak jeho spuštění. Pokud některá funkce nebyla vykonána nebo pokud dokonce dojde k uvíznutí mikroprocesoru v jakékoliv nekonečné smyčce, nedojde k vynulování hlídacího mechanismu a hlídací mechanismus se tedy po určité době spustí.		

Třída rizika B	Třída rizika C	Třída rizika D
I4-2: Prostředky zálohování *Musí existovat prostředky zajišťující pravidelnou zálohu naměřených dat, jako jsou naměřené hodnoty a současný stav procesu. Tato data musejí být uložena v energeticky nezávislé paměti.*		
Upřesnění: Intervaly uložení musí být dostatečně krátké, aby byl rozdíl mezi aktuálními a uloženými kumulativními hodnotami malý.		
Požadovaná dokumentace: Stručný popis toho, jaká data jsou zálohována a kdy se zálohování provádí. Výpočet maximální chyby, k níž může při zálohování kumulativních hodnot dojít.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda jsou naměřená data uložena v energeticky nezávislé paměti a zda je lze obnovit. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Naměřená data jsou zálohována dle potřeby (např. každých 60 minut).		

Třída rizika B	Třída rizika C	Třída rizika D
I4-3: MID Příloha I, 8.5 (zamezení vynulování naměřených kumulativních hodnot) *Údaje o celkovém spotřebovaném objemu nebo údaje, z nichž lze celkový spotřebovaný objem odvodit, které se částečně či plně využívají k výpočtu ceny k zaplacení, musí být u přístrojů na měření spotřeby chráněny proti vynulování během provozu.*		
Upřesnění: Kumulativní čítače měřicího přístroje lze vynulovat před uvedením do provozu.		
Požadovaná dokumentace: Dokumentace prostředků zabezpečení proti vynulování ukazatelů objemu.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda legálně relevantní hodnoty kumulativního měření nelze vynulovat, aniž by o to byl záznam. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Čítače objemu jsou chráněny proti změnám a vynulování stejnými prostředky jako parametry přístroje (viz P7).		

Třída rizika B	Třída rizika C	Třída rizika D
I4-4: Dynamické chování *Legálně nerelevantní software nesmí nežádoucím způsobem ovlivňovat dynamiku procesu měření.*		
Upřesnění: • Tento požadavek aplikujte jako doplnění požadavků S-1, S-2 a S-3 v případě, že bylo provedeno oddělení softwaru dle rozšíření S. • Tento doplňující požadavek má zajistit, že při použití měřicích přístrojů v reálném čase nedojde k nežádoucímu ovlivnění dynamického chování legálně relevantního softwaru legálně nerelevantním softwarem, tj. že zdroje legálně relevantního softwaru nebudou nežádoucím způsobem omezeny legálně nerelevantním softwarem.		
Požadovaná dokumentace: • Popis hierarchie přerušení. • Časové schéma úkolů softwaru. Limity a poměrné časy pro legálně nerelevantní úkoly.		
Postup validace: *Ověření na základě dokumentace:* • Programátor legálně nerelevantní části softwaru má k dispozici dokumentaci s limity poměrných časů pro legálně nerelevantní úkoly. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Návrh hierarchie přerušení musí zamezit nežádoucím vlivům.		

Třída rizika B	Třída rizika C	Třída rizika D
I4-5: Vytištěné označení softwaru *Označení softwaru je obvykle zobrazeno na displeji. U měřičů tepla může být označení softwaru uvedeno rovněž na tištěném štítku s názvem přístroje. Takové řešení je přijatelné, pokud jsou splněny následující podmínky A, B a C:* *A. Uživatelské rozhraní nenabízí nástroj k aktivaci zobrazení označení softwaru na displeji, nebo displej přístroje technicky neumožňuje zobrazit označení softwaru (mechanický čítač).* *B. Přístroj nemá žádné rozhraní, kterým by označení softwaru mohl sdělit.* *C. Na vyrobeném přístroji již není možné software měnit, nebo je změna softwaru možná pouze v kombinaci s výměnou hardwaru nebo jeho části.*		
Upřesnění: • Výrobce hardwaru nebo příslušné hardwarové části zodpovídá za to, že je označení softwaru správně uvedeno na příslušném hardwaru. • Dále platí všechna další upřesnění požadavků P2/U2.		
Požadovaná dokumentace: • Viz P2/U2.		
Postup validace: *Ověření na základě dokumentace:* • Viz P2/U2. *Ověření funkčnosti:* • Viz P2/U2.		
Příklad přijatelného řešení: Vytištěné označení softwaru na štítku přístroje.		

10.4.4 Příklady legálně relevantních parametrů, funkcí a dat

Parametry měřičů tepla zahrnují např. konstanty pro přepočty, konfiguraci, atd., ale také parametry pro nastavení funkcí přístroje. Označení a zabezpečení parametrů a skupin parametrů je popsáno v požadavcích P2 a P7 v části věnované přístrojům typu P.

V následující tabulce jsou uvedeny některé z typických parametrů měřičů tepla. (Tabulka bude doplněna, jakmile pracovní skupina WELMEC WG 11 rozhodne o její finální podobě.)

Parametr	Chráněný	Nastavitelný	Poznámka
Kalibrační faktor	x		
Linearizační faktor	x		

10.4.5 Další vlastnosti

Neočekává se, že při použití přístrojů v domácnostech bude mít stahování softwaru (rozšíření D, kapitola 9) velký význam.

Kumulativní čítač energie nebo objemu, jímž jsou vybaveny domácí přístroje, není přístrojem s dlouhodobým uložením dat ve smyslu rozšíření L (kapitola 6). U přístroje, který měří pouze kumulované množství energie/objem, není aplikace rozšíření L nutná.

10.4.6 Přiřazení třídy rizika

V současnou chvíli je dle rozhodnutí příslušné pracovní skupiny WELMEC WG 11 považována za odpovídající následující třída rizika. Měla by být použita při zkouškách softwaru elektroměrů činné energie (řízených softwarem) dle této příručky:

- **Třída rizika C pro přístroje typu P**

Konečné rozhodnutí nicméně dosud nebylo přijato a WG 11 tuto záležitost znovu zváží v souvislosti s rozhodováním o odpovídající třídě či třídách rizika pro přístroje typu U.

10.5 Měřicí systémy pro kontinuální a dynamické měření množství kapalin jiných než voda

Měřicí systémy pro kontinuální a dynamické měření množství kapalin jiných než voda podléhají požadavkům směrnice MID. Specifické požadavky jsou uvedeny v příloze MI-005. Tyto specifické požadavky ani jiné normy dosud nebyly zohledněny.

Odstavce 10.5.1 – 10.5.2 budou v případě nutnosti doplněny v budoucnosti.

10.5.3 Specifické požadavky na systém (měřicí systémy pro kontinuální a dynamické měření množství kapalin jiných než voda)

Třída rizika B	Třída rizika C	Třída rizika D
I5-1: Vytištěné označení softwaru *Označení softwaru je obvykle zobrazeno na displeji. U měřicích systémů pro kontinuální a dynamické měření množství kapalin jiných než voda může být označení softwaru uvedeno rovněž na tištěném štítku s názvem přístroje. Takové řešení je přijatelné, pokud jsou splněny následující podmínky A, B a C:* *A. Uživatelské rozhraní nenabízí nástroj k aktivaci zobrazení označení softwaru na displeji, nebo displej přístroje technicky neumožňuje zobrazit označení softwaru (mechanický čítač).* *B. Přístroj nemá žádné rozhraní, kterým by označení softwaru mohl sdělit.* *C. Na vyrobeném přístroji již není možné software měnit, nebo je změna softwaru možná pouze v kombinaci s výměnou hardwaru nebo jeho části.*		
Upřesnění: • Štítek s označením softwaru musí být nesmazatelný a nepřenosný. • Výrobce hardwaru nebo příslušné hardwarové části zodpovídá za to, že je označení softwaru správně uvedeno na příslušném hardwaru. • Dále platí všechna další upřesnění požadavků P2/U2.		
Požadovaná dokumentace: • Viz P2/U2.		
Postup validace: *Ověření na základě dokumentace:* • Viz P2/U2. *Ověření funkčnosti:* • Viz P2/U2.		
Příklad přijatelného řešení: Vytištěné označení softwaru na štítku přístroje.		

Odstavce 10.5.4 a 10.5.5 budou v případě nutnosti doplněny v budoucnosti.

10.5.6 Přiřazení třídy rizika

V současnou chvíli je dle výsledků dotazníku WELMEC WG 7 (2004) a v souladu s budoucími rozhodnutími příslušné pracovní skupiny WELMEC považována za odpovídající následující třída rizika. Měla by být použita při zkouškách softwaru měřicích systémů pro kontinuální a dynamické měření množství kapalin jiných než voda (řízených softwarem) dle této příručky:

- **Třída rizika C**

10.6 Váhy

Váhy se dělí do dvou hlavních kategorií:

1. váhy s neautomatickou činností (angl. zkratka „NAWI“)
2. váhy s automatickou činností (angl. zkratka „AWI“)

Většina vah s automatickou činností podléhá směrnici MID. To neplatí pro váhy s neautomatickou činností, které se dosud řídí evropskou směrnicí 90/384/EEC. **Na váhy s neautomatickou činností se vztahuje softwarová příručka WELMEC 2.3, zatímco tato příručka se zabývá pouze vahami s automatickou činností.**

Specifické požadavky uvedené v této kapitole vycházejí z přílohy MI-006 a norem uvedených v článku 10.6.1, jestliže jsou v souladu s interpretací požadavků směrnice MID.

10.6.1 Zvláštní předpisy, normy a jiné normativní dokumenty

Požadavky přílohy MI-006 směrnice MID se vztahují na 5 kategorií automatických vážicích přístrojů:

- dávkovací váhy s automatickou činností (R51)
- gravimetrické plnicí váhy s automatickou činností (R61)
- diskontinuální součtové váhy (R107)
- kontinuální součtové váhy (pásové váhy) (R50)
- automatické kolejové mostové váhy (R106)

Čísla v závorkách odkazují na příslušná doporučení organizace OIML, která jsou z pohledu směrnice MID vnímána jako normy. Organizace WELMEC kromě toho vydala příručku WELMEC Guide 2.6 pro testování dávkovacích vah s automatickou činností.

Směrnice MID se nevztahuje na následující kategorii automatických vážicích přístrojů:

- automatické přístroje na vážení silničních vozidel v pohybu (R134)

Všechny kategorie automatických vážicích přístrojů mohou být realizovány jako typ přístroje P nebo U, a na každou kategorii se tudíž mohou vztahovat všechna rozšíření.

Specifické požadavky na software dle typu přístroje se nicméně ze všech šesti kategorií vztahují pouze na **diskontinuální součtové váhy** a **kontinuální součtové váhy** (pásové váhy) (viz 10.6.3). Důvodem je to, že tyto přístroje slouží ke kumulativnímu, relativně dlouhodobému měření, které v případě významné chyby nelze opakovat.

10.6.2 Technický popis

10.6.2.1 Konfigurace hardwaru

Diskontinuální součtová váha je váha na sypké produkty. Používá se k vážení velkého množství sypkého produktu (např. zrní), které rozdělí do více samostatných dávek. Systém obvykle tvoří jedna či více násypek umístěných na snímačích zatížení, zdroj napájení, elektronické ovladače a indikační zařízení.

Kontinuální součtová váha je pásová váha určující hmotnost určitého produktu na dopravním pásu, který projíždí přes snímač zatížení. Systém se obvykle skládá z

dopravního pásu, válců, snímače váhy na siloměrech, zdroje napájení, elektronických ovladačů a indikačního zařízení. Je také vybaven prostředky na úpravu napnutí pásu.

10.6.2.2 Konfigurace softwaru

Konfigurace softwaru se liší podle výrobce, ale obvykle se předpokládá, že je v souladu s doporučeními uvedenými v hlavní části této příručky.

10.6.2.3 Princip měření

U diskontinuální součtové váhy probíhá měření tak, že se produkt sype do násypky a váží. Postupně se určuje hmotnost každé samostatné dávky produktu a jednotlivé údaje se nakonec sečtou. Samostatně dávky se po zvážení přidávají k již odváženému produktu.

U kontinuální součtové váhy se hmotnost produktu určuje bez přerušení tak, jak produkt postupně prochází přes snímač zatížení. Měření probíhá v jednotkách času, jejichž délka se odvíjí od rychlosti pohybu pásu a síly vyvinuté na snímač zatížení. Na rozdíl od diskontinuálních součtových vah se produkt nerozděluje do menších částí a dopravní pás s produktem se nezastavuje. Celková váha produktu je součtem jednotlivých vzorků. Snímač zatížení může fungovat na bázi odporového tenzometru nebo jiné podobné technologie, jako např. strunového tenzometru.

10.6.2.4 Chyby

Články pásu mohou způsobovat nárazové efekty, které mohou vést k chybovým událostem při nulování přístroje. U diskontinuálních součtových vah může dojít ke ztrátě jednotlivých (nebo dokonce všech) výsledků vážení samostatných dávek před jejich sečtením.

10.6.3 Specifické požadavky na software (diskontinuální a kontinuální součtové váhy)

Oddíl 8 kapitoly 4 a oddíl 6 kapitoly 5 přílohy MI-006 směrnice MID se zabývají elektromagnetickým rušením. Tyto požadavky je nutné interpretovat v souvislosti s přístroji ovládanými softwarem, jelikož detekce rušení a náprava chyb se neobejdou bez součinnosti specifických částí hardwaru a softwaru. Z hlediska softwaru nezáleží na typu rušení (tj. zda se jedná o elektromagnetické, elektrické či mechanické rušení), jelikož postupy obnovy jsou vždy stejné.

Třída rizika B	Třída rizika C	Třída rizika D
I6-1: Obnova po chybě *Software musí detekovat, že došlo k narušení běžného provozu.*		
Upřesnění: Je-li detekována chyba: a. Kumulativní měření a jiné legálně relevantní údaje musí být automaticky uloženy do energeticky nezávislé paměti (viz požadavek I6-2), a b. Váha s násypkou nebo pásová váha se musí automaticky zastavit, nebo se musí spustit slyšitelný varovný signál (viz oddíl Požadovaná dokumentace)		
Požadovaná dokumentace: Stručný popis toho, co se kontroluje, co je nutné ke spuštění procesu detekce chyb a jaký postup následuje po detekci chyby. Pokud při detekci chyby není možné transportační systém okamžitě automaticky zastavit (např. z důvodu bezpečnosti), dokumentace musí zahrnovat popis toho, jak se zachází s nezváženým materiálem, nebo jak je takový materiál odpovídajícím způsobem zohledněn.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda realizace obnovy po chybě probíhá náležitým způsobem. *Ověření funkčnosti:* • Pokud je to možné simulujte určité hardwarové chyby a zkontrolujte, zda jsou detekovány a zda na ně software reaguje způsobem popsaným v dokumentaci.		
Příklad přijatelného řešení: Cyklicky vykonávaný podprogram mikroprocesoru nuluje hlídací mechanismus hardwaru, a brání tak jeho spuštění. Před vynulováním podprogram zkontroluje, jestli je systém v pořádku, např. jestli byly v posledním úseku vykonány všechny legálně relevantní podprogramy. Pokud nějaká funkce vykonána nebyla nebo pokud dokonce dojde k uvíznutí mikroprocesoru v jakékoliv nekonečné smyčce, nedojde k vynulování hlídacího mechanismu a hlídací mechanismus se tedy po určité době spustí.		

Třída rizika B	Třída rizika C	Třída rizika D

I6-2: Prostředky zálohování

Pro případ rušení musí existovat prostředky zajišťující pravidelnou zálohu naměřených dat, jako jsou naměřené hodnoty a současný stav procesu.

Upřesnění:

a. Popis stavu a důležité údaje musí být uloženy v energeticky nezávislé paměti.

b. Tento požadavek obvykle implikuje použití řízené paměti zajišťující automatické zálohování v případě rušení. Pravidelné zálohování je přípustné pouze tehdy, když není možné použít řízenou paměť kvůli hardwarovým nebo funkčním omezením. V takovém výjimečném případě musí být intervaly uložení zálohy dostatečně krátké, tj. maximální možný rozdíl mezi aktuálními a uloženými hodnotami se musí vejít do definovaného zlomku maximální přípustné chyby (viz oddíl Požadovaná dokumentace).

c. Prostředky zálohování by obvykle měly zahrnovat i odpovídající prostředky pro probuzení z režimu spánku, bránící tomu, aby se vážicí systém (včetně příslušného softwaru) v důsledku rušení nedostal do neurčitého stavu.

Požadovaná dokumentace:

Stručný popis mechanismu zálohování a dat, která jsou zálohována, včetně situací, kdy k zálohování dochází. Specifikace nebo výpočet maximální chyby, k níž může dojít u kumulativních hodnot, pokud je prováděno cyklické (periodické) zálohování.

Postup validace:

Ověření na základě dokumentace:

- Ověřte prostředky zálohování.

Ověření funkčnosti:

- Ověřte, zda při simulovaném rušení mechanismus zálohování funguje způsobem popsaným v dokumentaci.

Příklad přijatelného řešení:

Hlídací mechanismus hardwaru se spustí, pokud není cyklicky nulován. Tento alarm vyvolá přerušení v mikroprocesoru. Přiřazený přerušovací program okamžitě nashromáždí naměřené hodnoty, hodnoty stavu a jiné relevantní údaje a uloží je do energeticky nezávislé paměti, např. EEPROM, nebo do jiné vhodné paměti.

Poznámka: Předpokládá se, že přerušení vyvolané hlídacím mechanismem má nejvyšší prioritu, a je tudíž nadřazené jakýmkoliv běžným operacím nebo jakékoliv případné nekonečné smyčce, tj. ovladač programu při spuštění hlídacího mechanismu vždy přeskočí na přerušovací program.

10.6.4 Příklady legálně relevantních parametrů, funkcí a dat

Tabulka 10-1: V tabulce jsou uvedeny příklady legálně relevantních funkcí a dat a také funkcí a dat specifických pro daný přístroj (DF, DD) či daný typ přístroje (TF, TD) u automatických vážicích přístrojů a neautomatických vážicích přístrojů (R76). Zkratka VV označuje proměnné.

Funkce/data	Typ	Číslo doporučení OIML						
		50	51 (X)	51 (Y)	61	76	106	107
Výpočet hmotnosti	TF, TD	X	X	X	X	X	X	X
Analýza stability	TF, TD		X	X	X	X	X	X
Výpočet ceny	TF, TD			X		X		
Algoritmus zaokrouhlení ceny	TF, TD			X		X		
Rozsah (citlivost)	DD	X	X	X	X	X	X	X
Korekce nelinearity	DD (TD)	X	X	X	X	X	X	X
Max, min, e, d	DD (TD)	X	X	X	X	X	X	X
Jednotky měření (např. g, kg)	DD (TD)	X	X	X	X	X	X	X
Zobrazená hodnota vážení (zaokrouhlena na násobky e nebo d)	VV	X		X		X	X	X
Tára, nastavení táry	VV		X	X	X	X	X	
Cena za jednotku, celková cena	VV			X		X		X
Hmotnost v interním rozlišení	VV	X	X	X	X	X	X	X
Stavové signály (nulová hodnota, stabilita rovnováhy)	TF	X	X	X	X	X	X	X
Porovnání aktuální hmotnosti s nastavenou hodnotou	TF		X		X			
Automatický tisk, např. přerušení automatické operace	TF	X						X
Doba zahřívání	TF (TD)	X	X	X	X	X	X	X
Vzájemné blokování funkcí,	TF		X	X				
např. nastavení nuly/nulování táry,			X	X	X	X		
automatický/neautomatický provoz,							X	
nastavení nuly/sčítání		X						X
Záznam o přístupu k dynamickému nastavení	TF (VV)		X	X				
Maximální rychlost provozu/rozsah rychlostí provozu (dynamické vážení)	DD (TD)	X	X	X	X		X	X
(Produktové) parametry výpočtu dynamického vážení	VV		X	X			X	
Přednastavená hmotnost	VV		X		X			
Rozsah možností nastavení	DD (TD)		X	X				
Kritéria pro automatické nastavení nuly (např. časový interval, konec cyklu vážení)	DD (TD)		X	X	X		X	X
Minimální výkon, jmenovité minimální plnění	DD				X			X
Limitní hodnota signifikantní chyby (pokud není 1e nebo 1d)	DD (TD)	X			X			
Krajní hodnota výkonu baterie	DD (TD)	X	X	X	X	X	X	X

Tabulka 10-1: Příklady funkcí a dat - legálně relevantních a specifických pro daný přístroj nebo typ

Funkce a parametry označené ve výše uvedené tabulce se pravděpodobně vyskytují u různých typů vážicích přístrojů. Pokud je tomu tak, je třeba k nim přistupovat jako k „legálně relevantním“. Tato tabulka nicméně není závazným předpisem, podle něhož by musel být každý přístroj vybaven funkcemi či parametry v něm uvedenými.

10.6.5 Další vlastnosti

Žádné

10.6.6 Přiřazení třídy rizika

V současné chvíli se na základě rozhodnutí příslušné pracovní skupiny WELMEC (24. schůze WG 2, 22. - 23. ledna 2004) na všechny kategorie automatických vážicích přístrojů bez ohledu na typ (P či U) **musí obecně vztahovat třída rizika „B“**.

Dle výsledků dotazníku WG 7 (2004) se nicméně doporučuje rozlišovat přístroje typu P a přístroje typu U a diskontinuální a kontinuální součtové váhy:

- **Třída rizika B pro přístroje typu P (kromě součtových vah)**
- **Třída rizika C pro přístroje typu U a součtové váhy typu P a U**

10.7 Taxametry

Taxametry podléhají předpisům směrnice MID. Specifické požadavky na tyto přístroje jsou uvedeny v Příloze MI-007, avšak nebyly dosud brány v potaz, stejně jako žádné jiné normy.

10.7.1 Zvláštní předpisy, normy a jiné normativní dokumenty

Evropská norma EN50148, která by se mohla stát normativním dokumentem ve smyslu směrnice MID, dosud nebyla zohledněna. Projekt „MID-Procedures“ dal nicméně vzniknout návodu pro taxametry, který se v budoucnu stane základem příručky WELMEC. Organizace OIML dále vydala první verzi doporučení pro taxametry. Tento dokument však ještě není v takové podobě, aby mohl být použit jako norma (stav k říjnu 2004).

10.7.2 Technický popis

Taxametr je ve směrnici MID definován jako měřič času a vzdálenosti vypočítávající jízdné za cestu na základě příslušných tarifů. Využívá přitom výstup generátoru signálu, který nepodléhá směrnici MID.

Moderní taxametry využívají integrovanou architekturu, tj. dle této příručky jsou považovány za jednoúčelové přístroje (typu P). Očekává se, že se v budoucnu budou vyrábět i jako přístroje využívající univerzální počítač (typ U).

10.7.3 Specifické požadavky na software

MID Příloha MI-007, 9:

> V případě poklesu napájení pod minimální hodnotu potřebnou pro provoz přístroje stanovenou výrobcem taxametr musí:
>
> – nadále správně fungovat, nebo správně obnovit svou činnost bez ztráty dat dostupných před výpadkem napájení, pokud se jedná o krátkodobý stav, tj. v důsledku restartování motoru,
> – ukončit stávající měření a vrátit se do stavu „volný“ („for hire“), pokud se jedná o dlouhodobější výpadek napájení.

Taxametr musí mít možnost dlouhodobého uložení dat - data v taxametru musí být dostupná nejméně 1 rok, viz MI-007, 15.2.

Třída rizika B	Třída rizika C	Třída rizika D
I7-1: Prostředky zálohování *Musí existovat prostředky zajišťující automatickou zálohu nejdůležitějších dat, jako jsou naměřené hodnoty a současný stav procesu, pro případ, že by došlo k dlouhodobějšímu výpadku napájení.*		
Upřesnění: 1) Tyto údaje by obvykle měly být uloženy v energeticky nezávislé paměti. 2) Přístroj musí být vybaven detektorem úrovně napětí, který vyhodnotí, kdy je nutné naměřené hodnoty uložit. 3) Prostředky zálohování musí zahrnovat i odpovídající prostředky probuzení přístroje ze spánku, aby se taxametr (včetně příslušného softwaru) nemohl dostat do neurčitého stavu.		
Požadovaná dokumentace: Stručný popis toho, jaká data jsou zálohována a kdy.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda jsou naměřená data zálohována v případě rušení. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Dojde-li k výpadku napětí přesahujícímu 15 vteřin, vyvolá detektor úrovně napětí přerušení. Přiřazený přerušovací program nashromáždí naměřené hodnoty, údaje o stavu a další relevantní údaje a uloží je do energeticky nezávislé paměti, např. EEPROM. Poté, co je napájení obnoveno, data jsou obnovena a přístroj pokračuje v provozu, nebo je měření ukončeno (viz MI-007, 9.) *Poznámka:* Předpokládá se, že přerušení v důsledku výpadku napájení má vysokou prioritu, a je tudíž nadřazené jakýmkoliv běžným operacím nebo jakékoliv případné nekonečné smyčce, tj. ovladač programu pří výpadku napájení vždy přeskočí na přerušovací program.		

10.7.4 Příklady legálně relevantních parametrů, funkcí a dat

V následující tabulce jsou uvedeny některé z typických parametrů taxametrů.

Parametr	Chráněný	Nastavitelný	Poznámka
K-faktor	x		impulzy / km
Tarify	x	x	jednotka měny / km, jednotka měny / h
Parametry rozhraní		x	modulační rychlost atd.

10.7.5 Další vlastnosti

Doporučujeme provést revizi směrnice pro motorová vozidla nebo jakékoliv jiné směrnice za účelem stanovení požadavků na generátory signálu v motorových prostředcích používaných jako taxi. Předběžný návrh zní:

Na motorová vozidla určená k použití jako taxi se vztahují následující požadavky:

1. Generátor signálu musí vysílat signál s minimálním rozlišením 2 metry.
2. Generátor signálu musí vysílat stabilní signál při jakékoliv rychlosti jízdy.
3. Generátor signálu musí mít definované následující vlastnosti: úroveň napájení, šířka impulzu a vztah rychlosti a frekvence.
4. Testovatelnost…

10.7.6 Přiřazení třídy rizika

V současnou chvíli jsou dle výsledků dotazníku WELMEC WG 7 (2004) a v souladu s budoucími rozhodnutími příslušné pracovní skupiny WELMEC považovány za odpovídající následující třídy rizika. Měly by být použity při zkouškách softwaru taxametrů (řízených softwarem) dle této příručky:

- **Třída rizika C pro přístroje typu P**
- **Třída rizika D pro přístroje typu U**

10.8 Ztělesněné míry

Ztělesněné míry jsou zařízení podléhající zvláštním požadavkům směrnice MID uvedené v Příloze MI-008.

V důsledku budoucího vývoje a dalších rozhodnutí nejsou ztělesněné míry považovány za měřicí přístroje ovládané softwarem ve smyslu přílohy MI-008 směrnice MID. Proto se na ně v současnou chvíli tato softwarová příručka nevztahuje.

10.9 Měřicí přístroje na měření rozměrů

Přístroje na měření rozměrů podléhají specifickým požadavkům směrnice MID uvedené v Příloze MI-009. Tyto specifické požadavky ani žádné jiné normy dosud nebyly brány v potaz.

Odstavce 10.9.1 - 10.9.5 budou v případě nutnosti doplněny v budoucnu.

10.9.6 Přiřazení třídy rizika

V současnou chvíli jsou dle výsledků dotazníku WELMEC WG 7 (2004) a v souladu s budoucími rozhodnutími příslušné pracovní skupiny WELMEC považovány za odpovídající následující třídy rizika. Měly by být použity při zkouškách softwaru měřicích přístrojů na měření rozměrů (řízených softwarem) dle této příručky:

- **Třída rizika B pro přístroje typu P**
- **Třída rizika C pro přístroje typu U**

10.10 Analyzátory výfukových plynů

Analyzátory výfukových plynů podléhají specifickým požadavkům směrnice MID uvedené v Příloze MI-010. Tyto specifické požadavky ani žádné jiné normy dosud nebyly brány v potaz.

Odstavce 10.10.1 - 10.10.5 budou v případě nutnosti doplněny v budoucnu.

10.10.6 Přiřazení třídy rizika

V současnou chvíli jsou dle výsledků dotazníku WELMEC WG 7 (2004) a v souladu s budoucími rozhodnutími příslušné pracovní skupiny WELMEC považovány za odpovídající následující třídy rizika. Měly by být použity při zkouškách softwaru analyzátorů výfukových plynů (řízených softwarem) dle této příručky:

- **Třída rizika B pro přístroje typu P**
- **Třída rizika C pro přístroje typu U**

11 Vzor protokolu o zkoušce (včetně kontrolních seznamů)

Tato kapitola obsahuje vzorový protokol o zkoušce. Skládá se z hlavní části a dvou příloh. Hlavní část protokolu obsahuje obecné informace o testovaném objektu. Musí být vždy náležitým způsobem upraven podle konkrétního případu. Přílohu 1 tvoří dva kontrolní seznamy usnadňující výběr odpovídajících konfigurací dle této příručky. Příloha 2 obsahuje dva kontrolní seznamy pro příslušné technické konfigurace. Doporučuje se, aby výrobce i zkoušející tyto seznamy používali jako pomůcku k prokázání, že byly zváženy všechny požadavky, které se na daný přístroj vztahují.

Kromě toho jsou v následující podkapitole vyjmenovány informace, které je třeba uvádět v certifikátu schválení typu.

11.3 Informace náležející do certifikátu

Protokol o zkoušce zahrnuje dokumentaci daného přístroje, informace o validaci a její výsledky. Pro certifikát je pak nutné vytvořit výtah z informací obsažených v protokolu o zkoušce. Tento výtah by měl zahrnovat následující body týkající se softwaru:

1. **Typ softwaru**
   - Uvedení verze WELMEC Guidu 7.2, typu softwaru (P či U), rizikové třídy (A až E) a aplikovaných rozšíření (L, T, S , D, Ix)

Riziková třída [A-E] _	P ☐	U ☐	L ☐	T ☐	S ☐	D ☐	Ix ☐ [1-6] _

2. **Označení softwaru**
   - Uvedení platné hodnoty označení legálně relevantního softwaru
   - Popis jak lze označení legálně relevantního softwaru zobrazit

3. **Ověření integrity softwaru**
   - **Pro rizikovou třídu C a vyšší:** uvedení kontrolního součtu či hodnoty alternativní metody se stejnou úrovní požadavků
   - **Pro rizikovou třídu C a vyšší: přesný** popis způsobu zobrazení kontrolního součtu či hodnoty alternativní metody se stejnou úrovní požadavků
     Pozn.: Odkaz na dokumentaci (např. uživatelský manuál) je nevhodný.
   - Popis způsobu zobrazení údajů z počítadla / záznamníku událostí, pokud jsou aplikovány
   - Popis hardwarového zabezpečení a dalších typů softwarového zabezpečení na úrovni plomby, pokud jsou aplikovány
   - Uvedení dalších způsobů ochrany integrity, pokud jsou aplikovány.

4. **Stručný popis softwarového prostředí**
   - Uvedení relevantních informací o:

- Operačním prostředí nezbytném pro fungování softwaru (např. operační systém).
- Softwarových modulech podléhajících legalní kontrole (v případě, že je aplikováno oddělení softwaru).
- Hardwarových a softwarových rozhraní (např. IR rozhraní, Bluetooth, bezdrátové sítě LAN…).
- Electronických (hardwarových) částech a jejich umístění v měřicím přístroji včetně jejich zabezpečení, pokud je třeba.

11.4 Vzor obecné části protokolu o zkoušce

Protokol o zkoušce č. XYZ122344

Průtokoměr Dynaflow, model DF101

Validace softwaru

(X příloh)

Pověření

Směrnice MID (Measuring Instruments Directive) udává základní požadavky na některé měřicí přístroje používané v Evropské unii. Software daného měřicího přístroje byl validován za účelem prokázání shody se základními požadavky této směrnice.

Validace byla založena na zprávě WELMEC MID Software Requirements Guide WELMEC Guide 7.2, v níž jsou vysvětleny základní požadavky na software měřicích přístrojů. Tato zpráva popisuje způsob zkoušení software za účelem prokázání souladu se směrnicí MID.

Zadavatel

Dynaflow
P.O. Box 1120333
100 Reykjavík
Island
Kontaktní osoba: Pan Bjarnur Sigfridson

Zkoušený přístroj

Průtokoměr Dynaflow DF100 je měřicí přístroj na měření průtoku kapalin. Zamýšlený rozsah měření je 1 - 2000 l/s. K základním funkcím přístroje patří:

- měření průtoku kapalin
- zobrazení změřeného objemu
- rozhraní převodníku

Dle příručky WELMEC Guide 7.2 je průtokoměr popsán následovně:

- jednoúčelový měřicí přístroj (se zabudovaným systémem)
- přístroj pro dlouhodobé uložení naměřených dat

Průtokoměr DF100 je samostatný přístroj s převodníkem, který je k přístroji pevně a trvale připojen a nelze ho odpojit. Naměřený objem se zobrazuje na displeji. Přístroj neumožňuje komunikaci s jinými zařízeními.

Vestavěný software měřicího přístroje vyvinula firma

Dynaflow, P.O. Box 1120333, 100 Reykjavík, Island.

strana 1 / 3

Validovaná verze software má označení **V1.2c**. Zdrojový kód je tvořen následujícími soubory:

main.c	12301 bytů	23. listopadu 2003
int.c	6509 bytů	23. listopadu 2003
filter.c	10897 bytů	20. října 2003
input.c	2004 bytů	20. října 2003
display.c	32000 bytů	23. listopadu 2003
Ethernet.c	23455 bytů	15. června 2002
driver.c	11670 bytů	15. června 2002
calculate.c	6788 bytů	23. listopadu 2003

Při validaci byly předloženy následující dokumenty výrobce:

- Uživatelská příručka DF 100
- Návod na údržbu DF 100
- Popis softwaru DF100 (vnitřní návrh, dokument z 22. listopadu 2003)
- Schéma elektronického obvodu DF100 (nákres č. 222-31 z 15. října 2003)

Konečná verze zkoušeného přístroje byla doručena do národní zkušební laboratoře (National Testing & Measurement Laboratory) dne 25. listopadu 2003.

Postup zkoušení

Validace byla provedena v souladu se softwarovou příručkou WELMEC 7.2 Software Guide, 2019 (ke stažení na www.welmec.org).

Validační zkoušky probíhaly od 1. 11. do 23. 12. 2003. Kontrola návrhu byla provedena 3. 12. doktorem K. Fehlerem v sídle firmy Dynaflow v Reykjavíku. Další validační úkony provedli v národní zkušební laboratoři doktor K. Fehler a M. S. Problème.

Byla ověřena shoda s následujícími požadavky:

- Specifické požadavky na vestavěný software jednoúčelových měřicích přístrojů (typ P)
- Rozšíření L: dlouhodobé uložení naměřených dat

Kontrolní seznam pro výběr konfigurace tvoří přílohu 1 této zprávy.

Přístroji byla přiřazena třída rizika C.

Byly použity následující metody validace:

- úplnost dokumentace
- kontrola operačního manuálu
- testy funkčnosti
- kontrola návrhu softwaru
- kontrola dokumentace softwaru
- analýza toku dat
- simulace vstupních signálů

Výsledek

Byla prokázána shoda s následujícími požadavky WELMEC Software Guide 7.2, a to bez nalezených chyb:

- P1, P2, P3, P5, P6, P7, P8
  (požadavek P4 byl vyhodnocen jako nerelevantní)
- L1, L2, L3, L4, L5, L6, L7, L8

Kontrolní seznamy k požadavkům P tvoří přílohu 2.1 této zprávy.

Kontrolní seznamy k požadavkům L tvoří přílohu 2.2 této zprávy.

Byly nalezeny dva příkazy, jež nebyly zahrnuty do původního návodu na obsluhu. Tyto dva příkazy byly následně začleněny do návodu na obsluhu z 10. prosince 2003.

V softwarovém balíčku V1.2b byla rovněž nalezena chyba omezující počet dní měsíce února na 28 i v přestupných letech. Tato chyba byla ve verzi V1.2c opravena.

Software přístroje Dynaflow DF100 V1.2c splňuje základní požadavky směrnice MID.

Tento výsledek je platný pouze pro zkoušený přístroj.

Národní zkušební laboratoř (National Testing & Measurement Lab)
Oddělení pro software (Software Department)

Dr. K.E.I.N. Fehler
Technický vedoucí

M. S.A.N.S Problème
Technický referent

Datum: 23. prosince 2003

strana 3 / 3

11.5 Příloha 1 protokolu o zkoušce: Kontrolní seznamy pro výběr odpovídajících konfigurací

První kontrolní seznam pomáhá uživateli rozhodnout, jakou má zkoušený přístroj základní konfiguraci (P nebo U).

Určení typu přístroje				
		(P)		**Poznámky**
1	Je celý aplikační software určen pro účely měření?			
		(Ano)		
2	Jsou splněny požadavky pro začlenění operačního systému nebo podsystémů?			
		(Ano)		
3	Pokud je možné přístroj přepnout do režimu provozu nepodléhajícího legální kontrole, je zamezen přístup do operačního systému?			
		(Ano)		
4	Jsou implementované programy a softwarové prostředí neměnné (kromě aktualizací)?			
		(Ano		
5	Existují v přístroji nějaké programovací nástroje?			
		(Ne)		
Zaškrtněte příslušná políčka.				

Požadavky na přístroje typu P (kapitola 4) se na daný přístroj budou vztahovat pouze tehdy, když budou všechny odpovědi na otázky zaškrtnuté tak, jak je uvedeno ve sloupci P. Ve všech ostatních případech se na přístroj musí vztahovat požadavky pro přístroje typu U (kapitola 5).

Druhý kontrolní seznam pomáhá uživatelům určit, jakou má zkoušený přístroj IT konfiguraci.

Určení požadovaného rozšíření					
Pož. rozšíření		**ANO**	**NE**	**Nerelevantní**	**Poznámky**
L	Dokáže přístroj uložit naměřená data do integrované paměti nebo do paměti univerzálního počítače či do vzdálené nebo výměnné paměti?				
T	Přenášejí se naměřená data přes komunikační sítě do vzdálených zařízení, kde jsou dále zpracovávána anebo používána k legálně relevantním účelům?				
S	Mají nějaké části softwaru funkce, které nepodléhají legální kontrole, a bude potřeba tyto části softwaru po schválení měnit?				
D	Bude možné (či bude potřeba) po uvedení přístroje do provozu stahovat software?				
U každé otázky, na kterou jste odpověděli ANO, je nutné zvážit požadavky příslušného rozšíření.					

11.6 Příloha 2 protokolu o zkoušce: Kontrolní seznamy pro konkrétní technické konfigurace

1) Kontrolní seznam základních požadavků na přístroje typu P

Kontrolní seznam požadavků na přístroje typu P						
Požadavek	**Postupy zkoušení**		**Vyhověl**	**Nevyhověl**	**Nerelevantní**	**Poznámky***
P1		Splňuje požadovaná dokumentace výrobce požadavek P1 (a-f)?				
P2		Je označení softwaru realizováno dle požadavku P2?				
P3		Nemohou příkazy zadávané přes uživatelská rozhraní nepřípustně ovlivnit legálně relevantní software či naměřená data?				
P4		Nedochází k nepřípustnému ovlivňování legálně relevantního softwaru, specifických parametrů přístroje a naměřených dat příkazy zadávanými přes komunikační rozhraní přístroje?				
P5		Jsou legálně relevantní software a naměřená data chráněny proti náhodným či neúmyslným změnám?				
P6		Je legálně relevantní software zabezpečen proti nepřípustným záměrným modifikacím, nahrávání či výměně hardwarové paměti?				
P7		Jsou legálně relevantní parametry zabezpečeny proti nepřípustným modifikacím?				
P8		Je zajištěna autentičnost prezentovaných naměřených dat?				
**V případě odchylky proti požadavkům na software je nutné uvést vysvětlení.*						

2) Kontrolní seznam základních požadavků na přístroje typu U

Kontrolní seznam požadavků na přístroje typu U						
Požadavek	**Postupy zkoušení**		**Vyhověl**	**Nevyhověl**	**Nerelevantní**	**Poznámky***
U1		Splňuje požadovaná dokumentace výrobce požadavek U1 (a-g)?				
U2		Je označení softwaru realizováno dle požadavku U2?				
U3		Nemohou příkazy zadávané přes uživatelské rozhraní nepřípustně ovlivňovat legálně relevantní software a naměřená data?				
U4		Nedochází k nepřípustnému ovlivňování legálně relevantního softwaru, specifických parametrů přístroje a naměřených dat příkazy zadávanými přes komunikační rozhraní přístroje?				
U5		Jsou legálně relevantní software a naměřená data chráněny proti náhodným či neúmyslným změnám?				
U6		Jsou legálně relevantní software a naměřená data chráněny proti nepřípustným záměrným modifikacím či výměně?				

U7		Jsou legálně relevantní parametry zabezpečeny proti nepřípustným modifikacím?				
U8		Je zajištěna autentičnost prezentovaných naměřených dat?				
U9		Je legálně relevantní software navržen tak, aby nemohl být nepřípustným způsobem ovlivněn jiným softwarem?				
**V případě odchylky proti požadavkům na software je nutné uvést vysvětlení.*						

3) Kontrolní seznam pro specifické požadavky rozšíření L

Kontrolní seznam požadavků rozšíření L						
Požadavek	**Postupy zkoušení**		**Vyhověl**	**Nevyhověl**	**Nerelevantní**	**Poznámky***
L1		Jsou naměřená data doplněna všemi důležitými informacemi potřebnými pro legálně relevantní účely?				
L2		Jsou uložená data zabezpečena proti náhodným či neúmyslným změnám?				
L3		Jsou uložená naměřená data chráněna proti záměrným změnám?				
L4		Je možné dohledat měření a měřicí přístroj, při němž konkrétní uložená naměřená data vznikla?				
L5		Je s klíči a s nimi souvisejícími informacemi nakládáno jako s naměřenými daty a jsou uchovávány v utajení a chráněny proti zneužití?				
L6		Je přístroj vybaven legálně relevantním softwarem pro čtení, verifikaci a zobrazení uložených naměřených dat?				
L7		Jsou naměřená data uložena automaticky po ukončení měření?				
L8		Je kapacita paměti na dlouhodobé uložení dat pro zamýšlený účel dostatečná?				
**V případě odchylky proti požadavkům na software je nutné uvést vysvětlení.*						

4) Kontrolní seznam pro specifické požadavky rozšíření T

Kontrolní seznam požadavků rozšíření T						
Požadavek	**Postupy zkoušení**		**Vyhověl**	**Nevyhověl**	**Nerelevantní**	**Poznámky***
T1		Obsahují přenášená data všechny informace potřebné k zobrazení nebo dalšímu zpracování naměřených výsledků v přijímací jednotce?				
T2		Jsou data při přenosu zabezpečena proti náhodným a neúmyslným změnám?				
T3		Jsou legálně relevantní data při přenosu zabezpečena proti záměrným změnám ?				
T4		Je možné dohledat měření a měřicí přístroj, při němž konkrétní přenesená data vznikla?				
T5		Je s klíči a s nimi souvisejícími informacemi zacházeno jako s naměřenými daty a jsou uchovávány v utajení a chráněny proti zneužití?				
T6		Je přístroj vybaven legálně relevantním softwarem pro čtení, verifikaci a zacházení s přenesenými naměřenými daty?				
T7		Existují prostředky bránící nepřípustnému ovlivnění měření v důsledku zpoždění při přenosu?				
T8		Je zajištěno, aby se naměřená data neztratila při výpadku služeb sítě?				
**V případě odchylky proti požadavkům na software je nutné uvést vysvětlení.*						

5) Kontrolní seznam pro specifické požadavky rozšíření S

Kontrolní seznam požadavků rozšíření S						
Požadavek	**Postupy zkoušení**		**Vyhověl**	**Nevyhověl**	**Nerelevantní**	**Poznámky***
S1		Je část softwaru zahrnující všechen legálně relevantní software a parametry jasně oddělená od ostatních částí softwaru?				
S2		Jsou informace generované legálně nerelevantním softwarem zobrazeny na displeji nebo tištěném výstupu takovým způsobem, aby nemohlo dojít k jejich záměně s informacemi generovanými legálně relevantním softwarem?				
S3		Je výměna dat mezi legálně relevantním softwarem a legálně nerelevantním softwarem prováděna pouze přes ochranné softwarové rozhraní?				
**V případě odchylky proti požadavkům na software je nutné uvést vysvětlení.*						

6) Kontrolní seznam pro specifické požadavky rozšíření D

Kontrolní seznam požadavků rozšíření D						
Požadavek	**Postupy zkoušení**		**Vyhověl**	**Nevyhověl**	**Nerelevantní**	**Poznámky***
D1		Proběhnou obě fáze stahování softwaru (tj. přenos a následná instalace) automaticky bez vlivu na zabezpečení legálně relevantního softwaru?				
D2		Má systém prostředky zaručující autentičnost staženého softwaru?				
D3		Je systém vybaven prostředky, jež zaručí, že při stahování nedošlo k nepřípustným změnám stahovaného softwaru?				
D4		Je systém vybaven odpovídajícími technickými prostředky, které umožní dohledat návaznost stahovaného legálně relevantního softwaru příslušného přístroje za účelem následných kontrol?				
**V případě odchylky proti požadavkům na software je nutné uvést vysvětlení.*						

12 Křížové odkazy požadavků této příručky k článkům a přílohám směrnice MID

(Související verze směrnice MID: DIRECTIVE 2014/32/EU, 26. února 2014)

12.3 Požadavky na software, odkaz na směrnici MID

Požadavek		MID	
Č.	**Označení**	**Článek / Příloha č.** (AI = Příloha 1)	**Označení**
	Základní příručka P		
P1	Dokumentace výrobce	AI-9.3 AI-12 Článek 18	Informace o přístroji, které přístroj provázejí Hodnocení shody Technická dokumentace
P2	Označení softwaru	AI-7.6 AI-8.3	Vhodnost Ochrana před zneužitím
P3	Příkazy zadané přes uživatelské rozhraní	AI-7.1	Vhodnost
P4	Příkazy zadané přes komunikační rozhraní	AI-7.1 AI-8.1	Vhodnost Ochrana před zneužitím
P5	Zabezpečení proti náhodným či neúmyslným změnám	AI-7.1, AI-7.2 AI-8.4	Vhodnost Ochrana před zneužitím
P6	Zabezpečení proti záměrným změnám	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Vhodnost[8] Ochrana před zneužitím
P7	Ochrana parametrů	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Vhodnost Ochrana před zneužitím
P8	Autentičnost softwaru a prezentace výsledků	AI-7.1, AI-7.2, AI-7.6 AI-8.3, AI-10.2, AI-10.3, AI-10.4	Vhodnost Ochrana před zneužitím Indikace výsledku
	Základní příručka U		
U1	Dokumentace výrobce	AI-9.3 AI-12 Článek 18	Informace o přístroji, které přístroj provázejí Hodnocení shody Technická dokumentace
U2	Označení softwaru	AI-7.6 AI-8.3	Vhodnost Ochrana před zneužitím
U3	Příkazy zadané přes uživatelská rozhraní	AI-7.1	Vhodnost
U4	Příkazy zadané přes komunikační rozhraní	AI-7.1 AI-8.1	Vhodnost Ochrana před zneužitím
U5	Zabezpečení proti náhodným či neúmyslným změnám	AI-7.1, AI-7.2 AI-8.4	Vhodnost Ochrana před zneužitím
U6	Zabezpečení proti záměrným změnám	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Vhodnost Ochrana před zneužitím
U7	Ochrana parametrů	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Vhodnost Ochrana před zneužitím
U8	Autentičnost softwaru a prezentace výsledků	AI-7.1, AI-7.2, AI-7.6 AI-8.3 AI-10.2, AI-10.3, AI-10.4	Vhodnost Ochrana před zneužitím Označení výsledku

[8] Poznámka: Co se týká obsahu, článek 7.1 přílohy 1 směrnice MID není otázkou „Vhodnosti“, ale „Ochrany proti zneužití“ (článek 8)

Požadavek		MID	
Č.	**Označení**	**Článek / Příloha č.** (AI = Příloha 1)	**Označení**
U9	Vliv jiného softwaru	AI-7.6	Vhodnost Ochrana před zneužitím
	Rozšíření L		
L1	Úplnost uložených dat	AI-7.1 AI-8.4 AI-10.2	Vhodnost Ochrana proti zneužití Označení výsledku
L2	Ochrana proti náhodným či neúmyslným změnám	AI-7.1, AI-7.2 AI-8.4	Vhodnost Ochrana proti zneužití
L3	Integrita dat	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
L4	Autentičnost uložených dat	AI-7.1 AI-8.4 AI-10.2	Vhodnost Ochrana proti zneužití Označení výsledku
L5	Utajení klíčů	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
L6	Načtení uložených dat	AI-7.2 AI-10.1, AI-10.2, AI-10.3, AI-10.4	Vhodnost Označení výsledku
L7	Automatické uložení	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
L8	Kapacita paměti a kontinuita	AI-7.1	Vhodnost
Lx	Celý obsah rozšíření L	AI-11.1	Další zpracovávání dat k uzavření obchodní transakce
	Rozšíření T		
T1	Úplnost přenášených dat	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
T2	Ochrana proti náhodným změnám	AI-7.1, AI-7.2 AI-8.4	Vhodnost Ochrana proti zneužití
T3	Integrita dat	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
T4	Autentičnost přenášených dat	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
T5	Utajení klíčů	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
T6	Zacházení s poškozenými daty	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
T7	Zpoždění při přenosu	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
T8	Dostupnost přenosových služeb	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
	Rozšíření S		
S1	Realizace oddělení softwaru	AI-7.6, AI-10.1	Vhodnost Označení výsledku
S2	Smíšená indikace	AI-7.1, AI-7.2, AI-7.6 AI-10.2	Vhodnost Označení výsledku
S3	Ochranné rozhraní softwaru	AI-7.6	Vhodnost
	Rozšíření D		
D1	Mechanismus stahování	AI-8.2, AI-8.4	Ochrana proti zneužití
D2	Prokázání věrohodnosti přeneseného softwaru	AI-7.6 AI-8.3, AI-8.4 AI-12	Vhodnost Ochrana proti zneužití Hodnocení shody
D3	Integrita stahovaného softwaru	AI-7.1, AI-8.4	Vhodnost Ochrana proti zneužití
D4	Dohledatelnost stahovaného legálně relevantního softwaru	AI-7.1, AI-7.6 AI-8.2, AI-8.3 AI-12	Vhodnost Ochrana proti zneužití Hodnocení shody

Požadavek		MID	
Č.	**Označení**	**Článek / Příloha č.** (AI = Příloha 1)	**Označení**
	Rozšíření I (Požadavky na software přístrojů konkrétního typu)		
I1-1, I2-1, I3-1, I4-1	Obnova po chybě	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Spolehlivost Specifické požadavky na přístroje na měření spotřeby
I1-2, I2-2, I3-2, I4-2	Prostředky zálohování	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Spolehlivost Specifické požadavky na přístroje na měření spotřeby
I1-4, I2-4, I3-4, I4-4	Vnitřní rozlišení, vhodnost označení	MI-002-5.3, MI-003-5.2	Specifické požadavky na přístroje na měření spotřeby
I1-3, I2-4, I3-4, I4-3	Zamezení vynulování naměřených kumulativních hodnot	AI-8.5	Ochrana proti zneužití
I1-4, I2-8, I3-5, I4-4	Dynamické chování	AI-7.6	Vhodnost Ochrana proti zneužití
I2-5	Životnost zdroje napájení	MI-002-5.2	Specifické požadavky na přístroje na měření spotřeby
I2-6	Elektronické přepočítávače objemu	MI-002-9.1	Specifické požadavky na přístroje na měření spotřeby
I2-7	Testovací prvek	MI-002-5.5	Specifické požadavky na přístroje na měření spotřeby
I6-1	Detekce chyb	MI-006-IV, MI-006-V	Diskontinuální a kontinuální součtové váhy
I6-2	Prostředky zálohování, detekce chyb	MI-006-IV, MI-006-V	Diskontinuální a kontinuální součtové váhy

12.4 Interpretace článků a příloh směrnice MID s požadavky této příručky

MID			Softwarová příručka
Článek / Příloha č. (AI = Příloha 1)	**Označení**	**Komentář**	**Požadavek č.**
	Část článku		
1, 2, 3		Bez zvláštní souvislosti se softwarem	
4(b)	Definice, uspořádání podsestav	Přenos naměřených dat... Základní pravidla pro podsestavy	T P, U
5 to 9		Bez zvláštní souvislosti se softwarem	

MID			Softwarová příručka
Článek / Příloha č. (AI = Příloha 1)	**Označení**	**Komentář**	**Požadavek č.**
10	Technická dokumentace	Dokumentace týkající se návrhu, výroby a provozu. Umožnění hodnocení shody. Obecný popis přístroje. Popis elektronických zařízení s výkresy, logickými schématy, obecnými informacemi o softwaru. Umístění plomb a značek. Podmínky kompatibility s rozhraními a podsestavami.	P1, U1
11 to 27		Bez zvláštní souvislosti se softwarem	
	Příloha 1		
AI-1 to AI-5		Bez zvláštní souvislosti se softwarem	
AI-6	Spolehlivost	Detekce chyb, zálohování, obnovení, restart	I1-1, I1-2, I2-1, I2-2, I3-1, I3-2, I4-1, I4-2, I6-1, I6-2
AI-7	Vhodnost	Žádné prostředky usnadňující podvodné použití; minimální možnosti nezáměrného zneužití.	P3 – P8, U3 - U8, L1 – L5, L7, L8, T1 – T8, S2, D3, D4, I1-4, I2-8, I3-5, I4-4
AI-8	Ochrana proti zneužití		
AI-8.1		Žádné vlivy v důsledku připojení jiných zařízení.	P4, U4
AI-8.2		Zabezpečení, důkazy intervence	P6, P7, U6, U7, D1, D4
AI-8.3		Označení softwaru, důkazy intervence	P2, P6, P7, P8 U2, U6, U7, U8, D2, D4
AI-8.4		Ochrana uložených nebo přenášených dat	P5 - P7, U5 - U7, L1 - L5, T1 - T8 D1 - D3
AI-8.5		Nevynulování kumulativních záznamníků	I1-3, I2-4, I3-4, I4-3
AI-9	Informace o přístroji, které přístroj provázejí		
AI-9.1		Kapacita měření (zbývající položky nerelevantní z hlediska softwaru)	L8
AI-9.2		Bez zvláštní souvislosti se softwarem	
AI-9.3		Návod na instalaci, ..., podmínky kompatibility s rozhraním, podsestavami nebo měřicími přístroji.	P1, U1
AI-9.4 to AI-9.8		Bez zvláštní souvislosti se softwarem	
AI-10	Indikace výsledku		
AI-10.1		Označení na displeji nebo na výtisku.	P8, U8, L6, S2
AI-10.2		Význam výsledku, nezaměnitelnost s dalšími označeními.	P8, U8, L1, L4, L6, S2
AI-10.3		Tištěný výstup nebo záznam snadno čitelný a nesmazatelný.	P8, U8, L6, S2

MID			Softwarová příručka
Článek / Příloha č. (AI = Příloha 1)	**Označení**	**Komentář**	**Požadavek č.**
AI-10.4		Pro přímé prodeje: prezentace výsledku oběma stranám.	P8, U8, S2
AI-10.5		Pro měřiče spotřeby: zobrazení pro zákazníka	I1-3, I2-3, I3-3/4, I4-3
AI-11	Další zpracování dat za účelem ukončení obchodní transakce		
AI-11.1		Zaznamenání naměřených výsledků trvalými prostředky.	L1 - L8
AI-11.2		Trvanlivý důkaz naměřených výsledků a informací za účelem identifikace transakce.	L1, L6
AI-12	Hodnocení shody	Okamžité hodnocení shody s požadavky směrnice.	P1, P2, U1, U2, D2, D4
	Přílohy A1 až H1		
A1 až H1		Žádné požadavky na vlastnosti přístrojů	
	Příloha MI-001		
MI-001-1 až MI-001-6		Bez zvláštní souvislosti se softwarem	
MI-001-7.1.1, MI-001-7.1.2	Ochrana před elektromagnetickým rušením	Detekce chyb Prostředky zálohování Prostředky buzení z režimu spánku a obnovy	I1-1, I1-2
MI-001-7.1.3 až MI-001-9		Bez zvláštní souvislosti se softwarem	
	Příloha MI-002		
MI-002-1 až MI-002-2		Bez zvláštní souvislosti se softwarem	
MI-002-3.1	Ochrana před elektromagnetickým rušením	Detekce chyb Prostředky zálohování Prostředky buzení z režimu spánku a obnovy	I2-1, I2-2
MI-002-3.1.3 až MI-002-5.1		Bez zvláštní souvislosti se softwarem	
MI-002-5.2	Vhodnost	Přijatelné řešení sledování životnosti zdroje napájení	I2-5
MI-002-5.3	Vhodnost	Vnitřní rozlišení	I2-3
MI-002-5.4 až MI-002-8		Bez zvláštní souvislosti se softwarem	
MI-002-5.5	Vhodnost	Testovací prvek	I2-7
MI-002-5.6 až MI-002-8		Bez zvláštní souvislosti se softwarem	
MI-002-9.1	Přepočítávače objemu Vhodnost	Přijatelné řešení sledování přepočítávače objemu plynu	I2-6
MI-002-9.2 až MI-002-10		Bez zvláštní souvislosti se softwarem	
	Příloha MI-003		
MI-003-1 až MI-003-4.2		Bez zvláštní souvislosti se softwarem	

MID			Softwarová příručka
Článek / Příloha č. (AI = Příloha 1)	**Označení**	**Komentář**	**Požadavek č.**
MI-003-4.3	Povolené působení přechodných elektromagnetických jevů	Detekce chyb Prostředky zálohování Prostředky buzení z režimu spánku a obnovy	I3-1, I3-2
MI-003-5.1		Bez zvláštní souvislosti se softwarem	
MI-003-5.2	Vhodnost	Vnitřní rozlišení	I3-3
MI-003-5.3 až MI-003-7		Bez zvláštní souvislosti se softwarem	
	Příloha MI-004		
MI-004-1 až MI-004-4.1		Bez zvláštní souvislosti se softwarem	
MI-004-4.2	Povolený vliv elektromagnetického rušení	Detekce chyb Prostředky zálohování Prostředky buzení z režimu spánku a obnovy	I4-1, I4-2
MI-004-4.3 až MI-004-7		Bez zvláštní souvislosti se softwarem	
	Příloha MI-005		
	Příloha MI-006		
MI-006-IV, MI-006-V	Diskontinuální a kontinuální součtové váhy	Detekce chyb Prostředky zálohování	I6-1, I6-2
	Příloha MI-007		
MI-007-8	Povolený vliv elektromagnetického rušení	Prostředky zálohování	I7-1
	Příloha MI-008		
	Příloha MI-009		
	Příloha MI-010		

13 Odkazy a literatura

[1] Software Requirements and Validation Guide, Version 1.00, 29 October 2004, European Growth Network "*MID-Software",* contract number G7RT-CT-2001-05064, 2004

[2] DIRECTIVE 2014/32/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (recast), Official Journal of the European Union L 96/149, 29.3.2014

[3] Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments. Official Journal of the European Union L 135/1, 30.4.2004

[4] Internet Security Glossary, http://www.ietf.org/rfc/rfc2828.txt

[5] ISO/IEC JTC1/SC7 3941, 2008-03-14, http://pef.czu.cz/~papik/doc/MHJS/pdf/IT-VOCABULARY.pdf

14 Přehled revizí

Vydání	Datum	Významné změny
1	květen 2005	První vydání příručky
2	duben 2007	Doplnění a propracování termínů v části 2 Redakční změny v oddílech 4.1 a 5.1 Úprava a vysvětlení otázky označování softwaru v oddílu 4.2 (požadavek P2), a v oddílu 5.2 (požadavek U2). Úprava požadavku L8, upřesňující poznámka 1. Přidáno vysvětlení k požadavku S1, upřesňující poznámka 1. Nahrazení požadavku D5 poznámkou. Změna třídy rizika u systémů pro měření objemu kapalin kromě vody. Změna tříd rizika u vážicích přístrojů. Několik menších redakčních změn v dokumentu. Přidání Přehledu revizí.
3	březen 2008	Přidání výjimek u uvádění označení softwaru: nové požadavky I1-5, I2-9, I3-6, I4-5, a I5-1.
4	květen 2009	Omezení rozsahu použití stahování softwaru, upřesnění požadavků na označování v souvislosti se stahováním softwaru. Revize požadavků P2 a U2: Vymazání neplatných částí textu.
5	květen 2011	Revize kapitoly 5 (část U): Pokrok v oblasti operačních systémů Náhrada termínu „komponenta" jinými vhodnými termíny v celé příručce, aby nedošlo k chybnému pochopení

		Doplnění požadavku D1 v oddílu 9.2 zavedením zaplombovatelného mechanismu stahování Propracování části „upřesnění“ u požadavků P2 a U2 v oddílech 4.2 a 5.2 v souvislosti s označováním softwaru Rozšíření příkladů přijatelných řešení v požadavku L2 (oddíl 6.2) a v požadavku U8 (oddíl 5.2)
6	březen 2015	Rozsáhlá revize - Ráz příručky: Příručka je považována za čistě technický dokument interpretující základní požadavky související se softwarem. Výroky, které nejsou v souladu s tímto principem, byly odstraněny. - Adresáti příručky: Tato příručka je určena vývojářům a zkoušejícím softwaru, ale mohou ji využít i jiné strany, především orgány dohledu nad trhem, kdykoliv a kdekoliv to bude vhodné. - Zavedení posledních dvou aktualizací se ukázalo být náročné z hlediska detailní redakční práce. Změny provedené v rámci této revize proto mají za cíl lepší čitelnost příručky, nemění však uvedené technické specifikace. - Označení softwaru (P2/U2): Ve verzi 7.2 příručky již není požadováno, aby samotný software poskytoval i označení softwaru. Stačí, aby označení softwaru dokázal bezpečným způsobem sdělit přístroj. - Rozlišení označení a integrity (P2/U2, P6/U6): Příloha 1 směrnice MID rozlišuje mezi označením softwaru (příloha 1, článek 7.6) a integritou, tj. ochranou softwaru (příloha 1, článek 8.4). Toto rozlišení neoslabuje platnost požadavků. - Podpora kontrol shody s typem: Technické prostředky potřebné k zajištění integrity softwaru jsou považovány rovněž za vhodné při kontrole shody s typem. Požadované prostředky zahrnují např. kontrolní součty nebo ekvivalentní prostředky na různých úrovních u všech přístrojů náležejících do třídy rizika C a vyšší. - Třídy rizika: Třída rizika C byla změněna, a veškerý legálně relevantní software přístrojů náležejících do třídy rizika C je proto nyní považován za fixní (neměnný). Tím pádem odpadají nejasnosti ohledně toho, jaká část softwaru je považována za fixní. V třídě rizika C a vyšší musí být implementováno označení softwaru na úrovni bitů (např. kontrolními součty). - Klasifikace přístrojů využívajících univerzální počítač (přístroje typu U) dle třídy rizika: Přístroje využívající univerzální počítač jsou v zásadě spojeny s vyšším rizikem, a proto je zařazení těchto přístrojů do třídy B považováno za neodpovídající. Přístroje typu U lze tedy zařadit jedině do třídy rizika C či vyšší. - Přijatelná bezpečnostní opatření pro třídy vysokého rizika (D a vyšší): Požadavky na algoritmy a minimální délku klíče se řídí doporučeními vydanými národními a me-

		zinárodními institucemi pro bezpečnost dat (např. NIST (USA), DCSSI (Francie), CESG (Velká Británie), CCN (Španělsko), NCSC (Nizozemí), BSI (Německo)). - Legálně relevantní software: již není vnímána nutnost rozlišovat legálně relevantní software od fixního legálně relevantního softwaru. Všechny požadavky na zabezpečení uvedené v Příloze 1 se vztahují na legálně relevantní software.
7	březen 2018	Rozšíření P7 o přijatelné řešení, které zajišťuje, že obsah záznamníku událostí je zobrazen na displeji měřidla. Rozšíření U8 a doplnění odpovídajícího požadavku P8 popisující spárování a proces „handshake“ („potřesení rukou“) mezi jednotkami ve všeobecnějším smyslu. Zlepšení srozumitelnosti rozšíření S odstraněním definice pro oddělení softwaru na nízké a vysoké úrovni.
8	duben 2019	Změny editačního charakteru vzniklé porovnáním překladů a údržbou, objasnění aplikace rozšíření T, opravy v P6, U6, T6 a L2. V každém požadavku reorganizace mezi „Přijatelným řešením“ a „Upřesněním“. Byla kompletně zrevidována specifická příloha 10.2 Plynoměry a přepočítávače množství plynu a příloha 10.3 Elektroměry pro měření činné energie. Upravena kapitola 11.1 „Informace náležející do certifikátu“.

Tabulka 14-1: Přehled revizí