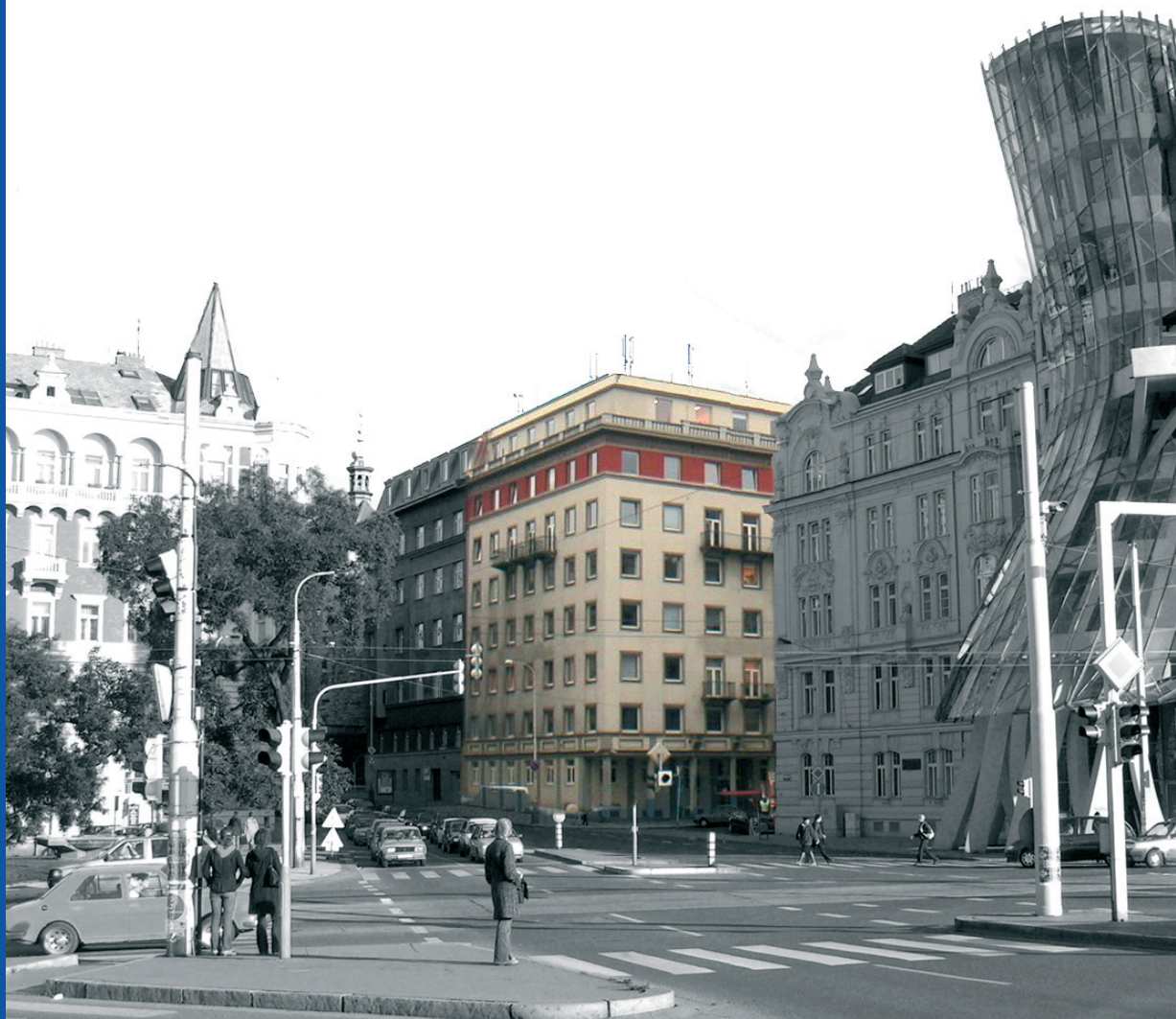


WELMEC GUIDE 7.2
(první vydání – překlad)



Vážení čtenáři a kolegové,

od r. 1996 vydával Úřad pro technickou normalizaci, metrologii a státní zkušebnictví edici nazvanou „K vnitřnímu trhu Evropské unie“. Většina svazků se těšila zcela mimořádné pozornosti a zájmu.

Cílem vydávání této edice bylo přiblížit technické veřejnosti principy a procedury technické legislativy, zaváděné v souladu s harmonizačními procesy v Evropské unii (EU) i v České republice. I když dnes existují daleko širší zdroje informací, než tomu bylo před několika lety, považujeme za potřebné v této iniciativě pokračovat, neboť jsme přesvědčeni, že napomáhá pochopení právní úpravy v oblastech působnosti ÚNMZ a jejímu správnému uplatňování. Navíc existuje řada dokumentů, které nejsou součástí práva, ale jsou důležité pro praxi. I v mnoha státech EU je technická regulace a harmonizace doprovázena ze strany státních orgánů širokou informační kampaní.

Proto je od roku 2004 vydávána inovovaná edice, přizpůsobená svým zaměřením aktuálnímu vývoji, podmínkám a potřebám. Byl zaveden nový název edice, který zní „Sborníky technické harmonizace ÚNMZ“, nová grafická podoba, i forma distribuce. Edice je k dispozici na stránkách ÚNMZ (www.unmz.cz) a v omezeném počtu nebo na vyžádání je též využívána forma CD-ROM. Je volně dostupná při respektování autorských práv.

Uplynulé dva roky, kdy v této edici bylo vydáno deset Sborníků, zatím prokázaly pokračující zájem odborné veřejnosti a redakční rada má i řadu námětů do blízké budoucnosti.

Věřím, že jak orgány státu, tak soukromá sféra resp. všichni účastníci procesu technické harmonizace a regulace budou v této edici i nadále nacházet užitečný zdroj informací a pomocníka v jejich práci.

Vaše podněty vedoucí k dalšímu zkvalitnění této činnosti ÚNMZ s povděkem uvítáme.


Ing. Alexander Šafařík-Pštrosz,
předseda ÚNMZ

Praha, 2006

OBSAH SBORNÍKU

1	ÚVODNÍ KOMENTÁŘ.....	4
2	WELMEC GUIDE 7.2.....	10

METROLOGICKÉ POŽADAVKY NA ZKOUŠENÍ SOFTWARE

Úvod

Stále se zdokonalující a množící se mikroelektronické komponenty v měřicí technice přinášejí do jisté míry přesun funkčnosti měřících zařízení z hardwarové do softwarové oblasti. Protože technologie výroby mechanických a elektrických komponent nejrozličnějších senzorů je v současné době na velmi vysoké úrovni, dochází často k situacím, kdy jsou funkčnost a metrologické vlastnosti přístrojů dány především jejich programovým vybavením. Nejvýraznější je tento trend u měřících systémů založených na využití volně programovatelných osobních počítačů.

Moderní programové vybavení měřicí techniky si žádá vývoj nových zkušebních metod, které by mohly být použity k testování metrologických vlastností softwaru. Při testování softwaru je třeba brát ohled na některá specifika, kterými se liší od běžných měřících zařízení.

- a) **složitost softwaru** – běžné programy mohou vykonávat větší množství rozdílných operací než čistě hardwarová zařízení. Z toho vyplývá nebezpečí vzájemného ovlivňování více programů nebo různých částí jednoho programu. I relativně krátké programy (ve smyslu délky zdrojového kódu) mohou být velmi složité.
- b) **změny** – na rozdíl od fyzického zařízení je software často – a velmi jednoduše – vylepšován pomocí bezpečnostních záplat, nových funkcí a modulů. Takové změny se mohou promítnout do ostatních částí programu. Stejně tak změny operačního systému mohou ovlivnit program, neboť ten využívá volání systémových funkcí.
- c) **chyby** – chyby softwaru nastávají většinou nečekaně, bez možnosti včas detekovat blížící se selhání. Způsob, jakým se software vyrovná s chybou, závisí jen na zodpovědnosti výrobce a kvalitě návrhu a implementace softwaru a operačního systému.
- d) **standardizace** – vývoj softwaru většinou nepodléhá žádným standardům, použité nástroje závisí na výrobcu a je těžké (a zpětně nemožné) je ovlivnit. Úroveň dokumentace také závisí jen na výrobcu, resp. na požadavcích zákazníka.

Testování softwaru – **validaci** – provádíme většinou pro účely typového schválení daného měřicího přístroje, pro splnění požadavků na akreditaci laboratoře či pro splnění požadavků kladených z hlediska managementu jakosti dané organizace.

V tomto dokumentu jsou popsány základní koncepty zkoušení softwaru v rámci směrnice Measurement Instruments Directive (MID) a souvisejícího dokumentu WELMEC 7.2.

Požadavky na software v legální metrologii–dokumenty WELMEC WG7

České předpisy pro požadavky na software v přístrojích používaných v oblasti legální metrologie jsou významně ovlivněny členstvím ČR ve sdružení WELMEC (Western European Legal Metrology Cooperation), které se zabývá sjednocováním metrologických předpisů používaných v legální metrologii.

Jak v rámci typového schvalování na základě směrnice MID (Measurement Instruments Directive), tak v rámci vývoje jiných předpisů je vycházeno především z dokumentu Welmec Software Guide, který je v tomto sborníku prezentován ve své české i anglické verzi.

Dokument WELMEC 7.2 popisuje jednotlivé požadavky na validaci softwaru s tím, že zavádí různé třídy rizika (risk classes) a k nim odpovídající požadavky. Je definováno celkem šest tříd rizika (A–F), přičemž naprostá většina přístrojů je zařazena do tříd B–D. Toto zařazení je výsledkem práce technických komisí WELMEC, které se zabývají jednotlivými měřicími přístroji. Třídy rizika i požadavky kladené na software závisí zejména na tom, zda se jedná o samostatný jednoúčelový přístroj (typ P instrument), nebo o přístroj využívající osobní počítač (typ U instrument). Pro přístroje typu U jsou požadavky obecně vyšší, neboť jsou vystaveny většímu nebezpečí ze strany uživatele.

Každý zkoušený přístroj musí být jednoznačně zařazen do některé z uvedených tříd rizika, aby bylo možné na něj aplikovat požadavky vyplývající z kapitol 5–10. Každá třída rizika odpovídá různým úrovním ochrany, zkoušení a shody, přičemž každý z těchto faktorů může mít tři stupně: nízký, střední a vysoký.

Požadavky na software v legální metrologii uvedené v dokumentu WELMEC 7.2 je přitom možné přeneseně aplikovat (po volbě vhodné třídy rizika) i na další software.

V souvislosti s přehledem požadavků na software je v tomto sborníku prezentován také informativní dokument WELMEC 7.1, který lze po revizích považovat za předchůdce dokumentu WELMEC 7.2. V tomto dokumentu jsou blíže rozvedeny některé koncepty tříd rizika a slouží zároveň jako reference pro zajištění kontinuity se staršími předpisy na validaci softwaru (které právě z dokumentu WELMEC 7.1 často vycházely).

Metody zkoušení softwaru

Vlastní testování závisí na charakteru softwaru a na cíli validace. Pokud provádíme validaci softwaru v legální metrologii, zaměřujeme se zejména na některé parametry zabezpečení programu a dat a na shodu funkčnosti s dokumentací, v souladu s doporučeními Welmec 7.2. V dokumentu samotném je podrobný návod, podle kterého je možné postupovat, z pohledu validace v oboru legální metrologie je tedy dostatečně zajištěna jednotnost přístupu při kontrole softwaru.

Praktické metody validace softwaru můžeme rozdělit do dvou skupin – na analýzu statickou a dynamickou. K těmto metodám souvisejícím s funkčností softwaru se v rámci přístupu dokumentu WELMEC 7.2 připojuje metoda třetí – kontrola dokumentace dodané výrobcem.

Jak vyplývá z požadavků dokumentu WELMEC 7.2, pro nižší třídy rizika ve většině případů aplikujeme pouze kontrolu dokumentace spojenou s dynamickou analýzou. Důraz je však kladen na kontrolu dokumentace, zahrnující kromě dokumentace uživatelské také deklarace výrobce speciálně vydané pro účely validace. Při přechodu do vyšších tříd rizika stoupá důraz na dynamickou analýzu a u nejvyšších tříd i statickou analýzu spolu se zvyšujícími se nároky na software.

V praxi jsou jednotlivé metody zkoušení softwaru prováděny například následujícím způsobem:

Statická analýza: cílem je kontrola kódu se zřetelem na jeho správnost a přehlednost. Je také kontrolován tok dat v programu a jsou hledány případné chyby v zacházení s daty a s pamětí. Postupujeme následujícím způsobem:

1. zběžná kontrola kódu, ověření jeho úplnosti, pokud je to možné, jeho překlad s přidáním informací pro debugger a kontrolou všech varování kompilátoru. Je vhodné použít kompilátor, který je použit v praxi (pokud nejde o software distribuovaný ve formě zdrojových souborů, který může být přeložen libovolným kompilátorem),
2. kontrola přehlednosti zdrojového kódu a jeho vhodného dělení do funkcí a modulů,
3. vyhledání toku dat v programu a kontrola jeho oddělení od ostatních částí programu (zejména se týká metrologických aplikací). Kontrola všech větví a cyklů souvisejících s tokem dat a kontrola zabezpečení dat (zejména při validaci zabezpečení). Můžeme definovat následující metriky pokrytí (např. 100% pokrytí větví pak znamená, že všechny větve byly kontrolovány a při dynamické analýze pak spuštěny):
 - pokrytí příkazů – všechny příkazy (ve zdrojovém kódu) jsou testovány a spuštěny,
 - pokrytí větví – všechny větve programu (ve zdrojovém kódu) jsou testovány a spuštěny,
 - pokrytí podmínek – všechny podmínky (např. ve větvení programu, při kontrole dat atd.) jsou testovány a spuštěny,
 - pokrytí cyklů – všechny cykly jsou spuštěny jednou, dvakrát a mnohokrát, je také kontrolováno, zda program pracuje dobře, pokud neproběhnou vůbec,
 - pokrytí cest – jsou kontrolovány všechny možné cesty programu (zahrnuje všechny větve, podmínky a jejich kombinace),
4. kontrola modularity programu (oddělení funkcí zabývajících se různými formami zpracování dat do samostatných modulů); kontrola, zda moduly vzájemně interagují jen očekávaným způsobem,
5. kontrola modulů – oddělení samostatných částí kódu zabývajících se zpracováním dat a statistické simulování vstupů a výstupů pro tyto části programu,
6. kontrola ošetření výjimek a nestandardních situací v programu,
7. testování vhodnosti – zahrnuje především testy určené uživatelem (z hlediska jeho požadavků), testy rychlosti, využití zdrojů, implementace zálohování, zaznamenání dat a podobných funkcí, které souvisí s uživatelským rozhraním. Testujeme, zda jsou funkce implementovány podle požadavků uživatele,

8. kontrola zabezpečení – sleduje se tok dat v programu, implementaci jednotlivých algoritmů zabezpečení (digitální podpisy, šifrování, kontrolní součty, správa uživatelů a jejich hesel atd.). Kontrolujeme, nakolik je program schopen sám detekovat nežádoucí změny a vytvářet svou identifikaci, zda je možné jej spustit s pozměněnými daty či knihovny.

Pro účely statické analýzy je vhodné použít softwarové nástroje pro sledování toku dat v programu, debuggery a programy kontrolující práci s pamětí.

Dynamická analýza: cílem je ověřit funkčnost a stabilitu programu a jeho shodu s dokumentací (případně dokumentaci nepopsaných či špatně popsanych částí na místě vytvořit). Test musí být přednostně proveden přímo v prostředí, ve kterém bude program používán, případně v simulovaném podobném prostředí (operační systém, hardware). Postupujeme následujícím způsobem:

1. identifikace binární verze programu, např. pomocí cyklického součtu a zálohování kopie programu jako reference aktuální validované verze,
2. předvedení typického užití programu zákazníkem s důrazem na běžně prováděné operace. V případě, že jde o program, který je určen k další distribuci, je testována také instalace programu a jeho inicializace,
3. kontrola všech větví a cyklů programu (pokud je to z technického hlediska možné) alespoň jedním průchodem,
4. oddělené vyhodnocení co možná nejširší množiny vstupů a kontrola výstupů. V ideálním případě (nezávislost na hardwaru) statistické testování velkým množstvím náhodě generovaných dat,
5. vyvolání kritických situací (chybějící hardware, špatná vstupní data) a kontrola výstupů, kontrola, zda program zaznamenává kritické situace a zda je možné vzniklé záznamy modifikovat,
6. kontrola dokumentace programu a její shody se skutečným stavem.

Kontrola dokumentace

Dokumentací výrobce dodanou pro účely validace rozumíme většinou uživatelské manuály, specifikace měřicího přístroje a sadu deklarácí a výčtů funkcí měřidla zhotovenou podle požadavků v příslušné třídě rizika (např. kompletní výčet všech příkazů komunikačního rozhraní měřidla a deklaraci úplnosti tohoto výčtu). Součástí dokumentace mohou být také popisy algoritmů (pro některé třídy rizika je postačující kontrola popisu algoritmů, bez statické či dynamické analýzy).

Konkrétní průběh validace závisí na typu softwaru, který je zkoušen, dostupnosti jeho zdrojových kódů a na účelu, pro který se validace provádí. Výstupem validace je tzv. *protokol o validaci*, ve kterém jsou popsány jednotlivé provedené testy a jejich výsledky. Nejedná se tedy jen o stanovisko vyhověl–nevyhověl, ale o celkový popis zkoušek, které byly na konkrétním programovém vybavení provedeny. Podle doporučení Welmec 7.2 je forma tohoto protokolu pevně dána specifikací jeho nezbytných součástí.

Závěr

Validace softwaru je soubor úkonů, které by měly zajistit správnou a bezpečnou funkcionalitu programového vybavení používaného v oblasti metrologie. Pro účely schvalování měřidel podle směrnice Measurement Instruments Directive (MID) je v tomto sborníku uveden dokument WELMEC 7.2, který kompletně popisuje požadavky na vývoj a zkoušení softwaru v měřicích přístrojích pokrytých touto směrnicí.

WELMEC GUIDE 7.2

Pokyn týkající se software

Požadavky na software související se směrnicí MID 2004/22/EC

(první vydání – překlad)

WELMEC je kooperace mezi autoritami na poli legální metrologie ze zemí Evropské unie a sdružení EFTA. Tento dokument je jedním z návodů, jejichž cílem je vytvořit vodítko pro výrobce a notifikované osoby pracující na poli zajištění shody. Tyto návody jsou čistě doporučujícího charakteru a samy o sobě nepřinášejí žádné další požadavky, které by byly nad rámec direktiv Evropské komise. Problémy popisované v těchto dokumentech mohou mít alternativní přijatelná řešení a zde uvedená řešení je třeba brát jen jako dobré příklady vyhovující daným požadavkům.

Přeloženo z anglického originálu:

WELMEC 7.2 Issue 1

Software Guide (Measuring Instruments Directive 2004/22/EC),
May 2005

Vydaného:

WELMEC Secretariat, BEV,

Arltgassee 35, A-1160 Vídeň, Rakousko

Tel: +43 1 21176 3608, Fax: +43 1 49 20 875

E-mail: welmec@metrologie.at

Web: www.welmec.org

Přeložil: Mgr. Petr Klapetek, Ph.D.

Vydal Úřad pro technickou normalizaci, metrologii a státní zkušebnictví se souhlasem WELMEC a při zachování všech práv WELMEC. Originál dokumentu v anglickém jazyce je umístěn na výše uvedených webových stránkách WELMEC.

OBSAH WELMEC GUIDE 7.2

	PŘEDMLUVA.....	15
1	ÚVOD.....	16
2	TERMINOLOGIE.....	17
3	JAK S TÍMTO DOKUMENTEM PRACOVAT.....	21
3.1	Obecná struktura dokumentu.....	21
3.2	Jak vybrat odpovídající části dokumentu.....	23
3.3	Jak pracovat se skupinami požadavků.....	24
3.4	Jak pracovat s kontrolními seznamy.....	25
4	ZÁKLADNÍ POŽADAVKY PRO SOFTWARE V JEDNOÚČELOVÝCH MĚŘICÍCH PŘÍSTROJÍCH (TYP P).....	26
4.1	Technický popis.....	26
4.2	Specifické požadavky pro přístroje typu P.....	27
5	ZÁKLADNÍ POŽADAVKY PRO SOFTWARE V MĚŘICÍCH PŘÍSTROJÍCH VYUŽÍVAJÍCÍCH POČÍTAČ (TYP U).....	38
5.1	Technický popis.....	38
5.2	Specifické požadavky pro přístroje typu U.....	39
6	ROZŠÍŘENÍ L: DLOUHODOBÉ UKLÁDÁNÍ MĚŘENÝCH DAT.....	54
6.1	Technický popis	54
6.2	Dodatečné požadavky	55
7	ROZŠÍŘENÍ T: PŘENOS DAT PO KOMUNIKAČNÍCH SÍTÍCH.....	66
7.1	Technický popis	66
7.2	Dodatečné požadavky	67
8	ROZŠÍŘENÍ S: ODDĚLENÍ SOFTWARE.....	77
8.1	Technický popis	77
8.2	Dodatečné požadavky	78
9	ROZŠÍŘENÍ D: STAHOVÁNÍ SOFTWARE.....	83
9.1	Technický popis	83
9.2	Dodatečné požadavky	83
10	ROZŠÍŘENÍ I: POŽADAVKY NA KONKRÉTNÍ TYPY PŘÍSTROJŮ.....	91
10.x.1	Specifické normy, standardy a jiné normativní dokumenty.....	91

10.1	Vodoměry.....	94
10.1.1	Specifické normy, standardy a jiné normativní dokumenty.....	94
10.1.2	Technický popis	94
10.1.3	Požadavky na software.....	95
10.1.4	Příklady softwaru a dat relevantních z pohledu legální metrologie.....	97
10.1.5	Další aspekty.....	98
10.1.6	Přiřazení tříd rizika.....	98
10.2	Plynoměry a přepočítávače.....	98
10.2.1	Specifické normy, standardy a jiné normativní dokumenty.....	98
10.2.2	Technický popis	98
10.2.3	Požadavky na software.....	99
10.2.4	Příklady softwaru a dat relevantních z pohledu legální metrologie.....	103
10.2.5	Další aspekty.....	104
10.2.6	Přiřazení tříd rizika.....	104
10.3	Elektroměry pro měření činné energie.....	104
10.3.1	Specifické normy, standardy a jiné normativní dokumenty.....	104
10.3.2	Technický popis	105
10.3.3	Požadavky na software.....	106
10.3.4	Příklady softwaru a dat relevantních z pohledu legální metrologie.....	108
10.3.5	Další aspekty.....	109
10.3.6	Přiřazení tříd rizika.....	109
10.4	Měřiče tepla.....	109
10.4.1	Specifické normy, standardy a jiné normativní dokumenty.....	109
10.4.2	Technický popis	110
10.4.3	Požadavky na software.....	111
10.4.4	Příklady softwaru a dat relevantních z pohledu legální metrologie.....	113
10.4.5	Další aspekty.....	113
10.4.6	Přiřazení tříd rizika.....	114
10.5	Měřicí systémy na kapaliny jiné než voda.....	114

10.5.6	Přiřazení tříd rizika.....	114
10.6	Vážicí zařízení.....	115
10.6.1	Specifické normy, standardy a jiné normativní dokumenty.....	115
10.6.2	Technický popis.....	116
10.6.3	Požadavky na software.....	116
10.6.4	Příklady softwaru a dat relevantních z pohledu egální metrologie.....	118
10.6.5	Další aspekty.....	119
10.6.6	Přiřazení tříd rizika.....	119
10.7	Taxametry.....	120
10.7.1	Specifické normy, standardy a jiné normativní dokumenty.....	120
10.7.2	Technický popis.....	120
10.7.3	Požadavky na software.....	120
10.7.4	Příklady softwaru a dat relevantních z pohledu legální metrologie.....	122
10.7.5	Další aspekty.....	122
10.7.6	Přiřazení tříd rizika.....	122
10.8	Ztělesněné míry.....	122
10.9	Měřidla rozměrů.....	123
10.9.6	Přiřazení tříd rizika.....	123
10.10	Analyzátory plynu.....	123
10.10.6	Přiřazení tříd rizika.....	123
11	DEFINICE TŘÍD RIZIKA.....	124
11.1	Obecný princip.....	124
11.2	Popis úrovní ochrany, zkoušení a shody.....	124
11.3	Rozdělení tříd rizika.....	125
11.4	Interpretace tříd rizika.....	125
12	VZOR PROTOKOLU O VALIDACI.....	127
12.1	Protokol o validaci.....	127
12.2	Příloha 1 protokolu o validaci: Kontrolní seznamy pro výběr typu požadavků.....	131
12.3	Příloha 2 protokolu o validaci: Kontrolní seznamy pro konkrétní technické požadavky.....	132
12.4	Informace, které by měly být součástí certifikátu schválení typu.....	138

13	KŘÍŽOVÉ REFERENCE.....	139
13.1	Vztah tohoto dokumentu ke článkům směrnice MID.....	139
13.2	Vztah článků směrnice MID k tomuto dokumentu.....	143
14	LITERATURA.....	146

PŘEDMLUVA

Tento dokument vychází z dokumentu „Software Requirements and Validation Guide“, verze 1.00 z 29. září 2004, vypracovaného v rámci projektu „European Growth Network MID Software“, který se s podporou Evropské komise uskutečnil pod registračním číslem G7RT-CT-2001-05064 v období od ledna 2002 do prosince 2004.

Návod má pouze charakter doporučení a neobsahuje žádná nařízení nebo technické požadavky, které by přesahovaly požadavky směrnice MID. Pro účely činností popisovaných v tomto návodu je možné využít alternativní postupy; níže popisované metody jsou doporučeny sdružením WELMEC.

Přestože je dokument zaměřen na měřicí přístroje regulované směrnicí MID, popisované postupy mají obecný ráz a mohou být použity i v jiných oblastech.

1 ÚVOD

Tento dokument by měl být vodítkem pro osoby zabývající se aplikací směrnice MID, zejména pak měřicími přístroji vybavenými softwarem. Dotýká se tedy jak výrobců měřicích přístrojů, tak notifikovaných osob, které jsou zodpovědné za posuzování shody v oboru měřicích přístrojů.

Dodržením tohoto postupu jsou splněny požadavky na software v měřicích přístrojích obsažené ve směrnici MID. Předpokládá se proto, že notifikované osoby budou používat tento návod jako výklad směrnice MID v otázkách týkajících se softwaru. Jako příklad provázanosti požadavků tohoto dokumentu a požadavků směrnice MID jsou v kapitole 13 uvedeny křížové reference.

Tento návod vychází z verze 7.1, vypracované skupinou WELMEC WG 7. I tento dokument byl zpracován na základě stejných principů a v současné revidované verzi (2. vydání) slouží jako informativní dokument. Pro účely vývoje, zkoušení a validace softwaru v měřicích přístrojích doporučuje sdružení WELMEC použít práci, kterou právě čtete.

Nejnovější informace související s prací skupiny WELMEC WG 7 a jí vypracovávanými návody je možné najít na adrese:

<http://www.welmecwg7.ptb.de/>

2 TERMINOLOGIE

Následující odstavec obsahuje výčet termínů použitých v tomto návodu. Reference na odkazy, z nichž použité pojmy a definice pocházejí, jsou uvedeny pouze v případě, že jsou z nich jednotlivé definice převzaty v úplné nebo téměř úplné podobě.

přijatelné řešení: návrh nebo princip softwarového nebo hardwarového modulu, které jsou v souladu s konkrétními požadavky. Přijatelné řešení je jedním z možných řešení problému v souladu s danými požadavky a nevylučuje v praxi použít jiné řešení, které by bylo rovněž v souladu s těmito požadavky.

kontrolní čítač: softwarový čítač nebo jiný záznamový zapisovač událostí souvisejících se změnami softwaru nebo jeho parametrů relevantních z pohledu legální metrologie.

autentizace: kontrola deklarované identity uživatele, procesu nebo zařízení.

základní konfigurace: návrh *měřicího přístroje* s ohledem na jeho základní architekturu. Rozlišujeme dvě základní konfigurace – *jednouúčelový měřicí přístroj* a *měřicí přístroj využívající počítače*. Obdobně je tento pojem možné použít pro dílčí části přístroje.

jednouúčelový měřicí přístroj (typ P): *měřicí přístroj* navržený a konstruovaný pro jeden konkrétní účel. Software v takovém zařízení je určen jen pro funkce související s tímto účelem. Více informací je uvedeno v kapitole 4.1.

uzavřená síť: síť s pevným počtem účastníků s neměnnými identitami, funkcí a rozmístěním (viz též heslo *Otevřená síť*).

komunikační rozhraní: elektronické, optické nebo jiné technické rozhraní, které umožňuje předávání dat mezi *přístroji* nebo *jejich dílčími částmi*.

specifické parametry přístroje: *legálně relevantní parametry*, jejichž hodnoty závisí na konkrétním použitém přístroji. Jejich součástí jsou kalibrační parametry (např. nastavení rozsahu nebo korekční součinitele) nebo konfigurace (např. maximální či minimální hodnoty, jednotky měřené veličiny). Mohou být nastavovány jen ve zvláštním pracovním režimu přístroje. Tyto pa-

rametry mohou být rozděleny na neměnné a nastavitelné (mohou být nastaveny k tomu pověřenou osobou).

integrovaná paměť: paměť, která je nedílnou součástí měřicího přístroje, např. RAM, EEPROM, pevný disk.

neporušenost dat a softwaru: fakt, že data ani software nebyly v průběhu používání, přenosu či uložení na paměťovém médiu neoprávněně měněny.

konfigurace IT: návrh *měřicího přístroje* z pohledu IT funkcí a schopností, které nesouvisí s měřicími schopnostmi měřidla. V tomto návodu se jedná o čtyři následující funkce: *dlouhodobé uchování měřených dat, přenos dat, stahování softwaru a oddělení částí softwaru* (viz též heslo *Základní konfigurace*). Stejně funkce můžeme kontrolovat i u *dílčích částí měřidla*.

legálně relevantní parametry: parametry *měřicího přístroje* nebo jeho *dílčí části*, které jsou předmětem kontroly z pohledu legální metrologie. Dělí se na dva typy: *specifické parametry přístroje a parametry specifické pro typ přístroje*.

legálně relevantní software: programy, data a parametry *specifické pro daný typ přístroje*. Jsou součástí *měřicího přístroje* nebo jeho *dílčí části* a souvisí s činností, která je předmětem kontroly z pohledu legální metrologie.

dlouhodobé uchování měřených dat: uchování dat po skončení měření za účelem jejich pozdějšího využití v legální metrologii (např. po skončení obchodní transakce).

měřicí přístroj: jakýkoliv přístroj obsahující funkce pro měření. Pokud není možná záměna, v tomto dokumentu slovo „měřicí“ vypouštíme (viz MID, článek 4).

měřicí přístroj využívající počítače (typ U): *měřicí systém*, který využívá víceúčelového počítače, nejčastěji osobního počítače pro funkce, které jsou předmětem kontroly z pohledu legální metrologie. Za tento typ měřicího zařízení považujeme všechny přístroje, které nesplňují požadavky na *jednoúčelové měřicí přístroje*.

otevřená síť: síť s libovolným počtem účastníků. Počet, identita, umístění a funkce účastníků se může dynamicky měnit a nemusí být jednotlivým účastníkům známa (viz též *uzavřená síť*).

třída rizika: skupina typů *měřících přístrojů* se srovnatelným rizikem.

stahování softwaru: proces automatického přenosu softwaru do cílového měřicího přístroje nebo jeho části z jakéhokoliv zdrojového umístění s využitím libovolných technických prostředků (vyměnitelná média, přenosný počítač, vzdálený server) a jakýchkoliv spojení (přímé propojení, síť).

identifikace softwaru: sekvence znaků jednoznačně spjatá s identitou softwaru (např. číslo verze nebo kontrolní součet).

oddělení softwaru: jednoznačné rozdělení softwaru na jeho *legálně relevantní* a legálně nerelevantní část. Pokud takové rozdělení není provedeno, celý software je považován za *legálně relevantní software*.

samostatná část měřidla: část měřidla, která funguje nezávisle na dalších částech a spolu s nimi tvoří měřicí přístroj.

přenos měřených dat: přenos dat do jiného zařízení s využitím komunikačních sítí nebo jiných prostředků za účelem jejich dalších zpracování nebo využití v oblasti legální metrologie.

parametry specifické pro typ přístroje: legálně relevantní parametry měřicího přístroje, které jsou závislé jen na jeho typu a jsou dané jeho typovým schválením. Jsou součástí legálně relevantního softwaru.

uživatelské rozhraní: rozhraní umožňující předat data mezi uživatelem a přístrojem nebo softwarové či hardwarové komponenty takového zařízení (např. přepínač, klávesnice, myš, displej, monitor, tiskárna aj.).

validace: potvrzení, že jsou splněny dané požadavky s ohledem na zamýšlené použití přístroje, v tomto případě požadavky směrnice MID. Toto potvrzení se zakládá na objektivně ověřitelných skutečnostech (na základě měření nebo pozorování).

Následující definice souvisí s některými specifickými požadavky na přístroje zařazené do třídy rizika D a vyšších.

hash algoritmus: algoritmus, který ztrátově komprimuje obsah bloku dat do čísla dané délky takovým způsobem, že změna jakéhokoli bitu v bloku dat vede k jinému výsledku (hash kódu). Pro výpočet hash kódu jsou zvoleny algoritmy, u nichž je co možná nejmenší pravděpodobnost, že by pro dva různé bloky dat byl výsledkem výpočtu stejný hash kód.

algoritmus podpisu: kryptografický algoritmus, který šifruje prostý text s použitím daného *klíče podpisu* a umožňuje zpětné dekódování šifrovaných dat s použitím *dekódovacího klíče*.

klíč: sekvence znaků používaná při zašifrování a dešifrování dat. Existují dvě třídy šifer: symetrické a nesymetrické. Při použití symetrického šifrování jsou data zakódována i dekódována stejným klíčem, při použití nesymetrického šifrování jsou použity dva různé (spolu související) klíče. V druhém případě je na zakódování dat použit soukromý klíč odesilatele a na jejich dekódování příjemcem je použit veřejně známý klíč odesilatele.

systém veřejného klíče: dvojice *klíčů*, z nichž jeden je soukromý a druhý veřejný. Aby bylo možné posoudit *autenticitu* a *neporušenost* dat, je jejich hash kód (vytvořený *hash algoritmem*) zašifrován soukromým klíčem odesilatele a následně je dešifrován příjemcem s využitím veřejného klíče odesilatele.

infrastruktura systému veřejného klíče: systém (infrastruktura) zajišťující důvěryhodnost veřejných klíčů. S touto infrastrukturou souvisí zejména vytváření a distribuce příslušných klíčů všem účastníkům komunikace.

certifikace klíčů: proces přiřazení veřejného klíče dané organizaci, osobě či jinému subjektu.

elektronický podpis: krátký blok dat přiřazený k přenášeným či uloženým datům za účelem zajištění jejich *autenticity* a *neporušenosti*. Je vytvořen algoritmem podpisu a s využitím soukromého klíče. Vytvoření takového podpisu obvykle probíhá v následujících krocích: 1. *hash algoritmus* zkomprimuje data, která se mají podepsat, 2. *algoritmus podpisu* zkombinuje výsledný hash kód se soukromým klíčem, který k podpisu používáme.

trust centre: organizace zabývající se generováním, distribuováním a uchováváním veřejných klíčů osob, organizací či jiných subjektů a objektů včetně měřicích přístrojů.

3 JAK S TÍMTO DOKUMENTEM PRACOVAT

Tento oddíl popisuje strukturu dokumentu a vysvětluje, jak má být dokument používán.

3.1 Obecná struktura dokumentu

Dokument je uspořádán jako strukturovaná sbírka skupin požadavků. Obecná struktura dokumentu je členěna podle základních konfigurací měřicích přístrojů a podle tzv. konfigurací IT. Nakonec jsou uvedeny také požadavky týkající se jednotlivých typů přístrojů.

V důsledku toho jsou uvedeny tři typy požadavků:

1. požadavky na měřicí přístroje ve dvou základních konfiguracích – typ P a U
2. požadavky na čtyři IT konfigurace (tzv. rozšíření L, T, S a D)
3. požadavky na jednotlivé typy přístrojů (rozšíření I.1, I.2 atd.),

přičemž první typ požadavků se týká všech přístrojů. Druhý typ požadavků souvisí s následujícími funkcemi softwaru: dlouhodobé uchování dat (L), přenos dat (T), stahování softwaru (D) a oddělení softwaru (S). Každý z těchto požadavků je platný pouze pro přístroje, které jsou danou funkcí vybaveny. Posledním typem požadavků je souhrn požadavků na jednotlivé typy přístrojů, které jsou v přílohách číslovaných obdobně, jako jsou jednotlivé měřicí přístroje číslovány ve směrnici MID. Následující blokové schéma znázorňuje celý postup aplikování požadavků na konkrétní typ přístroje:

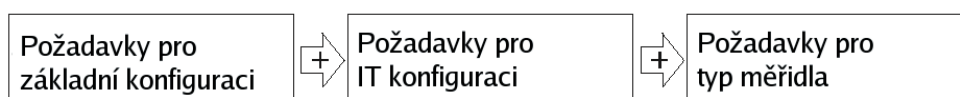
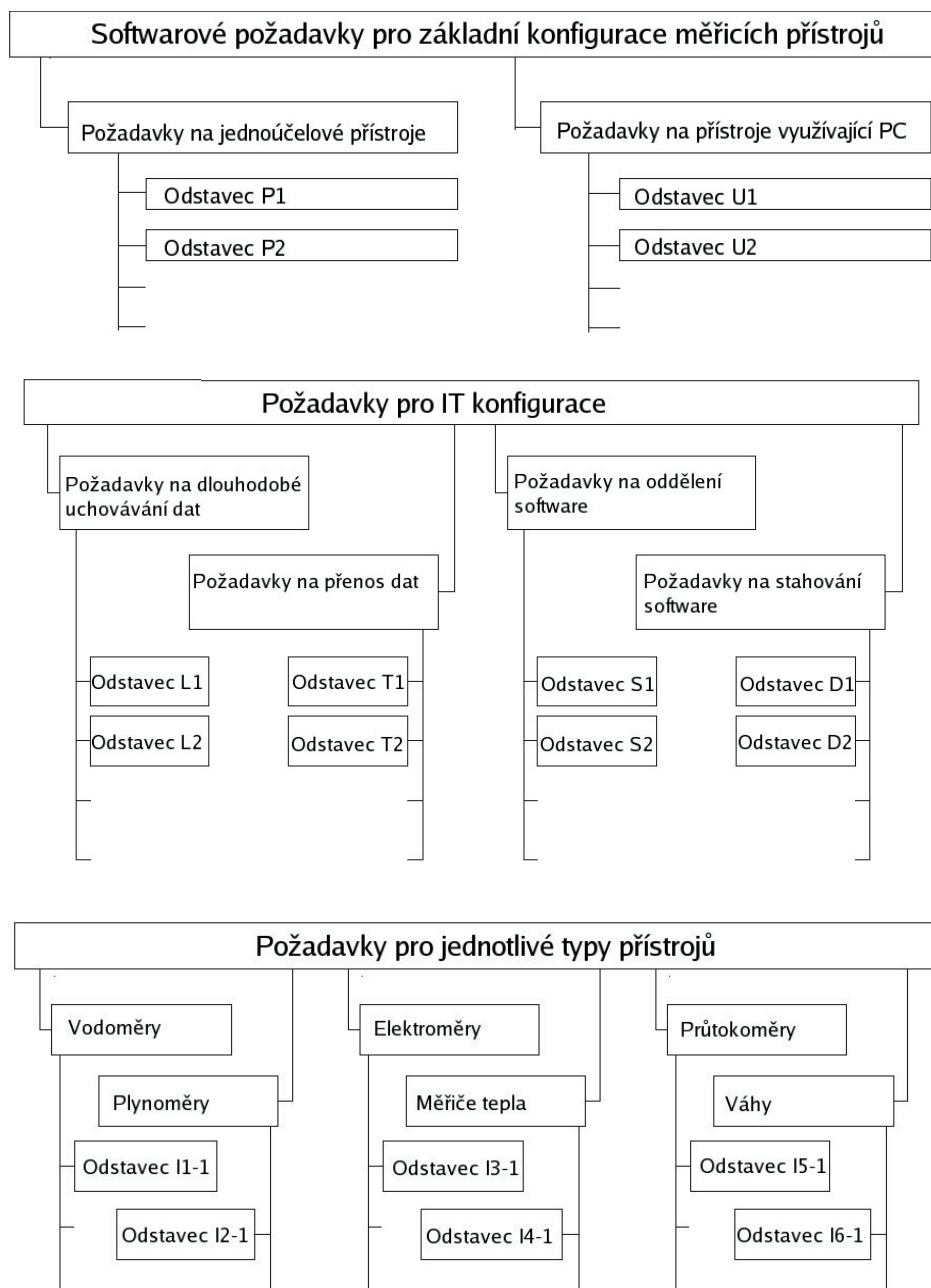


Schéma členění skupin požadavků je uvedeno na následujícím obrázku 3.2.



Obrázek 3.2: Přehled skupin požadavků

Kromě výše popsané struktury jsou jednotlivé skupiny požadavků členěny podle tříd rizika. Pro tyto účely je zavedeno šest tříd rizika A–F s postupně vzrůstajícími požadavky, přičemž nejnižší a nejvyšší třída (A a F) se v současnosti netýkají žádných přístrojů a jsou rezervovány pro budoucí potřeby. Zbývající čtyři třídy (B–E) zahrnují všechny druhy měřicích přístrojů, které pokrývá směrnice MID. Třídy rizika jsou definovány v kapitole 11 tohoto dokumentu.

Každý přístroj je tedy nejprve zařazen do své třídy rizika a z této třídy vyplývají požadavky na něj kladené.

3.2 Jak vybrat odpovídající části dokumentu

Dokument zahrnuje velké množství možných přístrojů a jejich konfigurací. Modulární formou je možné sestavit soubor požadavků na každý měřicí přístroj následujícími kroky:

Krok 1: výběr základní konfigurace (P nebo U)

Ze dvou možných základních konfigurací vždy aplikujeme jen požadavky na tu konkrétní konfiguraci, která odpovídá zkoušenému přístroji. Rozhodněte proto, zda se jedná o jednoúčelový měřicí přístroj s vestavěným softwarem (typ P, kapitola 4.1) nebo o přístroj používající počítač (typ U, kapitola 5.1). Pokud neposuzujeme celý přístroj, ale jen některou jeho součást, rozhodujeme podle základní konfigurace této součásti. Po volbě základní konfigurace aplikujeme všechny požadavky pro tuto konfiguraci.

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

IT konfigurace zahrnují tyto funkce: dlouhodobé uchování dat (L), přenos dat (T), stahování softwaru (D) a oddělení softwaru (S). Jednotlivé požadavky uvedené pro tyto IT konfigurace jsou na sobě nezávislé, je tedy možné je jakkoli kombinovat podle toho, jakými funkcemi je přístroj vybaven. Pokud je daná IT konfigurace zvolena, musí přístroj splnit veškeré požadavky na ni kladené. Zvolíme proto příslušné IT konfigurace a aplikujeme požadavky.

Krok 3: Výběr požadavků pro konkrétní typ přístroje (rozšíření I)

Podle daného druhu přístroje vybereme příslušnou třídu požadavků, vycházíme ze členění přístrojů podle směrnice MID.

Krok 4: Výběr třídy rizika (rozšíření I)

Třídy rizika pro jednotlivé typy přístrojů jsou dány v rozšířeních I, pro každý konkrétní typ přístroje v podkapitole I.x.6. Podle jednotlivých oborů mohou být třídy rizika buď shodné pro celou třídu měřicích přístrojů, nebo mohou být dále rozděleny do kategorií. Vybereme příslušnou třídu rizika a ve všech použitých skupinách požadavků (krok 1–4) aplikujeme jen požadavky na ni kladené.

3.3 Jak pracovat se skupinami požadavků

Každá skupina požadavků obsahuje dobře definovaný požadavek. Skládá se z definujícího textu, vysvětlujících poznámek, popisu dokumentace, která je k provedení kontroly nezbytná, a příkladů přijatelných řešení problému. Obsah skupiny požadavků může být (a většinou je) členěn podle tříd rizika. To vede k následujícímu schématu skupiny požadavků:

Název požadavku		
Popis požadavku (případně dělený podle tříd rizika)		
Specifikace požadavku (vysvětlující poznámky, případně dělené podle tříd rizika)		
Potřebná dokumentace (případně rozdělená podle tříd rizika)		
Validace (třída rizika B)	Validace (třída rizika C)	...
Přijatelné řešení (třída rizika B)	Přijatelné řešení (třída rizika C)	...

Obrázek 3.3: Struktura skupiny požadavků

Skupina požadavků zahrnuje jasný technický popis požadavku a také návod na validaci s ohledem na daný požadavek. Je proto adresována jak notifikovaným osobám, tak výrobcům s důrazem

na to, že by 1. výrobci měli považovat obsah požadavku za technické minimum při návrhu a konstrukci přístrojů a 2. notifikované osoby by neměly požadovat testy a funkcionalitu nad rámec popsaného požadavku.

Poznámky k výrobcům:

- prostudujte záměr požadavku a technickou specifikaci
- poskytněte potřebnou dokumentaci
- přijatelná řešení jsou jen příklady, jak splnit požadavek, můžete postupovat jiným způsobem
- návod k validaci má jen informativní charakter.

Poznámky k notifikovaným osobám

- prostudujte záměr požadavku a technickou specifikaci
- postupujte podle návodu k validaci
- zkontrolujte, zda je dokumentace kompletní.

3.4 Jak pracovat s kontrolními seznamy

Kontrolní seznamy jsou prostředkem ke kontrole splnění všech požadavků a jsou součástí protokolu o validaci. Nenahrazují skupiny požadavků, jsou jen pomůckou při validaci. Jsou koncipovány pro všechny třídy rizika dohromady.

Postup:

- použijte kontrolní seznamy podle příslušných parametrů přístroje
- zkontrolujte požadavky popsané v kontrolních seznamech (detailně popsané ve skupinách požadavků)
- vyplňte kontrolní seznamy.

4 ZÁKLADNÍ POŽADAVKY PRO SOFTWARE V JEDNOÚČELOVÝCH MĚŘICÍCH PŘÍSTROJÍCH (TYP P)

Skupina požadavků uvedená v této kapitole se týká jednoúčelových měřicích přístrojů nebo jednoúčelových samostatných částí měřidel. V případě, že měřicí přístroj využívá počítač (typ U), je třeba aplikovat požadavky z následující kapitoly. Tyto požadavky je navíc potřeba aplikovat ve všech případech, kdy nejsou splněna kritéria na zařazení do třídy jednoúčelových měřicích přístrojů podle následujícího odstavce.

4.1 Technický popis

Přístroj typu P je jednoúčelový měřicí přístroj s vestavěným procesorem, který může být charakterizován následujícími vlastnostmi:

- veškerý software je určen k měření a jeho obsluze, zahrnující v to funkce související s kontrolou z pohledu legální metrologie,
- software je považován za jeden celek, s výjimkou oddělených částí vyhovujících podmínkám kapitoly S,
- uživatelské rozhraní je určeno pro měření, při běžném užívání je tedy přístroj v pracovním režimu podléhající kontrolě z pohledu legální metrologie,
- operační systém použitý v přístroji (pokud je přístroj nějakým vybaven) nemá možnost uživatelského spouštění programů nebo zadávání příkazů,
- software ani jeho prostředí není možné měnit, a přístroj ani není vybaven programovacími nástroji, které by toto umožňovaly. Stažení programu do přístroje je možné, jen pokud to vyhovuje podmínkám kapitoly D,
- přístroj může být vybaven komunikačními nástroji pro přenos dat po otevřené nebo uzavřené síti podle kapitoly T,
- přístroj může být vybaven prostředky pro dlouhodobé ukládání dat podle kapitoly L.

4.2 Specifické požadavky na přístroje typu P

Třída rizika B–E

P1: Dokumentace

Kromě specifických částí dokumentace, které budou popsány v některých z následujících odstavců, je nezbytné, aby dokumentace k softwaru obsahovala následující části:

- a. *Popis softwaru relevantního z pohledu legální metrologie.*
- b. *Popis přesnosti výpočetních algoritmů (například výpočet ceny nebo její zaokrouhlování).*
- c. *Popis uživatelského rozhraní, nabídek a dialogů.*
- d. *Jednoznačnou identifikaci softwaru.*
- e. *Popis potřebného hardware, např. blokový diagram, popis počítače, sítě, na kterou je přístroj připojen, apod., pokud tyto údaje nejsou uvedeny v manuálu k programu.*
- f. *Manuál k programu.*

Třída rizika B	Třída rizika C	Třída rizika D
<p>P2: Identifikace softwaru <i>Software relevantní z pohledu legální metrologie musí být jednoznačně identifikovatelný. Identifikace softwaru musí být obsažena v softwaru samotném, musí být tedy mimo jiné možné získat ji v průběhu používání softwaru k tomu vyhrazeným příkazem.</i></p>		
<p>Specifikace: 1. Při změnách softwaru relevantního z pohledu legální metrologie je nezbytné informovat notifikovanou osobu. Notifikovaná osoba rozhodne, zda je nezbytné provést novou identifikaci softwaru nebo ne, přičemž nová identifikace je vyžadována jen tehdy, když se změny týkají funkcí podstatných pro metrologickou funkci softwaru, například funkcí schválených při typovém schválení daného měřidla.</p>	<p>Specifikace: Dodatek k 1B: každá změna softwaru, který je při schválení typu označen za neměnný, musí být doplněna novou identifikací.</p>	
<p>2. Identifikace musí zřetelně rozlišovat části, které souvisí se schválením typu a které s ním nesouvisí (pokud takové rozdělení existuje). 3. Jestliže může software pracovat ve více režimech, mezi kterými lze přepínat, může být identifikace provedena buď pro každý tento režim, nebo pro software jako celek.</p>		
<p>Potřebná dokumentace: V dokumentaci musí být popsána identifikace softwaru, metoda, jakou je tato identifikace generována, jakým způsobem je provázána se softwarem samotným a jak může být zjištěna. Pokud je software rozlišen na části, které podléhají kontrole z pohledu legální metrologie a které jí nepodléhají, musí být jejich rozlišení popsáno.</p>		<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jak je identifikace ochráněna proti jejím neoprávněným změnám.</p>
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Zkoumáme popis generování a vizualizace identifikace softwaru. • Kontrolujeme, zda je zřejmé, jak jsou identifikovány části relevantní z pohledu legální metrologie, a zda je zřejmé, které funkce softwaru jsou předmětem kontroly a které ne. • Kontrolujeme, zda výrobce uvedl nominální hodnotu identifikace. Tato hodnota musí být zmíněna v protokolu o validaci. 		<p>Validace: Dodatek k požadavkům pro třídy B a C: Kontrolujeme, zda je identifikace chráněna proti neoprávněným změnám.</p>

<p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda zobrazení identifikace je ve shodě s dokumentací. • Kontrolujeme, zda identifikace odpovídá nominální hodnotě. <p>Je-li to možné, jsou dokumentace a spustitelný soubor, který byl testován, archivovány notifikovanou osobou.</p>	
<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> • Identifikace softwaru se skládá ze dvou částí. Část A musí být změněna, pokud dojde ke změně, která vyžaduje nové schválení, část B označuje jen malé změny, například opravy chyb, které nové schválení nevyžadují. • Identifikace je generována a zobrazena na požádání přímo softwarem. 	
<p>Část A identifikace se skládá z čísla verze nebo z čísla schválení typu.</p>	<p>Část A identifikace je tvořena automaticky generovaným kontrolním součtem prováděným na softwaru relevantním z pohledu legální metrologie (v rozsahu stanoveném při schválení typu). Pro ostatní části softwaru je identifikace tvořena číslem verze nebo číslem schválení typu.</p> <p>Přijatelným řešením pro generování kontrolního součtu je algoritmus CRC-16.</p>
<p>Dodatek ke třídě rizika E</p>	
<p>Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód související s generováním identifikace</p>	
<p>Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda identifikace pokrývá všechny části, které jsou relevantní z pohledu legální metrologie. • Kontrolujeme, zda je algoritmus výpočtu identifikace správný. 	

Třída rizika B	Třída rizika C	Třída rizika D
<p>P3: Ovlivnění uživatelským rozhraním <i>Příkazy zadávané prostřednictvím uživatelského rozhraní nesmí narušit správnost měření a měřených dat.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> Příkazy mohou být zadávány jednotlivými stisknutími kláves nebo jejich sekvencemi. Je tedy možné, že ne všem kombinacím kláves jsou jednoznačně přiřazeny určité příkazy. Kombinace kláves, které nejsou uvedeny v dokumentaci, nesmí mít žádný vliv na chod přístroje. 		
<p>Potřebná dokumentace: Pokud má přístroj rozhraní, které umožňuje zadávat příkazy, dokumentace musí zahrnovat:</p> <ul style="list-style-type: none"> úplný seznam příkazů spolu s deklarácí jeho úplnosti, krátký popis jednotlivých příkazů a jejich vliv na měření a měřená data. 	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C:</p> <ul style="list-style-type: none"> Dokumentace musí popisovat prostředky, kterými je možno zkontrolovat úplnost seznamu příkazů. Dokumentace musí obsahovat protokol, který potvrzuje testování funkčnosti všech příkazů. 	
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme vliv jednotlivých příkazů na měření a měřená data. Kontrolujeme, zda dokumentace zahrnuje deklaraci úplnosti seznamu příkazů. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> Zkoušíme dokumentované a nedokumentované sekvence znaků a jejich vliv na chod měřidla. Procházíme všechny nabídky, má-li software nějaké. 	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Testujeme prostředky, kterými lze zkontrolovat úplnost seznamu příkazů. 	
<p>Přijatelné řešení: Součástí programu je modul uživatelského rozhraní, který je předmětem kontroly z pohledu legální metrologie. Tento modul přijímá všechny vstupy od uživatele a filtruje z nich příkazy, které nejsou definované. Žádná nedokumentovaná sekvence kláves tedy nemůže mít vliv na funkci ostatních částí softwaru.</p>		
<p>Dodatek ke třídě rizika E</p>		
<p>Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód</p>		

Validace (dodatek k požadavkům pro třídy B a C):

Kontrola zdrojového kódu:

- Kontrolujeme datový tok související s přijímáním příkazů z uživatelského rozhraní, zejména z pohledu jeho jednoznačnosti.
- Kontrolujeme ochranu před záměrným tokem dat, která by nebyla součástí schváleného uživatelského rozhraní.
- Kontrolujeme, zda neexistují nedokumentované příkazy.

Třída rizika B	Třída rizika C	Třída rizika D
<p>P4: Ovlivnění komunikačním rozhraním <i>Příkazy zadávané prostřednictvím komunikačního rozhraní nesmí narušit správnost měření a měřených dat.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> 1. Příkazy musí být jednoznačně přiřazeny funkcím či operacím s daty. 2. Příkazy mohou být tvořeny jednotlivými signály (elektrickými, optickými apod.) nebo jejich sekvencemi. 3. Sekvence signálů nebo kódů, které nejsou uvedeny v dokumentaci, nesmí mít žádný vliv na chod přístroje. 4. Požadavky zde uvedené se netýkají stahování dat podle rozšíření D. 5. Požadavky zde uvedené se týkají rozhraní, která nejsou označena úřední značkou. 		
<p>Potřebná dokumentace: Pokud má přístroj komunikační rozhraní, které umožňuje zadávat příkazy, dokumentace musí zahrnovat:</p> <ul style="list-style-type: none"> • úplný seznam příkazů spolu s deklarací jeho úplnosti, • krátký popis jednotlivých příkazů a jejich vliv na měření a měřená data. 	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C:</p> <ul style="list-style-type: none"> • Dokumentace musí popisovat prostředky, kterými je možno zkontrolovat úplnost seznamu příkazů. • Dokumentace musí obsahovat protokol, který potvrzuje testování funkčnosti všech příkazů. 	
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme vliv jednotlivých příkazů na měření a měřená data. • Kontrolujeme, zda dokumentace zahrnuje deklaraci úplnosti seznamu příkazů. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Zkoušíme vybrané příkazy s využitím příslušných komunikačních prostředků. <p><i>Upozornění:</i> Pokud není možné zajistit rozhraní validací podle tohoto odstavce, musí být v protokolu o validaci uvedeno, že není chráněné, a musí být zabezpečeno například úřední značkou.</p>	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Testujeme prostředky, kterými je možno zkontrolovat úplnost seznamu příkazů. 	
<p>Přijatelné řešení: Součástí programu je modul komunikačního rozhraní, který je předmětem kontroly z pohledu legální metrologie. Tento modul přijímá všechny vstupy a filtruje z nich příkazy, které nejsou definované. Žádná nedokumentovaná sekvence kódů nebo signálů tedy nemůže mít vliv na funkci ostatních částí softwaru.</p>		

Dodatek ke třídě rizika E

Potřebná dokumentace (dodatek k požadavkům pro třídy B a C):
Zdrojový kód

Validace (dodatek k požadavkům pro třídy B a C):

Kontrola zdrojového kódu:

- Kontrolujeme datový tok související s přijímáním příkazů z komunikačního rozhraní, zejména z pohledu jeho jednoznačnosti.
- Kontrolujeme ochranu před záměrným tokem dat, která by nebyla součástí schváleného komunikačního rozhraní.
- Kontrolujeme, zda neexistují nedokumentované příkazy.

Třída rizika B	Třída rizika C	Třída rizika D
<p>P5: Ochrana proti náhodným (nechtěným) změnám <i>Software relevantní z pohledu legální metrologie musí být chráněn proti náhodným (nechtěným) změnám.</i></p>		
<p>Specifikace: Příčiny náhodných změn mohou být zejména v neočekávaných vlivech okolního prostředí, vlivu uživatelem definovaných funkcí nebo chybách softwaru. Zde uvedené požadavky se proto zaměřují na:</p> <ol style="list-style-type: none"> Fyzické vlivy: uložená data musí být chráněna proti náhodným změnám či smazání, pokud by nastala hardwarová chyba nebo musí být tato chyba detekovatelná. Uživatelské funkce: změna či smazání dat musí být uživatelem potvrzeny. Chyby v softwaru: data musí být vhodným způsobem chráněna před chybami, které by mohly vzniknout kvůli špatnému návrhu programu nebo chybám v něm. 		
<p>Potřebná dokumentace: V dokumentaci musí být popsány prostředky, kterými je software chráněn proti nechtěným změnám.</p>		
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda je kontrolní součet programu a dat počítán automaticky. Kontrolujeme, zda nemůže dojít k přepsání dat, která by měla být v přístroji zachována po určitou dobu danou výrobcem. Kontrolujeme, zda program varuje uživatele před smazáním dat. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> Pokud je možné mazat data, kontrolujeme, zda je před jejich smazáním uživatel varován. 		
<p><i>Přijatelné řešení:</i></p> <ul style="list-style-type: none"> Při spuštění programu je prováděn kontrolní součet relevantních částí; pokud nesouhlasí s nominální hodnotou, je program zastaven. Měřená data nemohou být smazána bez varování. Metody detekce chyb jsou popsány také v Rozšíření I. 		
<p>Dodatek ke třídě rizika E</p>		
<p>Potřebná dokumentace (dodatek k požadavkům pro třídy B, C a D): Zdrojový kód</p>		
<p>Validace (dodatek k požadavkům pro třídy B, C a D): <i>Kontrola zdrojového kódu:</i></p> <ul style="list-style-type: none"> Kontrolujeme vhodnost metod kontroly náhodných změn. Pokud je počítán kontrolní součet, kontrolujeme, zda pokrývá všechny části relevantní z pohledu legální metrologie. 		

Třída rizika B	Třída rizika C	Třída rizika D
<p>P6: Ochrana proti záměrným změnám <i>Software relevantní z pohledu legální metrologie musí být chráněn proti záměrným změnám a záměnám.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> Přístroj bez rozhraní: software by mohl být modifikován fyzickou manipulací s pamětí, ve které je uchovávan, například její záměnou. Přístroj musí být proto zabezpečen jako celek nebo musí být vhodnými prostředky chráněna alespoň paměť, ve které je software uložen. Přístroj s rozhraním: software nesmí obsahovat rozhraní, která by nebyla kontrolována při schválení. Pokud je možné provádět stahování softwaru, musí tak být činěno v souladu s rozšířením D tohoto dokumentu. Data považujeme za dostatečně chráněná pouze v případě, jestliže s nimi pracuje software, který je předmětem kontroly z pohledu legální metrologie. Pokud přístroj obsahuje i jiný software, musí být v souladu s rozšířením S tohoto dokumentu. 		
<p>Potřebná dokumentace: Dokumentace musí zahrnovat popis ochrany proti záměrným změnám softwaru.</p>		<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeny konkrétní prostředky ochrany proti záměrným změnám softwaru.</p>
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda jsou prostředky pro ochranu fyzické paměti proti její záměně dostačující. Pokud je paměť prepisovatelná bez nutnosti jejího vyjmutí z přístroje, kontrolujeme, zda je takový přepis vhodným způsobem znemožněn, např. pomocí metrologických značek. (Pro stahování softwaru viz kapitolu D.) <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda není možné přepsat obsah paměti v programovacím režimu. 		<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme prostředky ochrany proti záměrným změnám.
<p>Přijatelné řešení: Celý přístroj je zaplombován úředními značkami a všechna jeho rozhraní splňují požadavky odstavců P3 a P4.</p>		
<p>Dodatek ke třídě rizika E</p>		
<p>Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód</p>		
<p>Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i> Kontrolujeme vhodnost metod kontroly ochrany proti záměrným změnám.</p>		

Třída rizika B	Třída rizika C	Třída rizika D
<p>P7: Ochrana parametrů <i>Parametry související s funkcí přístroje v legální metrologii musí být chráněny proti neoprávněným změnám.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> 1. Parametry specifické pro daný typ přístroje jsou pro všechny přístroje téhož typu stejné a jsou součástí jeho softwaru. Platí pro ně proto požadavky P6. 2. Parametry specifické pro daný přístroj mohou být měněny, pouze však v případě, že jsou příslušným způsobem chráněny. 3. Nastavitelné parametry specifické pro daný přístroj mohou být měněny libovolně. 		
<p>Potřebná dokumentace: V dokumentaci musí být popsány všechny parametry relevantní z pohledu legální metrologie, jejich rozsahy a nominální hodnoty, spolu s popisem, kde jsou uchovávány, jak mohou být zobrazeny a jak jsou chráněny.</p>	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jak jsou parametry chráněny proti změnám.</p>	
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda není možné parametry nastavovat poté, co byly zabezpečeny proti změnám. • Kontrolujeme, zda jsou všechny parametry relevantní z pohledu legální metrologie (dané rozšířením I) označeny jako zabezpečené parametry. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Testujeme přístroj v režimu jeho nastavování a v provozním režimu, přičemž kontrolujeme, zda je zabezpečení dat funkční. • Kontrolujeme klasifikaci parametrů a jejich popis (nastavitelný/zabezpečený) v nabídce přístroje (má-li nějakou). 	<p>Validace: Dodatek k požadavkům pro třídy B a C: Kontrolujeme, zda a jak jsou parametry chráněny proti změnám.</p>	
<p>Přijatelné řešení:</p> <p>a) Parametry jsou nahrány do paměti, jejíž přepisování může být hardwarově znemožněno (a příslušné prostředky jsou zaplombovány).</p>		
<p>b) Změny parametrů jsou zaznamenány čítačem změn, jehož hodnota může být zobrazena a porovnána s hodnotou při posledním ověření uvedenou na těle přístroje.</p>		

<p>c) Změny parametrů jsou zaznamenány kontrolním zapisovačem, který automaticky ukládá do nepřepisovatelné paměti následující údaje:</p> <ul style="list-style-type: none">• identifikaci parametru (např. jeho jméno)• hodnotu parametru• datum a čas změny (timestamp) <p>Kontrolní zapisovač nemůže být přepsán nebo smazán bez porušení plomby.</p>	
Dodatek ke třídě rizika E	
Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód související s ochranou parametrů	
Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i> <ul style="list-style-type: none">• Kontrolujeme, zda je ochrana parametrů realizována vhodným způsobem.	

5 ZÁKLADNÍ POŽADAVKY PRO SOFTWARE V MĚŘICÍCH PŘÍSTROJÍCH VYUŽÍVAJÍCÍCH POČÍTAČ (TYP U)

5.1 Technický popis

Soubor požadavků uvedených v této kapitole je určen pro měřicí přístroj, který využívá víceúčelového počítače, nejčastěji osobního počítače. Technické požadavky jsou popsány v následující tabulce. Je nutné zdůraznit, že tyto požadavky je nezbytné aplikovat i ve všech ostatních případech, kdy měřicí přístroj nevyhovuje technickým požadavkům na jednoúčelové měřicí přístroje uvedené v kapitole 4.1.

<p>Hardwarová konfigurace</p> <p>a) Modulární systém založený na využití víceúčelového počítače. Počítač může být připojen k uzavřené nebo otevřené síti.</p> <p>b) Senzor, který vykonává měření, je přídatným zařízením k počítači a je k počítači nejčastěji připojen pomocí uzavřené sítě. V principu ovšem může být připojen také pomocí otevřené sítě.</p> <p>c) Uživatelské prostředí může být přepínáno mezi režimem, který je předmětem kontroly z pohledu legální metrologie, a jiným režimem.</p> <p>d) Ukládání dat může být lokální nebo vzdálené. Vzdálené úložiště dat může být umístěno kdekoli, v jiné místnosti, budově, zemi nebo na jiném kontinentě mimo Evropskou unii. Komunikace související s ukládáním dat může být přímá i nepřímá, může zahrnovat dočasné uložení dat mimo kontrolu uživatele. Média pro uložení dat mohou být pevná (např. pevný disk) nebo výměnná (např. diskety, CD-ROM aj.).</p>
<p>Softwarová konfigurace</p> <p>e) Počítač může být vybaven libovolným operačním systémem a libovolnými dalšími programy. Zatímco části softwaru, které jsou předmětem kontroly z pohledu legální metrologie, nemohou být po schválení typu neoprávněně měněny, ostatní části programu mohou být jakkoliv modifikovány.</p> <p>f) Operační systém a hardwarové drivery (ovladače grafické karty, tiskárny, pevných disků aj.) nejsou předmětem kontroly z pohledu legální metrologie, pokud nejsou přímo určeny k měření.</p>

Tabulka 5.1: technický popis přístroje typu U

5.2 Specifické požadavky pro přístroje typu U

Třída rizika B–E

U1: Dokumentace

Kromě specifických částí dokumentace, které budou popsány v některých z následujících odstavců, je nezbytné, aby dokumentace k softwaru obsahovala tyto části:

- a. Popis softwaru a dat relevantních z pohledu legální metrologie.*
- b. Popis přesnosti výpočetních algoritmů (například výpočet ceny nebo její zaokrouhlování).*
- c. Popis uživatelského rozhraní, nabídek a dialogů.*
- d. Jednoznačná identifikace softwaru relevantního z pohledu legální metrologie.*
- e. Popis potřebného hardware (např. blokový diagram, popis počítače, sítě, na kterou je přístroj připojen, apod.), pokud tyto údaje nejsou uvedeny v manuálu k programu.*
- f. Popis zabezpečení na úrovni operačního systému, tj. uživatelské účty a oprávnění, apod.*
- g. Manuál k programu.*

Třída rizika B	Třída rizika C	Třída rizika D
<p>U2: Identifikace softwaru <i>Software relevantní z pohledu legální metrologie musí být jednoznačně identifikovatelný. Identifikace softwaru musí být obsažena v softwaru samotném, musí být tedy mimo jiné možné získat ji v průběhu používání softwaru k tomu vyhrazeným příkazem.</i></p>		
<p>Specifikace: 1. Identifikace se netýká operačního systému a nízkourovňových ovladačů, jako jsou ovladače grafické karty nebo tiskárny. Týká se však ovladačů, které by přímo souvisely s metrologickou funkcí. 2. Při změnách softwaru relevantního z pohledu legální metrologie je nezbytné informovat notifikovanou osobu. Notifikovaná osoba rozhodne, zda je nezbytné provést novou identifikaci softwaru nebo ne, přičemž nová identifikace je vyžadována jen tehdy, když se změny týkají funkcí podstatných pro metrologickou funkci softwaru, například funkcí schválených při schválení typu daného měřidla.</p>	<p>Specifikace: 1. Omezení proti 1B: Při schválení typu musí být použité ovladače posouzeny z pohledu jejich souvislosti s funkcí softwaru v legální metrologii, a pokud s ní souvisí, musí být zahrnuty do identifikace. 2. Dodatek k 2B: Každá změna softwaru, který je při schválení typu označen za neměnný, musí být doplněna novou identifikací.</p>	
<p>3. Identifikace musí zřetelně rozlišovat části, které souvisí se schválením typu a které s ním nesouvisí (pokud takové rozdělení existuje). 4. Identifikovány mohou být různé úrovně programu, jako jsou moduly, samostatné funkce apod. 5. Jestliže může software pracovat ve více režimech, mezi kterými lze přepínat, může být identifikace provedena buď pro každý tento režim, nebo pro software jako celek.</p>		
<p>Potřebná dokumentace: V dokumentaci musí být popsána identifikace softwaru, metoda, jakou je tato identifikace generována, jakým způsobem je provázána se softwarem samotným a jak může být zjištěna. Pokud je software rozlišen na části, které podléhají kontrole z pohledu legální metrologie a které jí nepodléhají, musí být jejich rozlišení popsáno.</p>		<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jak je identifikace ochráněna proti jejím neoprávněným změnám.</p>

<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Zkoumáme popis generování a vizualizace identifikace softwaru. • Kontrolujeme, zda je zřejmé, jak jsou identifikovány části relevantní z pohledu legální metrologie a zda je zřejmé, které funkce softwaru jsou předmětem kontroly a které ne. • Kontrolujeme, zda výrobce uvedl nominální hodnotu identifikace. Tato hodnota musí být zmíněna v protokolu o validaci. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda je zobrazení identifikace ve shodě s dokumentací. • Kontrolujeme, zda identifikace odpovídá nominální hodnotě. <p>Je-li to možné, jsou dokumentace a spustitelný soubor, který byl testován, archivovány notifikovanou osobou.</p>	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda je identifikace chráněna proti neoprávněným změnám.
<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> • Identifikace softwaru se skládá ze dvou částí. Část A musí být změněna, pokud dojde ke změně, která vyžaduje nové schválení, část B označuje jen malé změny, například opravy chyb, které nové schválení nevyžadují. • Identifikace je generována a zobrazena na požádání přímo softwarem. 	
<ul style="list-style-type: none"> • Část A identifikace se skládá z čísla verze nebo z čísla schválení typu. 	<ul style="list-style-type: none"> • Část A identifikace je tvořena automaticky generovaným kontrolním součtem prováděným na softwaru relevantním z pohledu legální metrologie (v rozsahu stanoveném při schválení typu). Pro ostatní části softwaru je identifikace tvořena číslem verze nebo číslem schválení typu.
	<ul style="list-style-type: none"> • Přijatelným řešením generování kontrolního součtu je algoritmus CRC-16. • Přijatelným řešením generování kontrolního součtu je algoritmus CRC-32 nebo hash algoritmus, jako jsou SHA-1, MD5, RipeMD160 apod.
<p>Dodatek ke třídě rizika E</p>	
<p>Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód související s generováním identifikace</p>	
<p>Validace (dodatek k požadavkům pro třídy B a C): Kontrola zdrojového kódu:</p> <ul style="list-style-type: none"> • Kontrolujeme, zda identifikace pokrývá všechny části, které jsou relevantní z pohledu legální metrologie. • Kontrolujeme, zda je algoritmus výpočtu identifikace správný. 	

Třída rizika B	Třída rizika C	Třída rizika D
<p>U3: Ovlivnění uživatelským rozhraním <i>Příkazy zadávané prostřednictvím uživatelského rozhraní nesmí ovlivnit software, správnost měření a měřených dat.</i></p>		
<p>Specifikace: 1. Příkazy mohou být tvořeny jednotlivými příkazy nebo jejich sekvencemi. 2. Je tedy možné, že ne všem sekvencím příkazů jsou jednoznačně přiřazeny určité funkce softwaru. 3. Kombinace příkazů, které nejsou uvedeny v dokumentaci, nesmí mít žádný vliv na chod přístroje.</p>	<p>Specifikace: Dodatek k požadavkům pro třídy B a C: 4. Uživatel nesmí mít přístup k příkazovému řádku operačního systému, nesmí být tedy možné spouštět programy, psát je nebo spouštět příkazy operačního systému.</p>	
<p>Potřebná dokumentace: Pokud má přístroj rozhraní, které umožňuje zadávat příkazy, dokumentace musí zahrnovat:</p> <ul style="list-style-type: none"> • Úplný seznam příkazů spolu s deklarací jeho úplnosti. • Krátký popis jednotlivých příkazů a jejich vlivu na měření a měřená data. 	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C:</p> <ul style="list-style-type: none"> • Dokumentace musí popisovat prostředky, kterými je možno zkontrolovat úplnost seznamu příkazů. • Dokumentace musí obsahovat protokol, který potvrzuje testování funkčnosti všech příkazů. 	
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme vliv jednotlivých příkazů na měření a měřená data. • Kontrolujeme, zda dokumentace zahrnuje deklaraci úplnosti seznamu příkazů. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Zkoušíme dokumentované a nedokumentované sekvence příkazů a jejich vliv na chod softwaru. Procházíme všechny nabídky, má-li software nějaké. 	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Testujeme prostředky, kterými je možno zkontrolovat úplnost seznamu příkazů. 	
<p>Přijatelné řešení: Součástí programu je modul uživatelského rozhraní, který je předmětem kontroly z pohledu legální metrologie. Tento modul přijímá všechny vstupy od uživatele a filtruje z nich příkazy, které nejsou definované. Žádná nedokumentovaná sekvence příkazů tedy nemůže mít vliv na funkci ostatních částí softwaru.</p>	<p>Přijatelné řešení: Dodatek k požadavkům pro třídy B a C: Přístup k prostředkům operačního systému je blokován.</p>	

Dodatek ke třídě rizika E

Potřebná dokumentace (dodatek k požadavkům pro třídy B a C):
Zdrojový kód.

Validace (dodatek k požadavkům pro třídy B a C):

Kontrola zdrojového kódu:

- Kontrolujeme datový tok související s přijímáním příkazů z uživatelského rozhraní, zejména z pohledu jeho jednoznačnosti.
- Kontrolujeme ochranu před záměrným tokem dat, která by nebyla součástí schváleného uživatelského rozhraní.
- Kontrolujeme, zda neexistují nedokumentované příkazy.

Třída rizika B	Třída rizika C	Třída rizika D
<p>U4: Ovlivnění komunikačním rozhraním <i>Příkazy zadávané prostřednictvím komunikačního rozhraní nesmí narušit správnost měření a měřených dat.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> Příkazy musí být jednoznačně přiřazeny funkcím či operacím s daty. Příkazy mohou být tvořeny jednotlivými signály (elektrickými, optickými apod.) nebo jejich sekvencemi. Sekvence signálů nebo kódů, které nejsou uvedeny v dokumentaci, nesmí mít žádný vliv na chod přístroje. Požadavky zde uvedené se netýkají stahování dat podle rozšíření D. 		
<p>5. Části softwaru, které interpretují příkazy zadávané přes komunikační rozhraní, považujeme za relevantní z pohledu legální metrologie.</p> <p>6. Komunikační rozhraní mohou používat i další programy v počítači (které nejsou relevantní z pohledu legální metrologie), nesmí však narušit tok dat a příkazů programů, které jsou relevantní z pohledu legální metrologie.</p>	<p>5. Všechny části softwaru, které souvisí s obsluhou komunikačního rozhraní, považujeme za relevantní z pohledu legální metrologie.</p> <p>6. Komunikační rozhraní musí být vyhrazeno jen pro metrologickou funkci. Toto omezení se netýká standardních počítačových rozhraní, která vyhovují rozšíření T tohoto dokumentu.</p>	
<p>Potřebná dokumentace: Pokud má přístroj komunikační rozhraní, které umožňuje zadávat příkazy, dokumentace musí zahrnovat:</p> <ul style="list-style-type: none"> Úplný seznam příkazů spolu s deklarací jeho úplnosti. Krátký popis jednotlivých příkazů a jejich vlivu na měření a měřená data. 	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C:</p> <ul style="list-style-type: none"> Dokumentace musí popisovat prostředky, kterými je možno zkontrolovat úplnost seznamu příkazů. Dokumentace musí obsahovat protokol, který potvrzuje testování funkčnosti všech příkazů. 	
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme vliv jednotlivých příkazů na měření a měřená data. Kontrolujeme, zda dokumentace zahrnuje deklaraci úplnosti seznamu příkazů. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> Zkoušíme vybrané příkazy s využitím příslušných komunikačních prostředků. 	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Testujeme prostředky, kterými je možno zkontrolovat úplnost seznamu příkazů. 	
<p>Přijatelné řešení: Součástí programu je modul komunikačního rozhraní, který je předmětem kontroly z pohledu legální metrologie. Tento modul přijímá všechny vstupy a filtruje z nich příkazy, které nejsou definované. Žádná nedokumentovaná sekvence kódů nebo signálů tedy nemůže mít vliv na funkci ostatních částí softwaru.</p>		

Dodatek ke třídě rizika E

Potřebná dokumentace (dodatek k požadavkům pro třídy B a C):
Zdrojový kód.

Validace (dodatek k požadavkům pro třídy B a C):

Kontrola zdrojového kódu:

- Kontrolujeme datový tok související s přijímáním příkazů z komunikačního rozhraní, zejména z pohledu jeho jednoznačnosti.
- Kontrolujeme ochranu před záměrným tokem dat, která by nebyla součástí schváleného komunikačního rozhraní.
- Kontrolujeme, zda neexistují nedokumentované příkazy.

Třída rizika B	Třída rizika C	Třída rizika D
<p>U5: Ochrana proti náhodným (nechtěným) změnám <i>Software relevantní z pohledu legální metrologie musí být chráněn proti náhodným (nechtěným) změnám.</i></p>		
<p>Specifikace: Příčiny náhodných změn mohou být následující:</p> <ol style="list-style-type: none"> Chyby v návrhu a realizaci softwaru, nechtěné změny globálních parametrů ve funkcích atd. Nesprávné použití prostředků operačního systému. Nechtěné smazání dat v softwaru (viz též rozšíření L). Nesprávné přiřazení měřených dat souvisejících s různými měřeními kvůli špatně navrženému toku dat v programu. Fyzické vlivy: uložená data musí být chráněna proti náhodným změnám či smazání, pokud by nastala hardwarová chyba nebo musí být tato chyba detekovatelná. 		
<p>Potřebná dokumentace: V dokumentaci musí být popsány prostředky, kterými je software chráněn proti nechtěným změnám.</p>	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být popsány prostředky, kterými je testována ochrana softwaru proti nechtěným změnám.</p>	
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda je kontrolní součet programu a dat počítán automaticky. Kontrolujeme, zda nemůže dojít k přepsání dat, která by měla být v přístroji zachována po určitou dobu danou výrobcem. Kontrolujeme, zda program varuje uživatele před smazáním dat. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> Pokud je možné mazat data, kontrolujeme, zda je před jejich smazáním uživatel varován. 	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda prostředky ochrany programu a dat odpovídají vysokému stupni ochrany. 	
<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> Prevence při návrhu programu (mimo rámec tříd rizika) Jsou využity všechny prostředky ochrany softwaru a dat na úrovni operačního systému a programovacího jazyka k ochraně proti zneužití prostředků operačního systému, přepsání nebo smazání programů a dat. Při spuštění programu může být prováděn kontrolní součet relevantních částí (softwaru i parametrů); pokud nesouhlasí s nominální hodnotou, je vyvolána příslušná reakce. Pokud to operační systém dovoluje, neměli by mít uživatelé práva k mazání či modifikaci relevantních dat a softwaru a pro přístup k datům a softwaru by měli používat hesla nebo přístup jen pro čtení. Jiná práva by měl správce systému nastavit jen v nezbytně nutných případech. 		

Dodatek ke třídě rizika E

Potřebná dokumentace (dodatek k požadavkům pro třídy B a C):
Zdrojový kód.

Validace (dodatek k požadavkům pro třídy B a C):

Kontrola zdrojového kódu:

- Kontrolujeme vhodnost metod ochrany proti náhodným změnám.
- Pokud je počítán kontrolní součet, kontrolujeme, zda pokrývá všechny části relevantní z pohledu legální metrologie.

Třída rizika B	Třída rizika C	Třída rizika D
<p>U6: Ochrana proti záměrným změnám <i>Software relevantní z pohledu legální metrologie musí být chráněn proti záměrným změnám a záměnám.</i></p>		
<p>Specifikace: 1. Záměrné změny by mohly být provedeny: a. Změnou kódu programu včetně integrovaných dat – pro třídy rizika B a C je postačující, aby byl program ve formě binárního spustitelného souboru b. Změnou měřených dat – viz rozšíření L 2. Software nesmí být možné změnit pomocí prostředků operačního systému, například prostým spuštěním jiného, neschváleného programu (viz U3). Pokud je možné stahování softwaru, musí vyhovovat rozšíření D. 3. V nutných případech musí být učiněna opatření, která zabrání změně programu jednoduchými prostředky, jakou jsou textové editory.</p>		<p>Specifikace: 1. Ochrana softwaru musí být na stejné úrovni, jako u softwaru souvisejícího s elektronickými platbami. Obecně je měřicí systém použitelný v této konfiguraci jen tehdy, je-li počítač vybaven dalšími hardwarovými prostředky zabezpečení.</p>
<p>Potřebná dokumentace: Dokumentace musí zahrnovat opatření proti záměrným změnám softwaru.</p>		<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeny konkrétní prostředky ochrany proti záměrným změnám softwaru.</p>
<p>Validace: <i>Varianta 1: příkazový řádek není dostupný</i> <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda se moduly softwaru nahrávají automaticky. • Kontrolujeme, zda uživatel nemá přístup k prostředkům operačního systému. • Kontrolujeme, zda uživatel nemá přístup k jinému softwaru, než který byl schválen. • V dokumentaci musí být deklarováno, že v softwaru neexistují prostředky, jak se dostat k příkazovému řádku operačního systému. 		<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda jsou prostředky ochrany proti záměrným změnám vhodně zvoleny vzhledem k vysoké úrovni ochrany.

<p><i>Varianta 2: příkazový řádek je dostupný</i> <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Spustitelný program je ověřován kontrolním součtem, je-li tento změněn, program se nespustí. 	
<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> Program může být kontrolován automaticky generovaným kontrolním součtem, který je porovnáván se známou hodnotou. Pokud je takto hodnota změněna, funkce programu je zablokována. Za dostatečné řešení je považován jakýkoli algoritmus digitálního podpisu, který má klíč dlouhý alespoň 2 byty, například CRC 16 s inicializačním vektorem, který není znám a je skryt přímo ve spustitelném souboru. Program může být chráněn prostředky operačního systému; v takovém případě musí být zaplombován vstup do administrátorského režimu. 	<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> Software a data relevantní z pohledu legální metrologie mohou být uloženy na samostatné paměťové jednotce, která je zaplombována. Může se jednat například o paměť určenou jen ke čtení nebo složitější zařízení.
Dodatek ke třídě rizika E	
<p>Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód.</p>	
<p>Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i></p> <ul style="list-style-type: none"> Kontrolujeme komunikaci s dodatečným hardwarem, který je použit pro zabezpečení programu a dat. Kontrolujeme, zda neoprávněná změna programu či dat vede k zastavení programu. 	

Třída rizika B	Třída rizika C	Třída rizika D
<p>U7: Ochrana parametrů <i>Parametry související s funkcí přístroje v legální metrologii musí být chráněny proti neoprávněným změnám.</i></p>		
<p>Specifikace: 1. Parametry specifické pro daný typ přístroje jsou pro všechny přístroje téhož typu stejné a jsou součástí jeho softwaru. Platí pro ně proto požadavky P6. 2. Parametry specifické pro daný přístroj mohou být měněny, ale pouze v případě, že jsou příslušným způsobem chráněny a jsou měněny jen při ověření softwaru. <i>Nemohou být uloženy v počítači, jen na samostatných zabezpečených jednotkách.</i> 3. Nastavitelné parametry specifické pro daný přístroj mohou být měněny libovolně.</p>		
<p>Potřebná dokumentace: V dokumentaci musí být popsány všechny parametry relevantní z pohledu legální metrologie, jejich rozsahy a nominální hodnoty, spolu s popisem, kde jsou uchovávané, jak mohou být zobrazeny a jak jsou chráněny.</p>	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jak jsou parametry chráněny proti změnám.</p>	
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda je ochrana parametrů specifických pro daný typ přístroje dostatečná. • Kontrolujeme, zda nejsou parametry specifické pro daný přístroj uloženy přímo v počítači. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Testujeme přístroj v režimu jeho nastavování a v provozním režimu, přičemž kontrolujeme, zda je zabezpečení dat funkční. • Kontrolujeme klasifikaci parametrů a jejich popis (nastavitelný/zabezpečený) v nabídce přístroje (má-li nějakou). <p>Parametry musí být uvedeny v certifikátu schválení typu.</p>	<p>Validace: Dodatek k požadavkům pro třídy B a C:</p> <ul style="list-style-type: none"> • <i>Kontrola založená na dokumentaci</i> Kontrolujeme, zda a jak jsou parametry chráněny proti změnám. 	
<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> • Parametry specifické pro daný typ přístroje jsou uloženy na samostatném paměťovém prvku nebo přímo v jednotce senzoru. Jejich přepsání je zablokováno hardwarovým přepínačem na paměťovém prvku. Tato metoda může být kombinována s kontrolním čítačem. • Nastavitelné parametry jsou uloženy přímo v počítači. 		

Dodatek ke třídě rizika E

Potřebná dokumentace (dodatek k požadavkům pro třídy B a C):
Zdrojový kód související s ochranou parametrů

Validace (dodatek k požadavkům pro třídy B a C):

Kontrola zdrojového kódu:

- Kontrolujeme, zda je ochrana parametrů realizována vhodným způsobem.

Třída rizika B	Třída rizika C	Třída rizika D
<p>U8: Autentičnost softwaru a výsledků <i>Autentičnost softwaru musí být zajištěna vhodnými prostředky, stejně jako autentičnost výsledků, které software vytváří.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> Schválený software nesmí být možné simulovat pomocí jednoduchých nástrojů. Výsledky jsou považovány za autentické, pokud jsou výstupem ze schváleného softwaru. 	<p>Specifikace:</p> <p>Omezení 1BC, 2BC:</p> <ol style="list-style-type: none"> Prostředky ochrany proti zneužití softwaru, včetně jeho simulace, jsou založeny na dodatečném hardwaru. 	
<ol style="list-style-type: none"> Měřené hodnoty musí být doplněny informací, která identifikuje jejich původ a znemožňuje záměnu s jinými daty. Musí být zajištěno, že jen schválený software může vykonávat funkce relevantní z pohledu legální metrologie (např. senzor může pracovat jen ve spojení se schváleným softwarem). 		
<p>Potřebná dokumentace: Dokumentace musí popisovat, jakým způsobem je zajištěna autentičnost softwaru.</p>	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakými prostředky je zajištěna autentičnost softwaru.</p>	
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, jak jsou prezentovány výsledky měření a zda není možné je simulovat. Kontrolujeme, zda funkce relevantní z pohledu legální metrologie nemůže vykonávat jiný software. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda jsou výsledky vizuálně dostatečně odlišené od ostatních dat. Kontrolujeme, zda je prezentovaná informace úplná a v souladu s dokumentací. 	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda je ochrana autentičnosti provedena způsobem odpovídajícím vysokému stupni ochrany. 	
<p>Přijatelné řešení: <i>Formální prostředky</i></p> <ol style="list-style-type: none"> Identifikace softwaru se musí shodovat s hodnotou uvedenou v certifikátu schválení typu. <p><i>Technické prostředky</i></p> <ol style="list-style-type: none"> Ochrana okna aplikace, která je relevantní z pohledu legální metrologie, by měla zajišťovat, že: <ul style="list-style-type: none"> měřené hodnoty jsou nejprve zobrazeny a teprve následně mohou být předány jiným programům, okno je pravidelně obnovováno a je vždy viditelné, pokud okno není viditelné nebo je zavřené, software přestává zpracovávat měřená data. 		

2a: Senzor šifruje měřené hodnoty s využitím klíče známého softwaru běžícího na centrálnímu počítači (např. číslo verze), ten posléze hodnoty dešifruje. Klíč není znám jiným programům.	
2b: Senzor před vysláním hodnot prověří komunikaci výměnou utajených klíčů s centrálním počítačem, pokud tato kontrola selže, nepošle měřené hodnoty.	
3. Klíč použitý v bodech 2a a 2b může být změněn bez zásahu do plomb.	3. Klíč použitý v bodech 2a a 2b nemůže být změněn bez zásahu do plomb.
Dodatek ke třídě rizika E	
Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód programu.	
Validace: (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i>	
<ul style="list-style-type: none"> • Kontrolujeme, jak jsou prezentovány výsledky měření. • Kontrolujeme, zda je ochrana autentičnosti programu a výsledků realizována vhodným způsobem. 	

Třída rizika B	Třída rizika C	Třída rizika D
U9: Ovlivnění jiným softwarem <i>Software relevantní z pohledu legální metrologie musí být navržen tak, aby jeho funkci nemohl ovlivnit jiný software.</i>		
Specifikace: Předpokládáme oddělení softwaru relevantního z pohledu legální metrologie a software, který relevantní není. Viz rozšíření S.		
Potřebná dokumentace: Viz rozšíření S.		
Validace: Viz rozšíření S.		
Přijatelné řešení: Viz rozšíření S.		

6 ROZŠÍŘENÍ L: DLOUHODOBÉ UKLÁDÁNÍ MĚŘENÝCH DAT

Toto rozšíření udává dodatečné požadavky na jednoúčelové měřicí přístroje (typ P) a měřicí přístroje využívající počítače (typ U). Týká se požadavků na uložení dat pro jejich uchování po skončení měření až do okamžiku, kdy jsou zpracována z pohledu legální metrologie. Může se také týkat následného uložení zpracovaných dat nebo výsledků měření.

6.1 Technický popis

Soubor požadavků uvedených v této kapitole aplikujeme pouze v případě, že měřicí přístroj je vybaven funkcí dlouhodobého uchování dat, a to jen v případě, že uchovávaná data jsou legálně relevantní. V následující tabulce jsou popsány tři různé technické konfigurace dlouhodobého uložení dat. Pro jednoúčelové zařízení je nejčastějším technickým prostředkem integrovaná paměť – zde je uložení dat součástí metrologického hardwaru a softwaru. Naopak měřicí přístroje využívající počítače nejčastěji využívají média, která jsou součástí počítače, např. pevný disk. Dalším využitelným technickým prostředkem je odnímatelná paměť dat, která může představovat jak jednoúčelové přenosné úložiště dat, tak jiný počítač. Pokud jsou data přenášena na odnímatelné paměti a následné operace s nimi jsou předmětem kontroly z pohledu legální metrologie, jsou i tato paměť a způsob uložení dat předmětem revize z pohledu legální metrologie.

Popis
<p>Integrovaná paměť Jednoduché zařízení určené jen pro ukládání dat, přičemž není možné data číst, ukládat nebo měnit bez použití dalších zařízení (např. RAM, Flash disk, pevný disk).</p>
<p>Paměť počítače Víceúčelový počítač s určitým operačním systémem a uživatelským rozhraním, kde souběžně existují programy a operace související a nesouvisející s činností, která je předmětem kontroly z pohledu legální metrologie. Jeho paměťové médium může být demontováno a přeneseno na jiný počítač a jeho obsah může být kopírován v rámci počítače i mimo něj.</p>

Odnímatelná paměť

Jakékoli zařízení, které není nedílnou součástí přístroje a může být použito k uložení dat, např. disketová média, paměťové karty nebo databáze na vzdálených počítačích.

Tabulka 6.1: technický popis přístroje typu U

6.2 Dodatečné požadavky

Požadavky aplikujeme na jednoúčelové měřicí přístroje (typ P) i měřicí přístroje využívající počítače (typ U) v případě, že jsou vybaveny zařízeními pro ukládání dat podle odstavce 6.1.

Třída rizika B	Třída rizika C	Třída rizika D
L1: Úplnost uložených dat		
<i>Uložená data musí obsahovat všechny informace potřebné k rekonstrukci měřených hodnot.</i>		
Specifikace:		
1. Ukládání měřených dat může být nezbytné například z důvodu kontroly účtování. Je třeba uchovávat všechny parametry a podmínky měření, které jsou relevantní pro takovou kontrolu.		
Potřebná dokumentace:		
Popis všech položek uložených dat.		
Validace:		
<i>Kontrola založená na dokumentaci</i>		
<ul style="list-style-type: none"> Kontrolujeme, zda jsou v datech obsaženy všechny informace potřebné pro legální a metrologické účely. 		
Přijatelné řešení:		
<ul style="list-style-type: none"> Záznam o měření, který je kompletní jak z pohledu metrologie, tak z pohledu legální metrologie, obsahuje <ul style="list-style-type: none"> měřené hodnoty s dostatečným rozlišením, jejich jednotky, jednotkovou nebo celkovou cenu (existuje-li), čas a místo měření, identifikaci měřicího přístroje (u externího uchování dat). Data jsou uložena ve stejném formátu (rozlišení, jednotky), jako jsou uvedena na účtence při platbě v okamžiku měření. 		
Dodatek ke třídě rizika E		
Potřebná dokumentace (dodatek k požadavkům pro třídy B, C a D): Zdrojový kód softwaru.		
Validace (dodatek k požadavkům pro třídy B, C a D): <i>Kontrola zdrojového kódu:</i> Kontrolujeme, zda jsou data ukládána správně.		

Třída rizika B	Třída rizika C	Třída rizika D
L2: Ochrana proti náhodným (nechtěným) změnám <i>Uložená data musí být chráněna proti náhodným (nechtěným) změnám.</i>		
Specifikace: Příčiny náhodných změn mohou být následující: <ol style="list-style-type: none"> 1. Fyzické vlivy: uložená data musí být chráněna proti náhodným změnám či smazání, pokud by nastala hardwarová chyba. 2. Chyba uživatele: data mohou být uživatelem mazána, například po uplynutí doby nutné k jejich uchování. V takovém případě musí být data, která mají být uchována, přiměřeným způsobem chráněna proti neúmyslnému smazání. Tento aspekt je zvláště důležité kontrolovat u systémů na síti nebo systému se vzdáleným uchováním dat, kde nemusí být všem uživatelům zřejmé, která data mají být uchována. 3. Pro kontrolu identity dat používáme kontrolní součet; pokud nesouhlasí s příloženou hodnotou, musí být data smazána nebo označena za poškozená. 		
Potřebná dokumentace: V dokumentaci musí být popsána ochrana dat, tedy algoritmus, který je pro tuto ochranu použit.	Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být popsány prostředky, kterými je testována funkce ochrany dat.	
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> • Kontrolujeme, zda je kontrolní součet programu a dat počítán. • Kontrolujeme, zda software, který data následně čte, porovnává tento kontrolní součet s nominální hodnotou. • Kontrolujeme, zda nemůže dojít k přepsání dat, která by měla být v přístroji zachována po určitou dobu danou výrobcem. • Kontrolujeme, zda program varuje uživatele před smazáním dat. <i>Funkční kontrola</i> <ul style="list-style-type: none"> • Pokud je možné mazat data, kontrolujeme, zda je před jejich smazáním uživatel varován. 	Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> • Kontrolujeme, zda prostředky ochrany dat odpovídají vysokému stupni ochrany. 	
Přijatelné řešení: <ul style="list-style-type: none"> • Pro detekci náhodných změn počítáme kontrolní součet pomocí algoritmu CRC-16 a jeho výslednou hodnotu ukládáme spolu s daty. Klíč algoritmu je znám také programu, který data následně načítá. 		

***Poznámka:** algoritmus není utajen a není utajen ani generující polynom ani inicializační vektor CRC. Tyto parametry jsou známy oběma programům, které generují a kontrolují kontrolní součty.*

- Měřená data i účtenky mohou být chráněny automaticky generovaným časovým údajem a údajem o tom, zda byla účtenka vydána/zaplacena. Není možné smazat měřená data, jestliže nebylo měření zapláceno.
- Měřená data nemohou být smazána bez potvrzení uživatelem.

Dodatek ke třídě rizika E

Potřebná dokumentace (dodatek k požadavkům pro třídy B, C a D):
Zdrojový kód.

Validace (dodatek k požadavkům pro třídy B, C a D):
Kontrola zdrojového kódu:
Kontrolujeme vhodnost a implementaci metod kontroly náhodných změn.

Třída rizika B	Třída rizika C	Třída rizika D
L3: Integrita dat <i>Měřená data musí být chráněna proti záměrným změnám.</i>		
Specifikace: 1. Tyto požadavky se týkají všech paměťových médií kromě integrovaných pamětí. 2. Kde je to nutné, musí být učiněna opatření, která zabrání změně dat jednoduchými prostředky. 3. Mezi jednoduché prostředky počítáme zejména běžně dostupné nástroje, jako jsou např. textové editory nebo kancelářské aplikace.	Specifikace: 1. Tyto požadavky se týkají všech paměťových médií kromě integrovaných pamětí. 2. Musí být učiněna opatření, která zabrání změně dat sofistikovanými prostředky. 3. Mezi sofistikované prostředky počítáme například diskové editory, debugery apod. 4. Ochrana dat musí být na stejné úrovni jako u dat souvisejících s elektronickými platbami. 5. Ochrana dat musí být realizována prostřednictvím algoritmu elektronického podpisu, u něž je zřejmé, že změna dat nepovede ke stejnému podpisu. <i>Poznámka: řešení na bázi PC není pro tuto třídu vyhovující. I když jsou klíče a algoritmy dostatečně bezpečné, programy, které data podepisují a ověřují, nejsou dostatečně zabezpečeny (viz požadavek U6-D).</i>	
Potřebná dokumentace: Dokumentace musí zahrnovat popis ochrany proti záměrným změnám dat.	Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeny konkrétní prostředky ochrany proti záměrným změnám dat.	
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> • Pokud je použit kontrolní součet, kontrolujeme, zda je počítán z celého bloku dat a zda je nominální hodnota kontrolního součtu následně použita při načítání dat. • Kontrolujeme, zda jsou klíče, které by měly být tajné, skutečně zabezpečeny proti zjištění jednoduchými nástroji. <i>Funkční kontrola</i> <ul style="list-style-type: none"> • Kontrolujeme, zda není možné načíst poškozená data. 	Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> • Kontrolujeme, zda jsou prostředky ochrany proti záměrným změnám vhodně zvoleny vzhledem k vysoké úrovni ochrany. 	

<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> • Data jsou kontrolována automaticky generovaným kontrolním součtem, který je porovnáván se známou hodnotou (uloženou spolu s daty). Pokud je takto hodnota změněna, data nemohou být použita. • Za dostatečné řešení je považován jakýkoli algoritmus digitálního podpisu, který má klíč dlouhý alespoň 2 byty, například CRC 16. <p><i>Poznámka: V tomto případě je algoritmus znám, nicméně (narozdíl od požadavku L2) pracuje s uživateli neznámými hodnotami inicializačních vektorů, se kterými je třeba zacházet jako s klíči.</i></p>	<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> • Namísto kontrolního součtu se provádí elektronické podepisování vhodným algoritmem, například pomocí hash algoritmu SHA-1 nebo RipeMD160 v kombinaci se šifrováním algoritmy, jako jsou RSA nebo eliptické křivky. Minimální délka klíče je 768 bitů (RSA) nebo 128–160 bitů (EC).
<p>Dodatek ke třídě rizika E</p>	
<p>Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód.</p>	
<p>Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i> Kontrolujeme mechanismy, které zajišťují kontrolu integrity dat.</p>	

Třída rizika B	Třída rizika C	Třída rizika D
L4: Autentičnost dat <i>Musí existovat způsob, jak doložit původ dat z daného měřidla.</i>		
Specifikace: <ol style="list-style-type: none"> Autentičnost dat je možné třeba kontrolovat například při placení nebo kontrole účtování. Je nezbytné, aby existovalo přiřazení mezi daty a konkrétním přístrojem, který je vytvořil (naměřil). Aby mohla být autentičnost kontrolována, musí být data jednoznačně identifikována. Autentičnost nemusí být nutně zajištěna šifrováním dat. 		
Potřebná dokumentace: Dokumentace musí popisovat, jak je zajištěna autentičnost dat.	Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakými prostředky je zajištěna autentičnost dat.	
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda existuje přiřazení mezi daty a konkrétním měřením. Pokud je využit kontrolní součet nebo elektronický podpis, kontrolujeme, zda je počítán z celého bloku dat. Kontrolujeme, zda data, která mají být skryta (např. klíče), nemohou být zjištěna jednoduchými nástroji. <i>Funkční kontrola</i> <ul style="list-style-type: none"> Kontrolujeme, zda jsou údaje v paměti a na účtence identická. 	Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda je ochrana autentičnosti provedena způsobem odpovídajícím vysokému stupni ochrany. 	
Přijatelné řešení: Uložená data obsahují následující prvky: <ul style="list-style-type: none"> jednoznačnou identifikaci stejnou jako na účtence, časový záznam o měření stejný jako na účtence, identifikaci měřícího přístroje, podpis, který je využit pro kontrolu integrity, může být zároveň využit pro kontrolu autentičnosti, na účtence může být zmíněno, že může být zkontrolována s paměťovým médiem, které je předmětem kontroly z pohledu legální metrologie. Přiřazení může být realizováno prostřednictvím čísla účtenky nebo časového údaje. 		
Dodatek ke třídě rizika E		
Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód programu.		
Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i> <ul style="list-style-type: none"> Kontrolujeme, zda jsou data ukládána ve formátu, který umožňuje kontrolu autentičnosti. 		

Třída rizika B	Třída rizika C	Třída rizika D
<p>L5: Důvěryhodnost klíčů <i>Klíče použité při zabezpečení dat musí být považovány za data relevantní z pohledu legální metrologie a musí být chráněny proti změnám softwarovými prostředky.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> 1. Tento blok požadavků aplikujeme pouze na skryté (utajené) klíče. 2. Tento blok požadavků se týká uchovávání měřených dat mimo přístroj, který měření provedl, nebo počítač, na kterém běžel software, který vyprodukoval měřená data. 3. Klíče musí být chráněny proti modifikaci jednoduchými nástroji. 4. Je postačující, je-li přístup ke klíčům zabezpečen hardwarovými prostředky, například plombováním. 	<p>Specifikace:</p> <ol style="list-style-type: none"> 1. Tento blok požadavků se týká uchovávání měřených dat v přístroji, který měření provedl (nebo v počítači, na kterém běžel software, který vyprodukoval měřená data) i mimo něj. 2. Klíče musí být chráněny proti modifikaci sofistikovanými nástroji. 3. Metody ochrany klíčů musí být obdobné ochraně klíčů při elektronických platbách. Uživatel musí mít možnost zkontrolovat autentičnost veřejného klíče. 	
<p>Potřebná dokumentace: Dokumentace musí popisovat, jak jsou zajištěna správa a utajení klíče a s nimi související informace.</p>	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakými prostředky je zajištěno utajení klíče a s ním souvisejících informací.</p>	
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda nemůže být skrytá informace odhalena. 	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda ochrana klíče odpovídá vysokému stupni ochrany. 	
<p>Přijatelné řešení: Soukromý klíč je uchováván v binární podobně přímo ve spustitelném souboru (uživatel neví, kde se v binárním souboru vyskytuje). V softwaru není žádný nástroj, který by klíč vizualizoval. Pokud je použit kontrolní součet, jako klíč se používá generující polynom nebo vstupní vektor.</p>	<p>Přijatelné řešení: Soukromý klíč je uchováván v externím paměťovém zařízení, které může být zaplombováno. V softwaru není žádný nástroj, který by klíč vizualizoval nebo umožňoval jeho editaci.</p>	

	<p><i>Poznámka:</i> Řešení na bázi PC není pro tuto třídu dostačující, pokud by nezahrnovalo další hardwarové prostředky ochrany klíče (viz požadavek U6).</p> <ol style="list-style-type: none"> 1. <i>infrastruktura veřejného klíče:</i> veřejný klíč je uložen v příslušném akreditovaném centru 2. <i>přímá důvěra:</i> po dohodě obou zúčastněných stran je klíč považován za důvěryhodný.
Dodatek ke třídě rizika E	
<p>Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód programu.</p>	
<p>Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda je ochrana klíče zabezpečena vhodným způsobem. 	

Třída rizika B	Třída rizika C	Třída rizika D
<p>L6: Načtení uložených dat <i>Software, který je použit pro kontrolu uložených dat, musí být schopen načíst, zobrazit či tisknout data, detekovat jejich změny a varovat v případě, že jsou data změněna. Změněná data nesmí být dále použita.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> Měřená data mohou být k dispozici k následným kontrolám. Existují-li pochybnosti o správnosti některého dokladu o měření, musí existovat způsob, jak identifikovat konkrétní měření mezi uloženými daty. Identifikační číslo měření musí být uvedeno na dokladu o měření (účtence) spolu s informací, že jsou data uložena v zařízení, které je předmětem kontroly z pohledu legální metrologie. Kontrolou uložených dat rozumíme kontrolu integrity, autenticity a přiřazení dat konkrétnímu měření. Software, který provádí kontrolu uložených dat, je předmětem kontroly z pohledu legální metrologie. Pro další specifické požadavky viz Rozšíření I. 		
<p>Potřebná dokumentace:</p> <ul style="list-style-type: none"> Popis funkcí softwaru určeného pro kontrolu uložených dat Popis detekce změn dat Uživatelský manuál 	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakými prostředky je zajištěna ochrana programu.</p>	
<p>Validace: <i>Kontrola založená na dokumentaci</i> Kontrolujeme, zda software skutečně porovnává vypočtené a nominální kontrolní součty. Kontrolujeme, zda je software určený pro kontrolu uložených dat předmětem kontroly z pohledu legální metrologie. <i>Funkční kontrola</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda program detekuje poškozená a modifikovaná data. Kontrolujeme, zda je informace získaná z uložených dat úplná. 	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda ochrana dat odpovídá vysokému stupni ochrany. 	
<p>Přijatelné řešení: Data jsou načtena a je spočítán jejich kontrolní součet. Ten je porovnán s nominální hodnotou a data jsou prohlášena za správná, jen pokud se oba součty shodují. Pokud se neshodují, jsou data prohlášena za poškozená a jsou smazána.</p>		
<p>Dodatek ke třídě rizika E</p>		
<p>Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód softwaru.</p>		
<p>Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda jsou algoritmy kontroly dat správným způsobem implementovány. 		

Třída rizika B	Třída rizika C	Třída rizika D
L7: Automatické ukládání		
<i>Data musí být ukládána automaticky po skončení měření.</i>		
Specifikace:		
<ol style="list-style-type: none"> 1. Tento požadavek se týká všech druhů dlouhodobého uchovávání dat. 2. Uložení/neuložení dat nesmí být dané vůlí operátora. Mohou však existovat měřené hodnoty, které jsou operátorem prohlášeny za špatné výsledky, a měření je opakováno (např. u vážení). Každá hodnota, kterou operátor akceptuje, však musí být automaticky uložena. 3. Požadavky na kapacitu paměti jsou dány v odstavci L8. 		
Potřebná dokumentace:		
Informace o automatickém ukládání dat, popis uživatelského rozhraní.		
Validace:		
<i>Funkční kontrola</i>		
<ul style="list-style-type: none"> • Náhodně kontrolujeme, zda jsou měření skutečně uložena v paměti. Kontrolujeme, zda není možné ukládání dat nějakým způsobem přerušit. 		
Přijatelné řešení:		
Neexistuje žádný prvek uživatelského rozhraní, kterým by bylo možné přerušit nebo vypnout automatické ukládání dat. Data jsou ukládána okamžitě po skončení měření (nebo akceptování výsledků operátorem) spolu s informací o čase měření.		
Dodatek ke třídě rizika E		
Potřebná dokumentace (dodatek k požadavkům pro třídy B, C a D): Zdrojový kód softwaru		
Validace (dodatek k požadavkům pro třídy B, C a D): <i>Kontrola zdrojového kódu:</i> Kontrolujeme, zda jsou prostředky použité pro automatické ukládání vhodně a správně navrženy a implementovány.		

Třída rizika B	Třída rizika C	Třída rizika D
L8: Kapacita paměti <i>Kapacita paměti musí být dostatečná pro zamýšlené použití.</i>		
Specifikace: <ol style="list-style-type: none"> 1. Pokud je kapacita paměti zaplněna nebo je paměť odejmuta/odpojena, musí být vyvoláno příslušné varování. Další požadavky na reakci jsou v rozšíření I. 2. Doba, po kterou mají být data uchovávána, je daná národní regulací a je mimo rámec tohoto dokumentu. Zodpovědnost za to, že přístroj je schopen ukládat data po příslušnou dobu, nese uživatel, notifikovaná osoba pak kontroluje, zda jsou tyto parametry přístroje ve shodě s národní regulací a zda není možné měřit, pokud je paměť plná. 3. Způsob stanovení přiměřené kapacity paměti je také mimo rámec tohoto dokumentu a je za ni zodpovědný výrobce. 		
Potřebná dokumentace: Popis chování programu, pokud se při ukládání dat do paměti vyskytne problém.		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> • Kontrolujeme, zda výrobce udává způsob, jakým stanovil kapacitu paměti. • Kontrolujeme, zda (podle dokumentace) nemůže nastat nechtěné přepsání dat dříve než po uplynutí doby stanovené výrobcem. <i>Funkční kontrola</i> <ul style="list-style-type: none"> • Kontrolujeme, zda je uživatel varován před smazáním dat (je-li možné je mazat). • Kontrolujeme, zda je vyvoláno varování, je-li kapacita paměti zaplněna nebo je paměť odejmuta/odpojena. 		
Přijatelné řešení: <ul style="list-style-type: none"> • Jednotlivá měření, která mohou být přerušena (např. vážení), mohou být dokončena i v případě, že je paměť nedostupná a data aktuálního měření mohou být uložena v dočasné paměti. Další měření však nesmí být započato a hodnoty v dočasné paměti musí být uchovány do doby, kdy bude paměť opět k dispozici. • Kontinuální měření mohou pokračovat i v případě výpadku paměti, pokud je možné hodnoty uložit v dočasné paměti a posléze doplnit do paměti v době, kdy bude paměť opět k dispozici. • Data v paměti mohou být přepisována, pokud jsou již zastaralá (jejich stáří přesáhlo dobu uchovávaní podle národní regulace), i tak musí být vyžádán souhlas uživatele a data musí být mazána počínaje nejstaršími hodnotami. 		
Dodatek k třídě rizika E		
Potřebná dokumentace (dodatek k požadavkům pro třídy B, C a D): Zdrojový kód softwaru		
Validace (dodatek k požadavkům pro třídy B, C a D): <i>Kontrola zdrojového kódu:</i> <ul style="list-style-type: none"> • Kontrolujeme, zda jsou prostředky použité pro ukládání vhodně a správně navrženy a implementovány. 		

7 ROZŠÍŘENÍ T: PŘENOS DAT PO KOMUNIKAČNÍCH SÍTÍCH

Toto rozšíření udává dodatečné požadavky na jednoúčelové měřicí přístroje (typ P) a měřicí přístroje využívající počítače (typ U). Týká se požadavků na přenos dat.

7.1 Technický popis

Soubor požadavků v této kapitole aplikujeme pouze v případě, že měřicí přístroj je vybaven funkcí přenosu dat, a to jen tehdy, pokud jsou přenášená data legálně relevantní. V následující tabulce jsou popsány tři různé síťové konfigurace přenosu dat. Nejjednodušší variantou je skupina přístrojů, které všechny podléhají kontrole z pohledu legální metrologie, přičemž jejich počet i identita jsou známy v okamžiku ověřování celé sestavy. Další variantou je síť daného počtu účastníků (s neměnnou identitou), ve které jsou jen některé přístroje předmětem kontroly z pohledu legální metrologie. Poslední variantou je otevřená síť bez jakýchkoli omezení na množství, identitu nebo funkcionalitu jednotlivých účastníků.

Popis
<p>Uzavřená síť, všichni účastníci jsou předmětem kontroly z pohledu legální metrologie Počet a identita účastníků jsou známy. V síti neexistují zařízení, která by nebyla předmětem kontroly z pohledu legální metrologie.</p>
<p>Uzavřená síť, někteří účastníci jsou předmětem kontroly z pohledu legální metrologie Počet a identita účastníků jsou známy. V síti existují zařízení, která nejsou předmětem kontroly z pohledu legální metrologie.</p>
<p>Otevřená síť K síti se může připojit libovolný počet účastníků. Identita a počet těchto účastníků nemusí být jednotlivým účastníkům známy. Za tuto síť považujeme i jakoukoliv síť, která je založena na bezdrátovém přenosu dat.</p>

Tabulka 7.1 Technický popis přístroje typu U

7.2 Dodatečné požadavky

Požadavky aplikujeme na jednoúčelové měřicí přístroje (typ P) i měřicí přístroje využívající počítače (typ U) v případě, že jsou vybaveny zařízeními pro přenos podle odstavce 7.1.

Třída rizika B	Třída rizika C	Třída rizika D
T1: Úplnost přenesených dat <i>Přenesená data musí obsahovat všechny informace potřebné k rekonstrukci měřených hodnot.</i>		
Specifikace: 1. Přenos dat může zahrnovat jednu nebo více měřených hodnot a dalších parametrů. Je třeba přenést všechny parametry a podmínky měření, které jsou relevantní pro rekonstrukci údajů o měření.		
Potřebná dokumentace: Popis všech položek uloženého záznamu o měření.		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> • Kontrolujeme, zda jsou v datech obsaženy všechny potřebné informace. 		
Přijatelné řešení: Záznam o měření, který je kompletní jak z pohledu metrologie, tak z pohledu legální metrologie, obsahuje <ul style="list-style-type: none"> • měřené hodnoty s dostatečným rozlišením, • jejich jednotky, • jednotkovou nebo celkovou cenu (existuje-li), • čas a datum měření, • identifikace měřicího přístroje (u externího uchování dat), • místo měření (je-li to relevantní). 		
Dodatek ke třídě rizika E		
Potřebná dokumentace (dodatek k požadavkům pro třídy B, C a D): Zdrojový kód softwaru		
Validace (dodatek k požadavkům pro třídy B, C a D): <i>Kontrola zdrojového kódu:</i> <ul style="list-style-type: none"> • Kontrolujeme, zda jsou přenášeny bloky dat správně sestavovány. 		

Třída rizika B	Třída rizika C	Třída rizika D
T2: Ochrana proti náhodným (nechtěným) změnám <i>Uložená data musí být chráněna proti náhodným (nechtěným) změnám.</i>		
Specifikace: Příčiny náhodných změn mohou být následující: <ol style="list-style-type: none"> 1. náhodné změny způsobené vlivy okolního prostředí, 2. chyby uživatele nebo zařízení, 3. chyby přenosu dat. 		
Potřebná dokumentace: V dokumentaci musí být popsána ochrana dat, tedy algoritmus kontrolního součtu, který je pro tuto ochranu použit.		Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být popsány prostředky, kterými je testována funkce ochrany dat.
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> • Kontrolujeme, zda je kontrolní součet programu a dat počítán z příslušných dat. • Kontrolujeme, zda software, který data následně přijímá, porovnává tento kontrolní součet s nominální hodnotou. 		Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> • Kontrolujeme, zda prostředky ochrany dat odpovídají vysokému stupni ochrany.
Přijatelné řešení: <ol style="list-style-type: none"> 1. Pro detekci náhodných změn počítáme kontrolní součet pomocí algoritmu CRC-16 a jeho výslednou hodnotu přenášíme spolu s daty. Klíč algoritmu je znám také programem, který data následně přijímá. <i>Poznámka: algoritmus není utajen a není utajen ani generující polynom ani inicializační vektor CRC. Tyto parametry jsou známy oběma programům, které generují a kontrolují kontrolní součty.</i> 2. Přenášená data mohou být chráněna prostředky daného přenosového protokolu, např. TCP/IP, IFSF. 		
Dodatek ke třídě rizika E		
Potřebná dokumentace (dodatek k požadavkům pro třídy B, C a D): Zdrojový kód.		
Validace (dodatek k požadavkům pro třídy B, C a D): <i>Kontrola zdrojového kódu:</i> <ul style="list-style-type: none"> • Kontrolujeme vhodnost a implementaci metod kontroly náhodných změn během přenosu. 		

Třída rizika B	Třída rizika C	Třída rizika D
T3: Integrita dat <i>Měřená data musí být chráněna proti záměrným změnám během přenosu.</i>		
<p>Specifikace:</p> <ol style="list-style-type: none"> 1. Tyto požadavky se týkají jen otevřených sítí nebo sítí, které nejsou plně pod kontrolou přístrojů souvisejících s legální metrologií. 2. Musí být učiněna opatření, která zabrání změně dat jednoduchými prostředky. 3. Mezi jednoduché prostředky počítáme zejména běžně dostupné nástroje, jako jsou např. textové editory nebo kancelářské aplikace. 	<p>Specifikace:</p> <ol style="list-style-type: none"> 1. Tyto požadavky se týkají všech sítí, otevřených i uzavřených. 2. Musí být učiněna opatření, která zabrání změně dat sofistikovanými prostředky. 3. Mezi sofistikované prostředky počítáme například diskové editory, debugery apod. 4. Ochrana dat musí být na stejné úrovni, jako u dat souvisejících s elektronickými platbami. 5. Ochrana dat musí být realizována prostřednictvím algoritmu elektronického podpisu, u něž je zřejmé, že změna dat nepovede ke stejnému podpisu. <p><i>Poznámka: řešení na bázi PC není pro tuto třídu vyhovující. I když jsou klíče a algoritmy dostatečně bezpečné, programy, které data podepisují a ověřují, nejsou dostatečně zabezpečeny (viz požadavek U6-D).</i></p>	
<p>Potřebná dokumentace:</p> <p>Dokumentace musí zahrnovat popis ochrany proti záměrným změnám dat.</p>	<p>Potřebná dokumentace:</p> <p>Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeny konkrétní prostředky ochrany proti záměrným změnám dat.</p>	
<p>Validace:</p> <p><i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Pokud je použit kontrolní součet, kontrolujeme, zda je počítán z celého bloku dat a zda je nominální hodnota kontrolního součtu následně použita při načítání dat. • Kontrolujeme, zda jsou soukromé klíče, které by měly být tajné, skutečně zabezpečeny proti zjištění jednoduchými nástroji. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda není možné načíst poškozená data. 	<p>Validace:</p> <p>Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda jsou prostředky ochrany proti záměrným změnám vhodně zvoleny vzhledem k vysoké úrovni ochrany. 	

<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> • Data jsou před přenosem kontrolována automaticky generovaným kontrolním součtem, který je porovnáván se známou hodnotou (přenášenou spolu s daty). Pokud je tato hodnota změněna poté, co je po přenosu znovu spočtena, data nemohou být použita. • Za dostatečné řešení je považován jakýkoli algoritmus digitálního podpisu, který má klíč dlouhý alespoň 2 byty, například CRC 16. <p><i>Poznámka: v tomto případě musí být klíč podpisu znám, aby bylo možné ověřit integritu dat.</i></p>	<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> • Namísto kontrolního součtu se provádí elektronické podepisování vhodným algoritmem, například pomocí hash algoritmu SHA-1 nebo RipeMD160 v kombinaci se šifrováním algoritmy, jako jsou RSA nebo eliptické křivky. Minimální délka klíče je 768 bitů (RSA) nebo 128–160 bitů (EC). • Ochrana může být zabezpečena adekvátním protokolem přenosu, např. HTTPS.
Dodatek ke třídě rizika E	
<p>Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód.</p>	
<p>Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i></p> <ul style="list-style-type: none"> • Kontrolujeme mechanismy, které zabezpečují kontrolu integrity dat během přenosu. 	

Třída rizika B	Třída rizika C	Třída rizika D
T4: Autentičnost dat <i>Musí existovat způsob, jak doložit původ dat z daného měřidla i po jejich přenosu do jiného zařízení.</i>		
Specifikace: 1a. V otevřené síti musí být jednoznačně dáno, odkud se data přenášejí (identifikace dat a identifikace adresy zdroje). 1b. Uzavřená síť je zaplombována v okamžiku ověření jejích jednotlivých účastníků, v takové konfiguraci nemusí být použity další prostředky zabezpečení sítě. 2. Během přenosu mohou nastat nepředvídatelná zpoždění, data proto musí být vybavena časovým údajem o tom, kdy bylo měření provedeno. 3. Autentičnost nemusí být nutně zajištěna šifrováním dat.		
Potřebná dokumentace: <i>Otevřená síť:</i> Dokumentace musí popisovat, jakým způsobem je zajištěno přiřazení dat konkrétnímu měření. <i>Uzavřená síť:</i> Dokumentace musí popisovat, jak je zajištěn neměnný počet účastníků, a popisovat jejich počáteční identifikaci.		Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakými prostředky je zajištěna autentičnost dat při přenosu sítí.
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda existuje přiřazení mezi daty a konkrétním měřením. Pokud je využit kontrolní součet nebo elektronický podpis, kontrolujeme, zda je správně počítán. 		Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda je ochrana autentičnosti provedena způsobem odpovídajícím vysokému stupni ochrany.
Přijatelné řešení: <ul style="list-style-type: none"> Každá množina dat obsahuje jednoznačný identifikátor, který zahrnuje čas, kdy byla data změřena. Každá množina dat obsahuje jednoznačné přiřazení k přístroji, který je vytvořil, například jeho sériové číslo. V otevřené síti je autentičnost dat potvrzena podpisem každé množiny dat. Při příjmu dat je kontrolována jejich správnost. 		
Dodatek ke třídě rizika E		
Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód programů, které posílají a přijímají data.		
Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i> <ul style="list-style-type: none"> Kontrolujeme, zda jsou data přenášena způsobem, který umožňuje kontrolu autentičnosti. 		

Třída rizika B	Třída rizika C	Třída rizika D
<p>T5: Důvěryhodnost klíčů <i>Klíče použité při přenosu dat musí být považovány za data relevantní z pohledu legální metrologie a musí být chráněny proti změnám softwarovými prostředky.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> 1. Tento blok požadavků aplikujeme pouze na skryté (soukromé) klíče (většinou se to netýká uzavřených sítí). 2. Tento blok požadavků se týká uchování měřených dat mimo přístroj, který měření provedl, nebo počítač, na kterém běžel software, který vyprodukoval měřená data. 3. Klíče musí být chráněny proti modifikaci jednoduchými nástroji. 4. Je postačující, je-li přístup ke klíčům zabezpečen hardwarovými prostředky nebo úřední značkou. 	<p>Specifikace:</p> <ol style="list-style-type: none"> 1. Tento blok požadavků aplikujeme pouze na skryté (soukromé) klíče (většinou se to netýká uzavřených sítí). 2. Přijaté měřené hodnoty jsou kontrolovány prostřednictvím jejich elektronického podpisu s využitím veřejného klíče měřidla (nebo zařízení, které data zaslalo). Je tedy možné zkontrolovat přiřazení měřidla (nebo zařízení, které data zaslalo) a dat. 3. Klíče musí být chráněny proti modifikaci sofistikovanými nástroji. 4. Metody ochrany klíčů musí být obdobné ochraně klíčů při elektronických platbách. 	
<p>Potřebná dokumentace: Dokumentace musí popisovat, jakým způsobem je zajištěna správa a utajení klíče a s ním souvisejících informací.</p>	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakými prostředky je zajištěno utajení klíče a s ním souvisejících informací.</p>	
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda nemůže být skrytá informace odhalena. 	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda ochrana klíče odpovídá vysokému stupni ochrany. 	
<p>Přijatelné řešení: Soukromý klíč je uchovávan v binární podobě přímo ve spustitelném souboru (uživatel neví, kde se v binárním souboru vyskytuje). V softwaru není žádný nástroj, který by klíč vizualizoval. Pokud je použit kontrolní součet, jako klíč se používá generující polynom nebo vstupní vektor.</p>	<p>Přijatelné řešení: Soukromý klíč je uchovávan v externím paměťovém zařízení, které může být zaplombováno. V softwaru není žádný nástroj, který by klíč vizualizoval.</p>	

	<p><i>Poznámka: technické řešení založené na prostém využití osobního počítače není v tomto případě přijatelné.</i></p> <ol style="list-style-type: none">1. Infrastruktura veřejného klíče: veřejný klíč je uložen v příslušném akreditovaném centru.2. Přímá důvěra: po dohodě obou zúčastněných stran je klíč považován za důvěryhodný.
Dodatek ke třídě rizika E	
Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód programu.	
Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i> <ul style="list-style-type: none">• Kontrolujeme, zda je ochrana klíče zabezpečena vhodným způsobem.	

Třída rizika B	Třída rizika C	Třída rizika D
T6: Zacházení s poškozenými daty <i>Poškozená data nemohou být dále použita.</i>		
Specifikace: 1. Při komunikaci dochází k opakovanému posílání dat, která se nepodařilo přenést v pořádku. Neměl by tedy nastat případ, že by byla data přenosem poškozena.		
Potřebná dokumentace: Popis detekce chyb při přenosu.		Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakými prostředky je zajištěna detekce chyb při přenosu.
Validace: <i>Kontrola založená na dokumentaci a funkční kontrola</i> <ul style="list-style-type: none"> Kontrolujeme, zda nejsou poškozená data dále použita. 		Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda detekce poškození dat odpovídá vysokému stupni ochrany.
Přijatelné řešení: Pokud program obdrží data, jejichž cyklický součet nesouhlasí s nominální hodnotou, nejprve se pokusí využít případné nadbytečné informace na jejich rekonstrukci. Pokud se rekonstrukce nezdaří, je generováno varování a měřená hodnota není indikována. Datový blok přitom může buď označit (po uložení do speciálního pole), NEBO přímo smazat.		
Dodatek ke třídě rizika E		
Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód softwaru.		
<ul style="list-style-type: none"> Validace (dodatek k požadavkům pro třídy B a C): Kontrolujeme, zda jsou algoritmy zacházející s poškozenými daty správným způsobem implementovány. 		

Třída rizika B	Třída rizika C	Třída rizika D
T7: Zpoždění při přenosu		
<i>Měření nesmí být negativně ovlivněno zpožděním dat při přenosu.</i>		
Specifikace:		
Výrobce musí deklarovat, jaké je zpoždění dat během přenosu, v jakých mezích se může pohybovat, a musí garantovat, že ani v nejhorším případě nedojde k ovlivnění měření zpožděním dat.		
Potřebná dokumentace:		
Popis koncepce zacházení se zpožděním dat při přenosu.		
Validace:		
<i>Funkční kontrola</i>		
<ul style="list-style-type: none"> Kontrolujeme celou koncepci zacházení se zpožděním dat při přenosu a vliv zpoždění na funkci softwaru. 		
Přijatelné řešení:		
Implementace přenosu v komunikačních rozhraních typu <i>field bus</i> .		
Dodatek ke třídě rizika E		
Potřebná dokumentace (dodatek k požadavkům pro třídy B, C a D):		
Zdrojový kód softwaru		
Validace (dodatek k požadavkům pro třídy B, C a D):		
<ul style="list-style-type: none"> <i>Kontrola zdrojového kódu:</i> Kontrolujeme, zda jsou prostředky použité pro zacházení se zpožděním dat vhodně zvoleny a implementovány. 		

Třída rizika B	Třída rizika C	Třída rizika D
T8: Dostupnost přenosu dat <i>Pokud nastane výpadek v přenosu, nesmí způsobit ztrátu dat.</i>		
Specifikace: <ol style="list-style-type: none"> Uživatel nesmí mít možnost poškodit data poškozením přenosu dat. Problémy při přenosu musí být vhodným způsobem ošetřeny a musí s nimi být v návrhu programu počítáno. Reakce přístroje na výpadek přenosu závisí na konkrétním typu měřidla (viz rozšíření I). 		
Potřebná dokumentace: Dokumentace popisující ošetření výpadků přenosu.		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, jaké nástroje jsou zvoleny, aby bylo zabráněno ztrátě dat. Kontrolujeme, jak je systém připraven na výpadky přenosu. <i>Funkční kontrola</i> <ul style="list-style-type: none"> Zkoušky by měly prokázat reakci na náhodné výpadky sítě. 		
Přijatelné řešení: <ol style="list-style-type: none"> Jednotlivá měření, která mohou být přerušena (např. vážení) mohou být dokončena i v případě, že je přenos nedostupný a data aktuálního měření mohou být uložena v dočasné paměti. Další měření však nesmí být započato a hodnoty v dočasné paměti musí být uchovány do doby, kdy bude přenos opět k dispozici. Viz též kapitulu I. Kontinuální měření mohou pokračovat i v případě výpadku přenosu dat, pokud je možné hodnoty uložit v dočasné paměti a posléze přenést v době, kdy bude přenos dat opět k dispozici. 		
Dodatek ke třídě rizika E		
Potřebná dokumentace (dodatek k požadavkům pro třídy B, C a D): Zdrojový kód softwaru.		
Validace (dodatek k požadavkům pro třídy B, C a D): <ul style="list-style-type: none"> <i>Kontrola zdrojového kódu:</i> Kontrolujeme, zda jsou prostředky použité pro přenos vhodně a správně navrženy a implementovány. 		

8 ROZŠÍŘENÍ S: ODDĚLENÍ SOFTWARE

Toto rozšíření udává dodatečné požadavky na jednoúčelové měřicí přístroje (typ P) a měřicí přístroje využívající počítače (typ U), týkající se oddělení částí softwaru. Oddělení částí programového vybavení, které je a není předmětem kontroly z pohledu legální metrologie, je způsob, jak umožnit výrobcí jednoduše modifikovat část softwaru v měřicím přístroji.

8.1 Technický popis

Programy používané v měřicí technice jsou obecně velmi komplikované a zahrnují jak funkce, které s legální metrologií souvisí, tak funkce, které s ní nesouvisí. Jak pro výrobce, tak pro notifikovanou osobu je proto výhodné obě části jednoznačně oddělit.

V následující tabulce jsou popsány dvě různé varianty oddělení softwaru.

Popis
<p>Oddělení na nízké úrovni je provedeno na úrovni programové, tedy formou samostatných programů, nezávisle na operačním systému.</p> <p><i>Poznámka:</i> Takové oddělení může být v praxi provedeno jak u jednoúčelových zařízení, tak u zařízení využívajících počítač.</p>
<p>Oddělení na vysoké úrovni je provedeno s využitím funkcí operačního systému v rámci programových komponent.</p> <p><i>Poznámka:</i> Jedná se v převážné většině o oddělení do knihoven (například dynamicky linkovaných knihoven), a proto se nejčastěji užívá u zařízení využívajících počítač.</p>

Tabulka 8.1: technický popis přístroje typu U

I v případě oddělení softwaru je nezbytné zajistit, aby části, které se nezabývají funkcionalitou relevantní z pohledu legální metrologie, nemohly narušit funkce či data částí, které jsou z pohledu legální metrologie relevantní.

8.2 Dodatečné požadavky

Požadavky aplikujeme na jednoúčelové měřicí přístroje (typ P) i měřicí přístroje využívající počítače (typ U) v případě, že jsou realizovány s využitím oddělení softwaru podle odstavce 8.1.

Třída rizika B	Třída rizika C	Třída rizika D
<p>S1: Realizace oddělení softwaru <i>Software, který obsahuje funkce a data relevantní z pohledu legální metrologie, by měl být jednoznačně oddělen od ostatních částí softwaru.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> Pokud se jedná o separaci na <i>nízké úrovni</i>, musí mezi části relevantní z pohledu legální metrologie patřit všechny <i>části programu</i> (funkce, procedury, třídy apod.). Pokud se jedná o separaci na <i>vysoké úrovni</i>, musí mezi ně patřit všechny <i>programy a rozhraní</i>, <ul style="list-style-type: none"> které souvisí se získáváním či přepočtem měřené hodnoty nebo na ně mají vliv, které souvisí s pomocnými funkcemi, jako jsou zobrazování dat, zabezpečení dat, ukládání dat, identifikace softwaru, stahování softwaru, přenos dat, kontrola uložených dat atd. Všechny <i>proměnné, dočasné soubory a parametry</i>, které mají vliv na měření, měřená data nebo jiné funkce relevantní z pohledu legální metrologie, patří také mezi části relevantní z pohledu legální metrologie. Komponenty ochranného rozhraní (viz S3) patří mezi části relevantní z pohledu legální metrologie. Parametry a software, které nejsou relevantní z pohledu legální metrologie, mohou být měněny po schválení bez upozornění notifikované osoby, pokud jsou splněny podmínky dané v tomto rozšíření S. 		
<p>Potřebná dokumentace: Popis všech komponent, které jsou relevantní z pohledu legální metrologie.</p>		<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakým způsobem je oddělení softwaru prakticky provedeno.</p>
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda jsou všechny komponenty popsané ve specifikaci tohoto bloku uvedeny jako relevantní z pohledu legální metrologie. 		<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda je oddělení provedeno správně.
<p>Přijatelné řešení: Jednoznačně plyne z požadavků samotných.</p>		

Dodatek ke třídě rizika E

Potřebná dokumentace (dodatek k požadavkům pro třídy B a C):
Zdrojový kód softwaru (částí relevantních z pohledu legální metrologie).

Validace (dodatek k požadavkům pro třídy B a C):

Kontrola zdrojového kódu:

- Kontrolujeme, zda je tok dat relevantních z pohledu legální metrologie jednoznačně definován a může být ověřen.
- Kontrolujeme, zda jsou všechny komponenty programu, které souvisí s měřením a zpracováním dat, součástí částí relevantní z pohledu legální metrologie.
- Kontrolujeme, zda neexistuje nepřijatelný tok dat mezi částmi, které jsou relevantní z pohledu legální metrologie a které relevantní nejsou.

Třída rizika B	Třída rizika C	Třída rizika D
<p>S2: Smíšená indikace <i>Doplňující informace, která by byla generována částmi nerelevantními z pohledu legální metrologie, může být zobrazena pouze tehdy, neexistuje-li nebezpečí, že bude zaměněna za některou informaci z části relevantní z pohledu legální metrologie.</i></p>		
<p>Specifikace: Vzhledem k tomu, že sám programátor softwaru nemusí mít všechny informace o částech a výstupech relevantních z pohledu legální metrologie, je zodpovědností výrobce zařízení zajistit, že bude tento požadavek splněn.</p>		
<p>Potřebná dokumentace: Popis softwaru, který zajišťuje indikaci, a popis indikovaných parametrů relevantních z pohledu legální metrologie.</p>	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakým způsobem je smíšená indikace v praxi realizována.</p>	
<p>Validace: <i>Funkční kontrola</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda nemůže dojít k záměně dat, která byla generována částmi nerelevantními z pohledu legální metrologie, a dat, která byla generována částmi relevantními z pohledu legální metrologie. 	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda je smíšená indikace vhodně implementována. 	
<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> Informace generované částmi, které nejsou relevantní z pohledu legální metrologie, jsou předávány přes ochranné rozhraní do indikační části. Jsou přitom filtrovány tak, aby nemohly být zobrazeny jiné než přípustné informace. Je-li indikace provedena na počítači formou okna s měřenými daty, software kontroluje v pravidelných intervalech, zda je okno viditelné. Pokud je minimalizované nebo zakryté jinými okny, je generováno varování a metrologická funkce i výstup jsou pozastaveny. Poté, co je měření ukončeno, může být okno zavřeno. 		
<p>Dodatek ke třídě rizika E</p>		
<p>Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód softwaru (části relevantní z pohledu legální metrologie).</p>		
<p>Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda a jak je generována indikace. Kontrolujeme, zda nemůže být indikace potlačena nebo nahrazena jinými programy. 		

Třída rizika B	Třída rizika C	Třída rizika D
<p>S3: Ochranné rozhraní <i>Výměna dat mezi částmi, které jsou a nejsou relevantní z pohledu legální metrologie, musí být realizována výhradně prostřednictvím ochranného rozhraní, zahrnujícího jak interakci s okolními programy tak, samotný tok dat.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> Interakce s okolními programy ani tok dat nesmí nepřipustným způsobem ovlivnit proces měření a přepočtu výsledků. Příkazy, které mohou být předány přes rozhraní, musí být jednoznačně přiřazeny daným funkcím nebo operacím s daty. Příkazy, které nejsou dokumentovány, nesmí mít žádný vliv na chod části relevantní z pohledu legální metrologie. Rozhraní musí být plně zdokumentované a veškerý tok informací musí být realizován jeho prostřednictvím. <p><i>Poznámka: za správnou realizaci je zodpovědný programátor. Neexistují technické prostředky, které by mohly nějakým zvláštním způsobem zabezpečit rozhraní proti nesprávnému návrhu a naprogramování.</i></p>		
<p>Potřebná dokumentace:</p> <ul style="list-style-type: none"> Popis rozhraní, zejména pak popis dat, kterých se přenos přes rozhraní týká. Úplný seznam příkazů spolu s deklarací jeho úplnosti. Stručný popis významu jednotlivých příkazů a jejich vlivu na funkci přístroje a měřená data. 		<p>Potřebná dokumentace:</p> <p>Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakými prostředky je rozhraní realizováno.</p>
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda jsou funkce, které mohou být přes rozhraní spouštěny, definovány a dokumentovány. Kontrolujeme, zda jsou parametry, které mohou být přes rozhraní předávány, definovány a dokumentovány. Kontrolujeme, zda je dokumentace funkcí a parametrů úplná. 		<p>Validace: <i>Dodatek k požadavkům pro třídy B a C: Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda je rozhraní správně realizováno.
<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> Data v části relevantní z pohledu legální metrologie jsou pouze lokální proměnné. Rozhraní je realizováno jako funkce části relevantní z pohledu legální metrologie, která může být zvencí spuštěna a mohou jí být předány parametry. Rozhraní filtruje všechny nepřipustné příkazy. 		

Dodatek ke třídě rizika E

Potřebná dokumentace (dodatek k požadavkům pro třídy B a C):
Zdrojový kód softwaru (části relevantní z pohledu legální metrologie).

Validace (dodatek k požadavkům pro třídy B a C):

Kontrola zdrojového kódu:

- Kontrolujeme, zda je tok dat v programu jednoznačně dán a může být ověřen.
- Kontrolujeme tok dat rozhraním.
- Hledáme možné toky dat mimo rozhraní.
- Kontrolujeme, zda neexistují nedokumentované příkazy, které by mohly být zadány přes rozhraní.

9 ROZŠÍŘENÍ D: STAHOVÁNÍ SOFTWARE

Toto rozšíření udává dodatečné požadavky na jednoúčelové měřicí přístroje (typ P) a měřicí přístroje využívající počítače (typ U), týkající se stahování nových aplikací, oprav chyb nebo nových verzí softwaru, který je předmětem kontroly z pohledu legální metrologie.

9.5 Technický popis

Software může být stahován jen do měřicích přístrojů, které mají následující vlastnosti:

Popis
<p>Hardwarová konfigurace Cílové zařízení je předmětem kontroly z pohledu legální metrologie. Může to být jak jednoúčelový měřicí přístroj (typ P), tak měřicí přístroj využívající počítače (typ U). Stahování může proběhnout prostřednictvím přímého propojení (RS232, USB, aj.) přes uzavřenou nebo otevřenou síť (internet).</p>
<p>Softwarová konfigurace Software, který je stahován, může být jako celek předmětem kontroly z pohledu legální metrologie nebo může být využita koncepce oddělení legálně relevantních částí. Pokud není použito toto oddělení, musí se níže uvedené požadavky vztahovat na software jako celek.</p>

Tabulka 9.1: technický popis přístroje typu U

9.6 Dodatečné požadavky

Třída rizika B	Třída rizika C	Třída rizika D
<p>D1: Mechanismus stahování <i>Stahování softwaru, který je předmětem kontroly z pohledu legální metrologie, i jeho následná instalace by měly probíhat automaticky a takovým způsobem, aby byl zajištěn dostatečný stupeň ochrany instalovaného softwaru.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> 1. Stahování by mělo probíhat automaticky, aby nebyla narušena aktuální úroveň ochrany softwaru. 2. Cílové zařízení je vybaveno softwarem, který zahrnuje kontrolní mechanismy popsané v odstavcích D2–D5. 3. Cílové zařízení musí být schopné detekovat případný neúspěch stahování. V takovém případě se musí přístroj navrátit do stavu před stahováním nebo musí nastavit trvalé chybové hlášení a jeho metrologická funkce musí být zablokována. 		

<p>4. Po dokončení stahování musí být všechny ochranné mechanismy uvedeny do původního stavu, pokud nemá novější software oprávnění (dané notifikovanou osobou v certifikátu schválení typu) je změnit.</p> <p>5. V průběhu stahování nesmí být prováděno měření nebo musí být zajištěno, že měření nebude stahováním a instalací softwaru narušeno.</p> <p>6. Ošetření chyb popsané v rozšíření I může být aplikováno i na chyby stahování. Počet opětovných stahování při neúspěchu by měl být omezen.</p> <p>7. Pokud nejsou splněny požadavky D2–D5, je přesto možné stahovat software, který není předmětem kontroly z pohledu legální metrologie. V takovém případě musí být splněny následující požadavky:</p> <ul style="list-style-type: none"> • Je zajištěno oddělení ve smyslu odstavce S. • Celý software, který je předmětem kontroly z pohledu legální metrologie, je neměnný a nemůže být přeinstalován bez porušení plomby. • Stahování je povoleno certifikátem schválení typu. 	
<p>Potřebná dokumentace: Dokumentace musí stručně popisovat, jakým způsobem je stahování prováděno automaticky, jak je stažený software kontrolován, instalován, jakým způsobem se nastavuje úroveň ochrany po stažení a jak jsou ošetřeny chyby při stahování.</p>	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakým konkrétním způsobem je realizován mechanismus stahování.</p>
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, jak je stahování zajištěno. • Kontrolujeme, zda je stahování automatické, je-li přístroj v tu chvíli zablokovaný (je-li to nutné) a není-li jeho ochrana v této době porušena. • Kontrolujeme, zda existuje pevný software (který nemůže být stahován) provádějící kontrolu autentičnosti a integrity staženého softwaru. • Kontrolujeme, zda není v průběhu stahování možné měřit nebo zda není měření stahováním ovlivněno. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Provedeme alespoň jedno stahování, abychom zkontrolovali jeho průběh. 	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i> Kontrolujeme, zda je mechanismus stahování správný.</p>
<p>Přijatelné řešení: Neměnný program zajišťující stahování postupuje následujícím způsobem:</p> <ol style="list-style-type: none"> a) Naváže spojení s poskytovatelem programu. b) Automaticky zablokuje měření, pokud by je mohlo stahování ovlivnit. c) Automaticky stáhne software do zabezpečeného dočasného adresáře. d) Automaticky provede kontroly dané v D2–D4. e) Automaticky nainstaluje software do správného umístění. f) V případě potřeby smaže duplicitní nebo staré soubory. g) Zajistí, že je stupeň ochrany po stahování nastaven do původního stavu. h) V případě, že nastane chyba, vyvolá příslušnou reakci. 	

Dodatek ke třídě rizika E

Potřebná dokumentace (dodatek k požadavkům pro třídy B a C):
Zdrojový kód softwaru, který je zodpovědný za stahování.

Validace (dodatek k požadavkům pro třídy B a C):

Kontrola zdrojového kódu:

- Kontrolujeme, zda jsou prostředky použité pro správu stahování vhodně zvolené a realizované.

Třída rizika B	Třída rizika C	Třída rizika D
<p>D2: Autentičnost stahovaného softwaru <i>Musí být zajištěno, že stahovaný software je autentický a je schválen notifikovanou osobou.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> Předtím, než je stažený software poprvé použit, musí měřicí přístroj automaticky zkontrolovat, zda je <ol style="list-style-type: none"> software autentický (nejedná se o podvrh), software schválen pro daný typ přístroje. Prostředky použité k rozpoznání, zda je software schválen, musí být zabezpečené natolik, aby zabránily podvrhům. Pokud stažený software nevyhoví těmto testům, postupujeme podle D1. 		
<p>Potřebná dokumentace: Dokumentace musí popisovat</p> <ul style="list-style-type: none"> jakým způsobem je zajištěna identifikace softwaru, jak je kontrolována autenticita schválení typu softwaru, jak je zajištěna kontrola, že software je určen pro daný typ přístroje. 	<p>Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakými prostředky je kontrola autentičnosti provedena.</p>	
<p>Validace: <i>Kontrola založená na dokumentaci a funkční kontrola</i></p> <ul style="list-style-type: none"> Kontrolujeme v dokumentaci, jakým způsobem se software staví ke stažení podvrženého softwaru. Totéž zjišťujeme funkční kontrolou. <p>Kontrolujeme testy pro zajištění autentičnosti softwaru.</p>	<p>Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda jsou použité prostředky úměrné vysokému stupni ochrany. 	
<p>Přijatelné řešení:</p> <ol style="list-style-type: none"> Autentičnost: z důvodu zajištění integrity (viz D3) je často vytvořen elektronický podpis. Pro zajištění autentičnosti je pak dostačující, je-li software podepsán výrobcem. Kontrola musí být provedena automaticky. Notifikovaná osoba: Klíč notifikované osoby je součástí softwaru, který provádí stahování. Správný typ přístroje: software je vybaven seznamem kompatibilních přístrojů, jenž je porovnáván s identifikací přístroje, který jej stáhl. 		
<p>4. Schválení notifikovanou osobou: je-li software podepsán výrobcem, předpokládáme, že je schválen.</p>	<p>4. Schválení notifikovanou osobou: software je podepsán notifikovanou osobou. Její veřejný klíč je přímo uložen v softwaru, který provádí stahování, a je automaticky použit ke kontrole staženého softwaru. Klíč může být na vyžádání zobrazen, je proto možné jej kdykoliv zkontrolovat.</p>	

Dodatek ke třídě rizika E

Potřebná dokumentace (dodatek k požadavkům pro třídy B a C):
Zdrojový kód softwaru, který zajišťuje kontrolu autentičnosti stahovaného softwaru.

Validace (dodatek k požadavkům pro třídy B a C):

- *Kontrola zdrojového kódu:*
Kontrolujeme, zda jsou prostředky zajištění autentičnosti vhodně zvolené a implementované.

Třída rizika B	Třída rizika C	Třída rizika D
D3: Integrita stahovaného softwaru <i>Musí být zajištěno, že se software nezměnil nebo neporušil během stahování.</i>		
Specifikace: 1. Předtím, než je stažený software poprvé použit, musí měřicí přístroj automaticky zkontrolovat, zda nebyl poškozen nebo úmyslně změněn. 2. Pokud stažený software nevyhoví těmto testům, postupujeme podle D1.		
Potřebná dokumentace: Dokumentace musí popisovat, jakým způsobem je zajištěna kontrola integrity softwaru.	Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakými prostředky je kontrola integrity provedena.	
Validace: <ul style="list-style-type: none"> Kontrolujeme, zda je prováděna kontrola integrity po stažení softwaru. 	Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda jsou použité prostředky úměrné vysokému stupni ochrany. 	
Přijatelné řešení: <ul style="list-style-type: none"> Integrita může být testována provedením kontrolního součtu a porovnáním se známou hodnotu přiloženou k softwaru. Přijatelný algoritmus je CRC-32, jehož inicializační vektor je skrytý v programu, který je použit ke stahování softwaru. 	Přijatelné řešení: <ul style="list-style-type: none"> Integrita může být testována pomocí hash algoritmu (SHA-1, RipeMD-160) a šifrování (RSA, EC) s klíčem příslušné délky. Dešifrování je provedeno klíčem skrytý bodem 4 nesedí s originálem dě s originálem načením ginálu. platí pro třídu D navím v programu, který je použit ke stahování softwaru. 	
Dodatek ke třídě rizika E		
Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód softwaru, který zajišťuje kontrolu integrity stahovaného softwaru		
Validace (dodatek k požadavkům pro třídy B a C): <ul style="list-style-type: none"> <i>Kontrola zdrojového kódu:</i> Kontrolujeme, zda jsou prostředky zajištění kontroly integrity vhodně zvolené a implementované. 		

Třída rizika B	Třída rizika C	Třída rizika D
D4: Doložitelnost stahování softwaru <i>Stažení softwaru musí být doložitelné a ověřitelné při následné metrologické kontrole přístroje.</i>		
Specifikace: 1. Autorita, která provádí metrologickou kontrolu měřidla, musí mít možnost zpětně vysledovat stažení softwaru provedené v minulosti. 2. Samotné záznamy o stažení softwaru musí být vhodným způsobem zabezpečeny.		
Potřebná dokumentace: <ul style="list-style-type: none"> • Stručný popis prostředků zajišťujících doložení stahování softwaru. • Popis, jak může být informace o stahování zjištěna. 		Potřebná dokumentace: Dodatek k požadavkům pro třídy B a C: V dokumentaci musí být uvedeno, jakými prostředky je stahování zaznamenáváno.
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> • Kontrolujeme, zda je stahování zaznamenáno a záznamy zabezpečeny. <i>Funkční kontrola</i> <ul style="list-style-type: none"> • Kontrolujeme funkčnost zaznamenávání stahování. 		Validace: Dodatek k požadavkům pro třídy B a C: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> • Kontrolujeme, zda jsou použité prostředky úměrné vysokému stupni ochrany.
Přijatelné řešení: <ul style="list-style-type: none"> • Přístroj je vybaven kontrolním čítačem, který automaticky zaznamenává datum a čas stahování, identifikaci staženého softwaru, identifikaci poskytovatele softwaru a informaci, zda byly všechny kontroly úspěšné. Záznam je proveden i v případě neúspěchu. • Poté, co je kapacita čítače zaplněna, je funkce stahování zablokována, a dokud není porušena plomba a čítač smazán autoritou, není možné stahovat nový software. 		
Dodatek ke třídě rizika E		
Potřebná dokumentace (dodatek k požadavkům pro třídy B a C): Zdrojový kód softwaru, který zajišťuje zaznamenávání stažení.		
Validace (dodatek k požadavkům pro třídy B a C): <i>Kontrola zdrojového kódu:</i> <ul style="list-style-type: none"> • Kontrolujeme, zda jsou prostředky zaznamenávání stažení vhodně zvolené a implementované. • Kontrolujeme, zda jsou prostředky zabezpečení stažení vhodně zvolené a implementované. 		

Třída rizika B	Třída rizika C	Třída rizika D
<p>D5: Souhlas se stažením <i>Příslušnými technickými prostředky musí být zajištěno, že lze stahování provést jen se souhlasem uživatele či majitele měřidla.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> 1. V okamžiku, kdy byl přístroj uveden uživatelem do provozu, je za něj odpovědný uživatel. Výrobce proto nemůže bez explicitního souhlasu uživatele měnit software v přístroji. 2. Technické prostředky, kterými uživatel může dát najevo souhlas se stahováním softwaru, jsou předmětem kontroly z pohledu legální metrologie stejně jako software samotný. 3. Připravenost přístroje ke stahování softwaru musí být deklarována uživatelem/majitelem měřidla. 		
<p>Potřebná dokumentace (dodatek k požadavkům pro třídy B, C a D): Dokumentace musí popisovat prostředky, jimiž je zajišťován souhlas uživatele/majitele se stahováním softwaru.</p>		
<p>Validace (dodatek k požadavkům pro třídy B, C a D): <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, jak je zablokováno stahování, pokud k němu nedal uživatel/majitel měřidla explicitní souhlas. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda je po stažení nové verze softwaru vyžadován souhlas uživatele k dalšímu stahování případných nových verzí. • Kontrolujeme, zda je zabráněno stahování, pokud k němu nedal uživatel souhlas. 		
<p>Přijatelné řešení:</p> <ul style="list-style-type: none"> • Jako prostředek vyjádření souhlasu se stahováním může být použit například přepínač, pokud je to technicky možné (uživatel má přístup k přístroji). • Pro stahování na dálku může být přístroj vybaven zabezpečeným softwarem, pomocí něhož je možné dát souhlas ke stahování. • Souhlas může být omezen jen na jedno stažení (nebo daný počet stažení), případně může souhlas po daném čase vypršet. • Pokud jsou k vyjádření souhlasu použity systémy založené na elektronickém podpisu, veřejný klíč odesílatele musí být součástí softwaru v měřidle. Kontrola klíčů je prováděna automaticky. 		
<p>Dodatek ke třídě rizika E</p>		
<p>Potřebná dokumentace: Zdrojový kód softwaru, který zajišťuje kontrolu souhlasu uživatele se stahováním softwaru.</p>		
<p>Validace: <i>Kontrola zdrojového kódu:</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda jsou prostředky zajištění souhlasu uživatele se stahováním vhodně zvolené a implementované. 		

10 ROZŠÍŘENÍ I: POŽADAVKY NA KONKRÉTNÍ TYPY PŘÍSTROJŮ

Cílem tohoto rozšíření je stanovit dodatečné požadavky na konkrétní typy přístrojů; nemůže tedy nahradit požadavky uvedené v předchozích kapitolách. Je obdobou přístrojově specifických dodatků MI-x ve směrnici MID a rozebírá konkrétní problémy a požadavky pro tyto měřicí přístroje a systémy. Požadavky však nepřesahují rámec směrnice MID, a pokud je v následujícím textu odkazováno na doporučení organizace OIML nebo na normy ISO/IEC, děje se tak pouze v případě, že se jedná o dokumenty v souladu se směrnicí MID.

Kromě již zmíněných dodatečných požadavků obsahuje rozšíření I také přiřazení tříd rizika, aby byla zajištěna harmonizace úrovní zkoušení, ochrany a shody softwaru u jednotlivých typů přístrojů.

V současné době by mělo být rozšíření I považováno za první návrh, který by měl být v budoucnu doplňován jednotlivými technickými komisemi sdružení WELMEC podle aktuálního stavu na poli měřicí techniky. Je to tedy do velké míry otevřená struktura, kostra, která je (až na třídy rizika) jen částečně vyplněná. Číslování kapitol odpovídá jednotlivým přístrojově specifickým dodatkům směrnice MID. Podle zkušeností a rozhodnutí technických komisí WELMEC může být v budoucnosti použita také pro přístroje, které nejsou zahrnuty ve směrnici MID (pro takové přístroje by bylo použito číslování kapitol od 10.11 dále).

Existuje několik aspektů, které musí být brány v potaz u každého typu měřicího přístroje. Jsou systematicky členěny do podkapitol 10.x.y tohoto rozšíření, a to následujícím způsobem:

10.x.1 Specifické normy, standardy a jiné normativní dokumenty

Zde by měly být zmíněny všechny předpisy, standardy a normativní dokumenty (například doporučení OIML) nebo doporučení sdružení WELMEC, které by mohly být užitečné z pohledu vývoje softwaru, a dále požadavky na jeho zkoušení v návaznosti na směrnici MID a její součásti.

Ve většině případů jsou požadavky uvedené v této kapitole **dodatečnými požadavky**, které rozšiřují obecné požadavky uvede-

né v předchozích kapitolách. Pokud některé požadavky nahrazují určité obecné požadavky nebo se některé obecné požadavky na daný typ přístroje nevztahují, musí to zde být zřetelně uvedeno a zdůvodněno.

10.x.2 Technický popis

V tomto odstavci jsou uvedeny následující informace:

- příklady nejčastějších technických konfigurací
- výskyt přístrojů typu P a U
- důležité kontrolní seznamy pro výrobce a pro osoby zkoušející software.

Popis by přitom měl zdůrazňovat zejména:

- měřicí princip (jednotlivá nebo kumulativní měření, statická nebo dynamická metoda, opakovatelnost měření)
- detekce chyb a reakce přístroje na chyby; zde jsou možné dva přístupy:
 - a) chyba může být snadno detekována hardwarovými prostředky,
 - b) chyba nemůže být detekována hardwarovými prostředky, přičemž v druhém případě musí být detekce chyb zajištěna odpovídajícím způsobem na softwarové úrovni.
- v popisu hardwarového uspořádání by měly být zmíněny při nejmenším následující aspekty:
 - a) jedná se o modulární přístroj založený na použití univerzálního počítače, nebo o jednoúčelové zařízení?
 - b) je měřicí zařízení používáno samostatně nebo jako součást uzavřené, či otevřené sítě?
 - c) pokud se jedná o přístroj typu U, je jeho snímač integrální součástí přístroje, nebo může být oddělen?
 - d) je uživatelské rozhraní vždy předmětem kontroly z pohledu legální metrologie, nebo může pracovat i v jiných režimech?
 - e) je měřicí zařízení vybaveno funkcí dlouhodobého uchování dat a jak je tato funkce realizována?
 - f) jakou formu má použité paměťové zařízení (pevné, nebo přenosné)?
- v popisu softwarového uspořádání a popisu prostředí by měly být zmíněny přinejmenším následující aspekty:

- a) jaký operační systém je použit nebo může být použit?
- b) pokud je v souvislosti s provozem měřicího zařízení používán další software, je předmětem kontroly z pohledu legální metrologie?
- c) je součástí systému nějaký software, který by nebyl předmětem kontroly z pohledu legální metrologie, nebo by mohl být volně měněn po typovém schválení?

10.x.3 Požadavky na software

V tomto odstavci by měly být obdobnou formou uvedeny specifické požadavky na software.

10.x.4 Příklady softwaru a dat relevantních z pohledu legální metrologie

V tomto odstavci by měly být uvedeny příklady:

- parametrů typických pro konkrétní typy přístrojů (např. kalibrační parametry)
- parametrů typických pro konkrétní přístroje (určené při typovém schválení)
- funkce přístroje relevantní z pohledu legální metrologie.

10.x.5 Další aspekty

V tomto odstavci mohou být uvedeny například speciální nároky na dokumentaci požadovanou pro zkoušení softwaru, informace, které by měly být uvedeny v certifikátu schválení typu.

10.x.6 Přiřazení tříd rizika

Třídy rizika mohou být přiřazeny buď obecně pro všechny přístroje v dané kategorii, nebo s rozčleněním podle typu využití, typu přístroje či jiných okolností.

10.1 Vodoměry

10.1.1 Specifické normy, standardy a jiné normativní dokumenty

Podle článku 2 směrnice MID mohou členské státy zařadit vodoměry používané v domácnostech, obchodě či lehkém průmyslu mezi měřidla podléhající této směrnici.

Požadavky popsané v tomto odstavci vycházejí pouze z přílohy MI-001 směrnice MID; doporučení a normy organizace OIML nejsou brány v potaz.

10.1.2 Technický popis

10.1.2.1 Hardwarové uspořádání

Vodoměry jsou obvykle uspořádány jako jednoúčelová měřicí zařízení (typ P ve smyslu tohoto dokumentu).

10.1.2.2 Softwarové uspořádání

Softwarové uspořádání se u jednotlivých výrobců liší, předpokládá se však, že vyhovuje doporučením daným v textu tohoto dokumentu.

10.1.2.3 Měřicí princip

Vodoměry průběžně načítají protečený objem vody. Zobrazují celkový protečený objem. Pro jeho měření využívají různé principy.

Měření nemůže být opakováno.

10.1.2.4 Detekce chyb a reakce na ně

Požadavky směrnice MID MI-001 7.2 na chování měřidla při rušení elektromagnetickým polem je třeba interpretovat i ve smyslu softwaru, neboť detekce a reakce na chyby nemůže být prováděna bez součinnosti příslušného softwaru a hardwaru. Z pohledu softwaru navíc není rozhodující, zda bylo rušení elektromagnetické nebo jiného charakteru (např. mechanické); mechanismy reakce na chyby a zotavení z nich jsou vždy stejné.

10.1.3 Požadavky na software

Třída rizika B	Třída rizika C	Třída rizika D
I1-1: Zotavení po chybě		
<i>Software by se měl dokázat zotavit z chyby a vrátit se do běžného provozu.</i>		
Specifikace:		
Potřebná dokumentace:		
Stručný popis mechanismu zotavení a popis impulzu, který tento mechanismus vyvolá.		
Validace:		
<i>Kontrola založená na dokumentaci</i>		
<ul style="list-style-type: none"> • Kontrolujeme, zda je realizace zotavení po chybě přiměřená. 		
<i>Funkční kontrola</i>		
<ul style="list-style-type: none"> • Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
Přijatelné řešení:		
Hardwarově je kontrolován stav mikroprocesoru prostřednictvím samostatné cyklicky běžící funkce. Pokud není některá funkce přístroje dokončena nebo mikroprocesor dokonce uvízne v nekonečné smyčce, hardwarová kontrola po určité době zajistí přiměřené zotavení do normálního stavu.		

Třída rizika B	Třída rizika C	Třída rizika D
I1-2: Prostředky zálohování		
<i>Data relevantní z pohledu legální metrologie, jako jsou měřené hodnoty a stav měření, musí být průběžně zálohována v energeticky nezávislé paměti.</i>		
Specifikace:		
Intervaly zálohování musí být dostatečně malé, aby byl dostatečně malý také rozdíl mezi aktuální a zálohovanou hodnotou.		
Potřebná dokumentace:		
Stručný popis dat, která jsou předmětem zálohování, a situace, kdy toto zálohování nastává. Výpočet maximální chyby, která může nastat u kumulativních hodnot vlivem intervalu zálohování.		

<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda jsou všechna data relevantní z pohledu legální metrologie zálohována v energeticky nezávislé paměti. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu.
<p>Přijatelné řešení: Data relevantní z pohledu legální metrologie jsou průběžně zálohována (například každých 60 minut).</p>

Třída rizika B	Třída rizika C	Třída rizika D
<p>I1-3: MID–Příloha I, 8.5 (zamezit vymazání kumulativních údajů) <i>U přístrojů, které udávají celkové množství daného produktu nebo z jejichž údajů může být toto celkové množství odvozeno (a toto množství je použito v oboru legální metrologie), musí být znemožněno vymazání během provozu.</i></p>		
<p>Specifikace: Kumulativní čítače měřidla mohou být resetovány před uvedením do provozu.</p>		
<p>Potřebná dokumentace: Dokumentace prostředků ochrany proti resetování čítače celkového objemu.</p>		
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda nemohou být kumulativní čítače resetovány, aniž je to patrné. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
<p>Přijatelné řešení: Kumulativní čítače jsou chráněny stejnými prostředky jako parametry přístroje (viz P7).</p>		

Třída rizika B	Třída rizika C	Třída rizika D
I1-4: Dynamické chování <i>Software, který není předmětem kontroly z pohledu legální metrologie, nesmí narušit dynamiku měřicího procesu.</i>		
Specifikace: <ul style="list-style-type: none"> Tento požadavek je doplňkem k požadavkům S, je-li realizováno oddělení softwaru v souladu s rozšířením S. Smyslem tohoto požadavku je zajistit, že software, který není předmětem kontroly z pohledu legální metrologie, nevyužívá takové množství hardwarových zdrojů, které by vedlo k narušení funkce softwaru, jenž je předmětem kontroly z pohledu legální metrologie. 		
Potřebná dokumentace: <ul style="list-style-type: none"> Popis hierarchie přerušení Schéma časování jednotlivých softwarových úkolů. Limity a poměrné časy pro části, které nejsou předmětem kontroly z pohledu legální metrologie. 		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Popis limitů a poměrného času stanovených pro části, které nejsou předmětem kontroly z pohledu legální metrologie. <i>Funkční kontrola</i> <ul style="list-style-type: none"> Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
Přijatelné řešení: Hierarchie přerušení je taková, že přístroj splňuje tento požadavek.		

10.1.4 Příklady softwaru a dat relevantních z pohledu legální metrologie

Vodoměry využívají řadu parametrů, například konstanty pro přepočty a konfiguraci vodoměru nebo parametry nezbytné pro samotný chod přístroje. Z pohledu jejich rozčlenění a zabezpečení je možné využít odstavce P2 až P9 tohoto dokumentu.

V následující tabulce jsou uvedeny typické parametry vodoměru (tabulka bude doplněna po jednání technické komise WELMEC WG 11).

parametr	chráněný	nastavitelný	poznámka
kalibrační faktor	x		
linearizační faktor	x		

10.1.5 Další aspekty

Pro využití v domácnostech nepředpokládáme stahování softwaru (rozšíření D, kapitola 9).

Kumulování objemu nebo energie při použití v domácnostech není považováno za dlouhodobé uchovávání dat ve smyslu rozšíření L, kapitoly 6 tohoto dokumentu. Pokud přístroj měří pouze kumulované množství vody nebo kumulovanou energii, není nutné toto rozšíření brát v potaz.

10.1.6 Přiřazení tříd rizika

Podle rozhodnutí technické komise WELMEC WG 11 (3/4. 3. 2005) byly stanoveny následující třídy rizika pro účely zkoušení vodoměrů vybavených softwarem:

- třída rizika C pro všechny přístroje typu P.

Rozhodnutí není definitivní a bude ještě předmětem diskusí stejně jako stanovení tříd rizika pro vodoměry typu U.

10.2 Plynoměry a přepočítávače

10.2.1 Specifické normy, standardy a jiné normativní dokumenty

Podle článku 2 směrnice MID mohou členské státy zařadit plynoměry a přepočítávače množství plynu používané v domácnostech, obchodě či lehkém průmyslu mezi měřidla podléhající této směrnici.

Požadavky popsané v tomto odstavci vycházejí pouze z přílohy MI-002 směrnice MID; doporučení a normy organizace OIML nejsou brány v potaz.

10.2.2 Technický popis

10.2.2.1 Hardwarové uspořádání

Plynoměry a přepočítávače objemu jsou obvykle uspořádány jako jednoúčelová měřicí zařízení (typ P ve smyslu tohoto dokumentu). Mohou mít jeden či více vstupů pro externí snímače. Měřidlo a přepočítávač mohou být odděleny.

10.2.2.2 Softwarové uspořádání

Softwarové uspořádání se u jednotlivých výrobců liší, předpokládá se však, že vyhovuje doporučením daným v textu tohoto dokumentu.

10.2.2.3 Měřicí princip

Plynoměry průběžně načítají proteklý objem plynu. Zobrazují celkový proteklý objem. Pro jeho měření využívají různé principy. Přepočítávače provádějí přepočet na referenční podmínky a mohou být integrální součástí plynoměru.

Měření proteklého objemu nemůže být opakováno.

10.2.2.4 Detekce chyb a reakce na ně

Požadavky směrnice MID MI-002 4.3.1 na chování měřidla při rušení elektromagnetickým polem je třeba interpretovat i ve smyslu softwaru, neboť detekce a reakce na chyby nemůže být prováděna bez součinnosti příslušného softwaru a hardwaru. Z pohledu softwaru navíc není rozhodující, zda bylo rušení elektromagnetické nebo jiného principu (např. mechanické); mechanismy reakce na chyby a zotavení z nich jsou vždy stejné.

10.2.3 Požadavky na software

Třída rizika B	Třída rizika C	Třída rizika D
I2-1: Zotavení po chybě		
<i>Software by se měl dokázat zotavit z chyby a vrátit se do běžného provozu.</i>		
Specifikace:		
Potřebná dokumentace:		
Stručný popis mechanismu zotavení a popis situace, kdy je tento mechanismus vyvolán.		
Validace:		
<i>Kontrola založená na dokumentaci</i>		
<ul style="list-style-type: none"> Kontrolujeme, zda je realizace zotavení po chybě přiměřená. 		
<i>Funkční kontrola</i>		
<ul style="list-style-type: none"> Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
Přijatelné řešení:		
Hardwarově je kontrolován stav mikroprocesoru prostřednictvím samostatné cyklicky běžící funkce. Pokud není některá funkce přístroje dokončena nebo mikroprocesor dokonce uvízne v nekonečné smyčce, hardwarová kontrola po určité době zajistí přiměřené zotavení do normálního stavu.		

Třída rizika B	Třída rizika C	Třída rizika D
I2-2: Prostředky zálohování		
<i>Data relevantní z pohledu legální metrologie, jako jsou měřené hodnoty a stav měření, musí být průběžně zálohována v energeticky nezávislé paměti.</i>		
Specifikace: Intervaly zálohování musí být dostatečně malé, aby byl dostatečně malý také rozdíl mezi aktuální a zálohovanou hodnotou.		
Potřebná dokumentace: Stručný popis dat, která jsou předmětem zálohování, a situace, kdy toto zálohování nastává. Výpočet maximální chyby, která může nastat u kumulativních hodnot vlivem intervalu zálohování.		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda jsou všechna data relevantní z pohledu legální metrologie zálohována v energeticky nezávislé paměti. <i>Funkční kontrola</i> <ul style="list-style-type: none"> Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
Přijatelné řešení: Data relevantní z pohledu legální metrologie jsou průběžně zálohována (například každých 60 minut).		

Třída rizika B	Třída rizika C	Třída rizika D
I2-3: Indikace		
<i>Zobrazení celkového nepřepočteného objemu musí mít dostatečné množství číslic, tak aby odpovídaly alespoň 8 000 hodinám provozu při maximálním průtoku.</i>		
Specifikace: <i>Potřebná dokumentace:</i> Dokumentace popisující vnitřní reprezentaci čítače objemu.		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda je kapacita paměti dostatečná. 		
Přijatelné řešení: Typická hodnota maximálního průtoku pro bytový plynoměr je 6 m ³ /h. Požadovaný rozsah je 48 000 m ³ (soudobé plynoměry jsou běžně schopné zobrazit 99 999 m ³).		

Třída rizika B	Třída rizika C	Třída rizika D
I2-4: MID–Příloha I, 8.5 (zamezit resetování kumulativních údajů)		
<i>U přístrojů, které udávají celkové množství daného produktu nebo z jejichž údajů může být toto celkové množství odvozeno (a toto množství je použito v oboru legální metrologie), musí být znemožněno resetování během provozu.</i>		
Specifikace: Kumulativní čítače měřidla mohou být resetovány před uvedením do provozu.		
Potřebná dokumentace: Dokumentace prostředků ochrany proti resetování čítače celkového objemu.		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda nemohou být kumulativní čítače resetovány, aniž je to patrné. <i>Funkční kontrola</i> <ul style="list-style-type: none"> Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
Přijatelné řešení: Kumulativní čítače jsou chráněny stejnými prostředky jako parametry přístroje (viz P7).		

Třída rizika B	Třída rizika C	Třída rizika D
I2-5: MI-002, 5.2 (doba životnosti zdroje)		
<i>Určený zdroj napájení musí mít životnost nejméně pět let. Po uplynutí 90 % jeho životnosti musí být zobrazeno varovné hlášení.</i>		
Specifikace: Životností je zde míněna kapacita dostupné energie. Pokud je možné vyměnit zdroj v místě instalace, nesmí být jeho výměnou narušeny data a parametry, které jsou relevantní z pohledu legální metrologie.		
Potřebná dokumentace: Popis zdroje a jeho kapacity, maximální životnosti (nezávisle na odběru), popis prostředků měření zbývající kapacity a prostředků vyvolávajících varování při nedostatečné kapacitě energie ve zdroji.		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda je kontrola dostupnosti dostatečné kapacity zdroje přiměřená. 		
Přijatelné řešení: Celková doba provozu je načítána do energeticky nezávislé paměti a porovnávána s nominální životností baterie. Poté, co uplyne 90 % z doby životnosti baterie, je zobrazeno varování. Přístroj detekuje výměnu baterie a resetuje čítač.		

Třída rizika B	Třída rizika C	Třída rizika D
I2-6: MI-002, 9.1 (Elektronické přepočítávače) <i>Elektronický přepočítávač musí být schopen poznat, kdy pracuje mimo povolené rozsahy pracovních podmínek a mezních hodnot proměnných. V takovém případě musí zastavit načítání integrované hodnoty, případně může načítat tuto hodnotu do samostatné proměnné po celou dobu, kdy se nachází v takovém stavu.</i>		
Specifikace: Chybový stav musí být indikován na displeji.		
Potřebná dokumentace: Popis čítačů pro měření objemu a objemu v chybovém režimu.		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda je chybový stav správně ošetřen. 		
Přijatelné řešení: Software sleduje všechny vstupy a kontroluje, zda jsou v předepsaných mezích. Pokud ano, výsledná hodnota objemu je integrována do čítače celkového proteklého objemu. Pokud ne, je načítána jinam. Další možností je použít jen jeden čítač, ale zaznamenávat, kdy nastaly chybové stavy (jejich začátek a konec). Uživatel musí mít schopnost oba údaje číst a během měření sledovat, zda přístroj pracuje v normálním nebo chybovém režimu.		

Třída rizika B	Třída rizika C	Třída rizika D
I2-7: MI-002, 5.5 (Testovací prvek): <i>Plynoměr musí být vybaven testovacím prvkem, který umožní vykonávat dlouhodobé zkoušky v rozumném čase.</i>		
Specifikace: Testovací prvek zrychlující načítání je obvykle používán pro zkoušky před instalací měřidla. Během testovacího režimu musí být všechny čítače používány stejně jako v běžném režimu.		
Potřebná dokumentace: Popis testovacího prvku a nastavování testovacího režimu.		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda je možné pomocí testovacího prvku provést dlouhodobé zkoušky. 		

Přijatelné řešení: Časová základna vnitřních hodin může být zrychlena. Procesy vedoucí k možnému přetečení čítače, které jinak trvají týdny, měsíce či roky, tak mohou proběhnout v minutách či hodinách.		
Třída rizika B	Třída rizika C	Třída rizika D
I2-8: Dynamické chování <i>Software, který není předmětem kontroly z pohledu legální metrologie, nesmí narušit dynamiku měřicího procesu.</i>		
Specifikace: <ul style="list-style-type: none"> Tento požadavek je doplňkem k požadavkům S, je-li realizováno oddělení softwaru v souladu s rozšířením S. Smyslem tohoto požadavku je zajistit, že software, který není předmětem kontroly z pohledu legální metrologie, nevyužívá takové množství hardwarových zdrojů, které by vedlo k narušení funkce softwaru, jež je předmětem kontroly z pohledu legální metrologie. 		
Potřebná dokumentace: <ul style="list-style-type: none"> Popis hierarchie přerušení. Schéma časování jednotlivých softwarových úkolů. Limity a poměrné časy pro části, které nejsou předmětem kontroly z pohledu legální metrologie. 		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Popis limitů a poměrného času, stanovených pro části, které nejsou předmětem kontroly z pohledu legální metrologie. <i>Funkční kontrola</i> <ul style="list-style-type: none"> Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
Přijatelné řešení: Hierarchie přerušení je taková, že přístroj splňuje tento požadavek.		

10.2.4 Příklady softwaru a dat relevantních z pohledu legální metrologie

Plynoměry a přepočítávače objemu využívají řadu parametrů, například konstanty pro přepočty a konfiguraci přístroje nebo parametry nezbytné pro samotný chod přístroje. Z pohledu jejich rozčlenění a zabezpečení je možné využít odstavce P2 až P9 tohoto dokumentu.

V následující tabulce jsou uvedeny typické parametry plynomě-
rů a přepočítávačů objemu (tabulka bude doplněna po jednání
technické komise WELMEC WG 11).

parametr	chráněný	nastavitelný	poznámka
kalibrační faktor	x		
linearizační faktor	x		

10.2.5 Další aspekty

Pro využití v domácnostech nepředpokládáme stahování softwaru (rozšíření D, kapitola 9).

Kumulování objemu nebo energie při použití v domácnostech není považováno za dlouhodobé uchovávání dat ve smyslu rozšíření L kapitoly 6 tohoto dokumentu. Pokud přístroj měří pouze kumulované množství plynu nebo kumulovanou energii, není nutné toto rozšíření brát v potaz.

10.2.6 Přiřazení tříd rizika

Podle rozhodnutí technické komise WELMEC WG 11 (3/4. 3. 2005) byly stanoveny následující třídy rizika pro účely zkoušení plynoměrů a přepočítávačů objemu vybavených softwarem:

- třída rizika C pro všechny přístroje typu P.

Rozhodnutí není definitivní a bude ještě předmětem diskusí stejně jako stanovení tříd rizika pro plynoměry a přepočítávače objemu typu U.

Komise WG 11 považuje funkci předplacení a intervalového měření za funkci dodatečnou k základním měřicím funkcím popsaným v doplňku MI-002; pokud je přístroj těmito funkcemi vybaven, není tedy nutné stanovovat vyšší třídu rizika. V každém případě však musí být kontrolována základní měřicí funkce, aby bylo možné dokázat, že software, který zajišťuje tyto dodatečné funkce, nemá vliv na měření samotné.

10.3 Elektroměry pro měření činné energie

10.3.1 Specifické normy, standardy a jiné normativní dokumenty

Podle článku 2 směrnice MID mohou členské státy zařadit elektroměry pro měření činné energie (v tomto dokumentu dále jen „aktivní elektroměry“) používané v domácnostech, obchodě či lehkém průmyslu mezi měřidla podléhající této směrnici.

Požadavky popsané v tomto odstavci vycházejí pouze z přílohy MI-003 směrnice MID; doporučení a normy organizace OIML nebo normy IEC nejsou brány v potaz.

10.3.2 Technický popis

Aktivní elektroměry využívají měření napětí a proudu pro stanovení výkonu a tento výkon integrují v čase pro stanovení celkového množství elektrické energie.

10.3.2.1 Hardwarové uspořádání

Aktivní elektroměry jsou obvykle uspořádány jako jednoúčelová měřicí zařízení (typ P ve smyslu tohoto dokumentu). Mohou mít jeden či více vstupů a mohou být použity spolu s externími transformátory.

10.3.2.2 Softwarové uspořádání

Softwarové uspořádání se u jednotlivých výrobců liší, předpokládá se však, že vyhovuje doporučením daným v textu tohoto dokumentu.

10.3.2.3 Měřicí princip

Aktivní elektroměry průběžně načítají výkon spotřebovaný v daném elektrickém obvodu. Na přístroji je zobrazeno celkové množství elektrické energie. Pro měření se využívají různé typy a principy převodníků.

Měření energie nemůže být opakováno.

10.3.2.4 Detekce chyb a reakce na ně

Požadavky směrnice MID MI-003 4.3.1 na chování měřidla při rušení elektromagnetickým polem je třeba interpretovat i ve smyslu softwaru, neboť detekce a reakce na chyby nemůže být prováděna bez součinnosti příslušného softwaru a hardwaru. Z pohledu softwaru navíc není rozhodující, zda bylo rušení elektromagnetické nebo jiného charakteru (např. mechanické); mechanismy reakce na chyby a zotavení z nich jsou vždy stejné.

10.3.3 Požadavky na software

Třída rizika B	Třída rizika C	Třída rizika D
I3-1: Zotavení po chybě		
<i>Software by se měl dokázat zotavit z chyby a vrátit se do běžného provozu.</i>		
Specifikace:		
Potřebná dokumentace: Stručný popis mechanismu zotavení a popis situace, kdy je tento mechanismus vyvolán.		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> • Kontrolujeme, zda je realizace zotavení po chybě přiměřená. <i>Funkční kontrola</i> <ul style="list-style-type: none"> • Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
Přijatelné řešení: Hardwarově je kontrolován stav mikroprocesoru prostřednictvím samostatné cyklicky běžící funkce. Pokud není některá funkce přístroje dokončena nebo mikroprocesor dokonce uvízne v nekonečné smyčce, hardwarová kontrola po určité době zajistí přiměřené zotavení do normálního stavu.		

Třída rizika B	Třída rizika C	Třída rizika D
I3-2: Prostředky zálohování		
<i>Data relevantní z pohledu legální metrologie, jako jsou měřené hodnoty a stav měření, musí být průběžně zálohována v energeticky nezávislé paměti.</i>		
Specifikace: Intervaly zálohování musí být dostatečně malé, aby byl dostatečně malý také rozdíl mezi aktuální a zálohovanou hodnotou.		
Potřebná dokumentace: Stručný popis dat, která jsou předmětem zálohování, a situace, kdy toto zálohování nastává. Výpočet maximální chyby, která může nastat u kumulativních hodnot vlivem intervalu zálohování.		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> • Kontrolujeme, zda jsou všechna data relevantní z pohledu legální metrologie zálohována v energeticky nezávislé paměti. <i>Funkční kontrola</i> <ul style="list-style-type: none"> • Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		

Přijatelné řešení:

Data relevantní z pohledu legální metrologie jsou průběžně zálohována (například každých 60 minut).

Třída rizika B	Třída rizika C	Třída rizika D
I3-3: MI-003, 5.2 Indikace		
<i>Zobrazení celkové energie musí mít dostatečné množství číslic, tak aby odpovídaly alespoň 4 000 hodinám provozu při maximálním zatížení ($I = I_{max}$, $U = U_{rf}$, $PF = 1$).</i>		
Specifikace:		
Potřebná dokumentace:		
Dokumentace popisující vnitřní reprezentaci čítače energie a pomocných proměnných.		
Validace:		
<i>Kontrola založená na dokumentaci</i>		
<ul style="list-style-type: none"> Kontrolujeme, zda je kapacita paměti dostatečná. 		
<i>Přijatelné řešení:</i>		
Typická hodnota pro třífázový elektroměr je $P_{max} (4\ 000\ h) = 3 \cdot 60\ A \cdot 230\ V \cdot 4\ 000\ h = 165\ 600\ kWh$. To odpovídá ve vnitřní reprezentaci 4 bytům.		

Třída rizika B	Třída rizika C	Třída rizika D
I3-4: MID–Příloha I, 8.5 (zamezit resetování kumulativních údajů)		
<i>U přístrojů, které udávají celkové množství daného produktu nebo z jejichž údajů může být toto celkové množství odvozeno (a toto množství je použito v oboru legální metrologie), musí být znemožněno resetování během provozu.</i>		
Specifikace:		
Kumulativní čítače měřidla mohou být resetovány před uvedením do provozu.		
<i>Potřebná dokumentace:</i>		
Dokumentace prostředků ochrany proti resetování čítače celkové energie.		
Validace:		
<i>Kontrola založená na dokumentaci</i>		
<ul style="list-style-type: none"> Kontrolujeme, zda nemohou být kumulativní čítače resetovány, aniž je to patrné. 		
<i>Funkční kontrola</i>		
<ul style="list-style-type: none"> Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		

Přijatelné řešení:

Kumulativní čítače jsou chráněny stejnými prostředky jako parametry přístroje (viz P7).

Třída rizika B	Třída rizika C	Třída rizika D
I3-5: Dynamické chování		
<i>Software, který není předmětem kontroly z pohledu legální metrologie, nesmí narušit dynamiku měřicího procesu.</i>		
Specifikace:		
<ul style="list-style-type: none"> Tento požadavek je doplňkem k požadavkům S, je-li realizováno oddělení softwaru v souladu s rozšířením S. Smyslem tohoto požadavku je zajistit, že software, který není předmětem kontroly z pohledu legální metrologie, nevyužívá takové množství hardwarových zdrojů, které by vedlo k narušení funkce softwaru, který je předmětem kontroly z pohledu legální metrologie. 		
Potřebná dokumentace:		
<ul style="list-style-type: none"> Popis hierarchie přerušení. Schéma časování jednotlivých softwarových úkolů. Limity a poměrné časy pro části, které nejsou předmětem kontroly z pohledu legální metrologie. 		
Validace:		
<i>Kontrola založená na dokumentaci</i>		
<ul style="list-style-type: none"> Popis limitů a poměrného času, které jsou stanoveny pro části, které nejsou předmětem kontroly z pohledu legální metrologie. 		
<i>Funkční kontrola</i>		
<ul style="list-style-type: none"> Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
Přijatelné řešení:		
Hierarchie přerušení je taková, že vylučuje vlivy.		

10.3.4 Příklady softwaru a dat relevantních z pohledu legální metrologie

Aktivní elektroměry využívají řadu parametrů, například konstanty pro přepočty a konfiguraci přístroje nebo parametry nezbytné pro samotný chod přístroje. Z pohledu jejich rozčlenění a zabezpečení je možné využít odstavce P2 až P9 tohoto dokumentu.

V následující tabulce jsou uvedeny typické parametry aktivních elektroměrů (tabulka bude doplněna po jednání technické komise WELMEC WG 11)

parametr	chráněný	nastavitelný	poznámka
kalibrační faktor	x		
linearizační faktor	x		

10.3.5 Další aspekty

Pro využití v domácnostech nepředpokládáme stahování softwaru (rozšíření D, kapitola 9).

Registry pro kumulování energie či objemu při použití v domácnostech nejsou považovány za dlouhodobé uchovávání dat ve smyslu rozšíření L kapitoly 6 tohoto dokumentu. Pokud přístroj měří pouze kumulovanou energii, není nutné brát toto rozšíření v potaz.

10.3.6 Přiřazení tříd rizika

Podle rozhodnutí technické komise WELMEC WG 11 (3/4. 3. 2005) byly stanoveny následující třídy rizika pro účely zkoušení aktivních elektroměrů vybavených softwarem:

- **třída rizika C pro všechny přístroje typu P.**

Rozhodnutí není definitivní a bude ještě předmětem diskusí stejně jako stanovení tříd rizika pro aktivní elektroměry typu U.

Komise WG 11 považuje funkci předplacení a intervalového měření za funkci dodatečnou k základním měřicím funkcím popsaným v doplňku MI-002, v případě, že je přístroj těmito funkcemi vybaven, není tedy nutné stanovovat vyšší třídu rizika. V každém případě však musí být kontrolována základní měřicí funkce, aby bylo možné dokázat, že software, který zajišťuje tyto dodatečné funkce, nemá vliv na měření samotné.

10.4 Měřiče tepla

10.4.1 Specifické normy, standardy a jiné normativní dokumenty

Podle článku 2 směrnice MID mohou členské státy zařadit měřiče tepla používané v domácnostech, obchodě či lehkém průmyslu mezi měřidla podléhající této směrnici.

Požadavky popsané v tomto odstavci vycházejí pouze z přílohy MI-004 směrnice MID; doporučení a normy organizace OIML nejsou brány v potaz.

10.4.2 Technický popis

10.4.2.1 Hardwarové uspořádání

Měřiče tepla jsou obvykle uspořádány jako jednoúčelová měřicí zařízení (typ P ve smyslu tohoto dokumentu). Může se jednat o samostatný přístroj nebo o kombinaci více komponentů, jako jsou snímač průtoku, dvojice snímačů teploty a přepočítávací jednotka podle odstavce 4(b) směrnice MID.

10.4.2.2 Softwarové uspořádání

Softwarové uspořádání se u jednotlivých výrobců liší, předpokládá se však, že vyhovuje doporučením daným v textu tohoto dokumentu.

10.4.2.3 Měřicí princip

Měřiče tepla průběžně načítají energii spotřebovanou v daném obvodu. Na přístroji je zobrazeno celkové množství tepelné energie. Pro měření se využívají různé typy a principy převodníků.

Měření energie nemůže být opakováno.

10.4.2.4 Detekce chyb a reakce na ně

Požadavky směrnice MID MI-004 4.3.1 na chování měřidla při rušení elektromagnetickým polem je třeba interpretovat i ve smyslu softwaru, neboť detekce a reakce na chyby nemůže být prováděna bez součinnosti příslušného softwaru a hardwaru. Z pohledu softwaru navíc není rozhodující, zda bylo rušení elektromagnetické nebo jiného charakteru (např. mechanické); mechanismy reakce na chyby a zotavení z nich jsou vždy stejné.

10.4.3 Požadavky na software

Třída rizika B	Třída rizika C	Třída rizika D
I4-1: Zotavení po chybě		
<i>Software by se měl dokázat zotavit z chyby a vrátit se do běžného provozu.</i>		
Specifikace:		
Potřebná dokumentace:		
Stručný popis mechanismu zotavení a popis situace, kdy je tento mechanismus vyvolán.		
Validace:		
<i>Kontrola založená na dokumentaci</i>		
<ul style="list-style-type: none"> • Kontrolujeme, zda je realizace zotavení po chybě přiměřená. 		
<i>Funkční kontrola</i>		
<ul style="list-style-type: none"> • Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
Přijatelné řešení:		
Hardwarově je kontrolován stav mikroprocesoru prostřednictvím samostatné cyklicky běžící funkce. Pokud není některá funkce přístroje dokončena nebo mikroprocesor dokonce uvízne v nekonečné smyčce, hardwarová kontrola po určité době zajistí přiměřené zotavení do normálního stavu.		

Třída rizika B	Třída rizika C	Třída rizika D
I4-2: Prostředky zálohování		
<i>Data relevantní z pohledu legální metrologie, jako jsou měřené hodnoty a stav měření, musí být průběžně zálohována v energeticky nezávislé paměti.</i>		
Specifikace:		
Intervaly zálohování musí být dostatečně malé, aby byl dostatečně malý také rozdíl mezi aktuální a zálohovanou hodnotou.		
Potřebná dokumentace:		
Stručný popis dat, která jsou předmětem zálohování, a situace, kdy k tomuto zálohování dochází. Výpočet maximální chyby, která může nastat u kumulativních hodnot vlivem intervalu zálohování.		
Validace:		
<i>Kontrola založená na dokumentaci</i>		
<ul style="list-style-type: none"> • Kontrolujeme, zda jsou všechna data relevantní z pohledu legální metrologie zálohována v energeticky nezávislé paměti. 		
<i>Funkční kontrola</i>		
<ul style="list-style-type: none"> • Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		

Přijatelné řešení:

Data relevantní z pohledu legální metrologie jsou průběžně zálohována (například každých 60 minut).

Třída rizika B	Třída rizika C	Třída rizika D
I4-3: MID–Příloha I, 8.5 (zamezit resetování kumulativních údajů) <i>U přístrojů, které udávají celkové množství daného produktu nebo z jejichž údajů může být toto celkové množství odvozeno (a toto množství je použito v oboru legální metrologie), musí být znemožněno resetování během provozu.</i>		
Specifikace: Kumulativní čítače měřidla mohou být resetovány před uvedením do provozu.		
Potřebná dokumentace: Dokumentace prostředků ochrany proti resetování čítače celkového objemu.		
Validace: <i>Kontrola založená na dokumentaci</i> <ul style="list-style-type: none"> Kontrolujeme, zda nemohou být kumulativní čítače resetovány, aniž je to patrné. <i>Funkční kontrola</i> <ul style="list-style-type: none"> Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
Přijatelné řešení: Kumulativní čítače jsou chráněny stejnými prostředky jako parametry přístroje (viz P7).		

Třída rizika B	Třída rizika C	Třída rizika D
I4-4: Dynamické chování <i>Software, který není předmětem kontroly z pohledu legální metrologie, nesmí narušit dynamiku měřicího procesu.</i>		

<p>Specifikace:</p> <ul style="list-style-type: none"> • Tento požadavek je doplňkem k požadavkům S, je-li realizováno oddělení softwaru v souladu s rozšířením S. • Smyslem tohoto požadavku je zajistit, že software, který není předmětem kontroly z pohledu legální metrologie, nevyužívá takové množství hardwarových zdrojů, které by vedlo k narušení funkce softwaru, který je předmětem kontroly z pohledu legální metrologie.
<p>Potřebná dokumentace:</p> <ul style="list-style-type: none"> • Popis hierarchie přerušení • Schéma časování jednotlivých softwarových úkolů. Limity a poměrné časy pro části, které nejsou předmětem kontroly z pohledu legální metrologie.
<p>Validace:</p> <p><i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Popis limitů a poměrného času stanovených pro části, které nejsou předmětem kontroly z pohledu legální metrologie. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu.
<p>Přijatelné řešení:</p> <p>Hierarchie přerušení je taková, že přístroj splňuje tento požadavek.</p>

10.4.4 Příklady softwaru a dat relevantních z pohledu legální metrologie

Měřiče tepla využívají řadu parametrů, například konstanty pro přepočty a konfiguraci přístroje nebo parametry nezbytné pro samotný chod přístroje. Z pohledu jejich rozčlenění a zabezpečení je možné využít odstavce P2 až P9 tohoto dokumentu.

V následující tabulce jsou uvedeny typické parametry měřiče tepla (tabulka bude doplněna po jednání technické komise WELMEC WG 11).

parametr	chráněný	nastavitelný	poznámka
kalibrační faktor	x		
linearizační faktor	x		

10.4.5 Další aspekty

Pro využití v domácnostech nepředpokládáme stahování softwaru (rozšíření D, kapitola 9).

Kumulování energie při použití v domácnostech není považováno za dlouhodobé uchovávání dat ve smyslu rozšíření L, kapitoly 6 tohoto dokumentu. Pokud přístroj měří pouze kumulovanou energii, není nutné toto rozšíření brát v potaz.

10.4.6 Přiřazení tříd rizika

Podle rozhodnutí technické komise WELMEC WG 11 (3/4. 3. 2005) byly stanoveny následující třídy rizika pro účely zkoušení měřičů tepla vybavených softwarem:

- **třída rizika C pro všechny přístroje typu P.**

Rozhodnutí není definitivní a bude ještě předmětem diskusí, stejně jako stanovení tříd rizika pro měřiče tepla typu U.

10.5 Měřicí systémy na kapaliny jiné než voda

Měřicí systémy na kontinuální a dynamické měření kapalin jiných než voda jsou předmětem regulace ve smyslu směrnice MID. Požadavky specifické pro tyto typy měřicích přístrojů jsou uvedeny v dodatku MI-005, nebyly však brány v potaz, stejně jako nebyly brány v potaz ani žádné další normy.

Odstavce 10.5.1–10.5.5 budou v případě nutnosti doplněny v budoucnosti.

10.5.6 Přiřazení tříd rizika

Podle výsledku dotazníku skupiny WELMEC WG 7 (2004) byly stanoveny následující třídy rizika pro účely zkoušení měřicích systémů na kapaliny jiné než voda vybavených softwarem:

- **třída rizika B pro přístroje typu P nekritických typů a v nekritických aplikacích**
- **třída rizika C pro přístroje typu P kritických typů nebo v kritických aplikacích**
- **třída rizika C pro přístroje typu U nekritických typů a v nekritických aplikacích**
- **třída rizika D pro přístroje typu U kritických typů nebo v kritických aplikacích.**

Rozhodnutí není definitivní a bude ještě předmětem diskusí příslušné technické komise sdružení WELMEC. Tato komise bude zároveň definovat kritické a nekritické aplikace a typy.

10.6 Vážicí zařízení

Vážicí zařízení dělíme do dvou kategorií:

1. neautomatické váhy (NAWI),
2. automatické váhy (AWI),

příčemž AWI spadají pod regulaci směrnice MID, zatímco NAWI se řídí evropskou směrnicí 90/384/EEC. *Tento dokument se proto týká pouze automatických vah; pro neautomatické váhy je nutné použít dokument WELMEC 2.3.*

Specifické požadavky uvedené v této kapitole jsou založeny na příloze MI-006 a normativních dokumentech uvedených v odstavci 10.6.1, jsou-li tyto dokumenty v souladu se směrnicí MID.

10.6.1 Specifické normy, standardy a jiné normativní dokumenty

Směrnicí MID je regulováno celkem 5 různých typů vážicích zařízení s automatickou činností

- automatické detektory přetížení (R51)
- automatické gravimetrické plničky (61)
- nespojité totalizéry (R107)
- spojité totalizéry (pásové váhy) (R50)
- automatické mostní železniční váhy (R106)

V závorkách jsou přitom uvedena příslušná doporučení sdružení OIML, která jsou normativními dokumenty ve smyslu směrnice MID. Kromě toho byl pro testování detektorů přetížení vydán dokument WELMEC Guide 2.6.

Dále existuje jeden typ automatických vah, který nespadá pod regulaci směrnice MID

- automatické dynamické silniční váhy.

Všechny typy vah mohou být konstruovány jako oba základní typy měřidel, tj. P i U, a u všech připadají v úvahu všechna rozšíření uvedená v tomto dokumentu. Nicméně pouze pro **totalizéry** je nezbytné uvést v tomto dokumentu typově specifické požadavky na software, a to proto, že tyto přístroje měří dlouhodobě a jejich měření nemohou být opakována.

10.6.2 Technický popis

10.6.2.1 Hardwarové uspořádání

Nespojitý totalizér je násypková váha, které měří hmotnost objemového produktu (například obilí) takovým způsobem, že jej dělí na diskrétní části. Skládá se většinou z jedné či více násypky umístěných na senzorech, přídatné elektroniky a zobrazovací jednotky.

Spojité totalizér je pásová váha, u které se produkt posouvá na pásu přes senzor. Skládá se většinou z pásového dopravníku, senzorů, přídatné elektroniky a zobrazovací jednotky. Napětí pásu je možné nastavovat.

10.6.2.2 Softwarové uspořádání

Výrobce je povinen splňovat požadavky dané v textu tohoto dokumentu.

10.6.2.3 Měřicí princip

V případě použití nespojitého totalizéru je produkt postupně vkládán (sypán) do násypky a vážen, přičemž se vyhodnocuje celkové vážené množství.

V případě použití spojitého totalizéru je hmotnost produktu měřena průběžně, zatímco se posouvá přes měřicí senzor. Měření probíhá v pravidelných intervalech, jejichž perioda závisí na rychlosti pohybu pásu a aktuální měřené hmotnosti. Pás se přitom nezastavuje ani produkt se nijak nedělí a výsledek se vypočítá integrací.

10.6.2.4 Detekce chyb a reakce na ně

Klouby dopravníku mohou způsobovat rázové jevy, které mohou negativně ovlivnit měření, zejména při nulování. U nespojitého totalizéru může dojít ke ztrátě některé hodnoty před jejím přičtením do celkové sumy.

10.6.3 Požadavky na software

Požadavky směrnice MID MI-006 na chování měřidla při rušení elektromagnetickým polem je třeba interpretovat i ve smyslu softwaru, neboť detekce a reakce na chyby nemůže být prováděna bez součinnosti příslušného softwaru a hardwaru. Z pohledu softwaru

navíc není rozhodující, zda bylo ručení elektromagnetické nebo jiného principu (např. mechanické); mechanismy reakce na chyby a zotavení z nich jsou vždy stejné.

Třída rizika B	Třída rizika C	Třída rizika D
I6-1: Detekce chyby		
<i>Software by měl dokázat detekovat vybočení z normálního provozu.</i>		
Specifikace:		
Je-li detekována chyba, proběhnou následující operace:		
b) Kumulativní měření a související relevantní data jsou automaticky uložena do energeticky nezávislé paměti.		
c) Pás či násypka musí být automaticky zastavena nebo musí být dán zřetelný signál.		
Potřebná dokumentace:		
Stručný popis mechanismu zotavení a popis situace, kdy je tento mechanismus vyvolán.		
Validace:		
<i>Kontrola založená na dokumentaci</i>		
<ul style="list-style-type: none"> • Kontrolujeme, zda je realizace zotavení po chybě přiměřená. 		
<i>Funkční kontrola</i>		
<ul style="list-style-type: none"> • Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
Přijatelné řešení:		
Hardwarově je kontrolován stav mikroprocesoru prostřednictvím samostatné cyklicky běžící funkce. Pokud není některá funkce přístroje dokončena nebo mikroprocesor dokonce uvízne v nekonečné smyčce, hardwarová kontrola po určité době zajistí přiměřené zotavení do normálního stavu.		

Třída rizika B	Třída rizika C	Třída rizika D
I6-2: Prostředky zálohování		
<i>Data relevantní z pohledu legální metrologie, jako jsou měřené hodnoty a stav měření, musí být průběžně zálohována v energeticky nezávislé paměti.</i>		
Specifikace:		
a) Stavové proměnné a podstatná data musí být uloženy v energeticky nezávislé paměti.		
b) Součástí systému musí být zálohovací zařízení. Intervaly zálohování musí být dostatečně malé, aby byl dostatečně malý také rozdíl mezi aktuální a zálohovanou hodnotou tak, aby maximální rozdíl byl danou částí nejvyšší dovolené chyby.		
c) Součástí zařízení musí být také prostředky pro návrat do původního stavu po chybě, nebo jiné příčině využití zálohy.		

<p>Potřebná dokumentace: Stručný popis dat, která jsou předmětem zálohování, a situace, kdy toto zálohování nastává. Výpočet maximální chyby, která může nastat u kumulativních hodnot vlivem intervalu zálohování.</p>
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> Kontrolujeme, zda jsou všechna data relevantní z pohledu legální metrologie zálohována v energeticky nezávislé paměti. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu.
<p>Přijatelné řešení: Hardwarově je kontrolován stav mikroprocesoru a stavových proměnných prostřednictvím samostatné cyklicky běžící funkce. Tato funkce periodicky zálohuje stavové proměnné do energeticky nezávislé paměti.</p> <p><i>Poznámka: předpokládáme, že přerušení výše uvedené funkce má nejvyšší prioritu, a nedotkne se ho tudíž případné uvíznutí programu v nekonečné smyčce.</i></p>

10.6.4 Příklady softwaru a dat relevantních z pohledu legální metrologie

Funkce a parametry uvedené v předchozí tabulce se objevují u různých typů vážicích zařízení. Pokud k tomu dojde, je nutné je považovat za relevantní z pohledu legální metrologie. Nepředpokládá se však, že se budou všechny vyskytovat u jednoho typu přístroje. Čísla ve sloupcích udávají číslo příslušného doporučení OIML. Typy jsou rozlišeny na data/funkce specifické pro typ přístroje (TF/TD), specifické pro přístroj (DF/DD) a proměnné (VV).

funkce/data	typ	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		
zaokrouhlení ceny	TF, TD			X		X		
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	DD (TD)	X	X	X	X	X	X	X

funkce/data	typ	50	51 (X)	51 (Y)	61	76	106	107
zobrazovaná hodnota	VV	X		X		X	X	X
tára, preset táry	VV		X	X	X	X	X	
jednotková a aktuální cena	VV			X		X		X
hmotnost v interním rozlišení	VV	X	X	X	X	X	X	X
stavové signály (stabilita, nula)	TF	X	X	X	X	X	X	X
srovnání aktuální hmotnosti s presetem	TF		X		X			
automatický tisk, např. při přerušení automatické operace	TF	X						X
zahřívací čas	TF (TD)	X	X	X	X	X	X	X
vzájemné blokování funkcí, např. při nastavení nuly	TF		X	X	X	X		
automatický/neautomatický provoz							X	
nastavování nuly/čítání		X						X
záznam o přístupu k nastavení	TF (VV)		X	X				
maximální rychlost provozu (dynamické vážení)	DD (TD)	X	X	X	X		X	X
parametry dynamického vážení	VV		X	X			X	
přednastavená hodnota hmotnosti	VV		X		X			
meze nastavení	DD (TD)		X	X				
kritéria nastavení nuly	DD (TD)		X	X	X		X	X
minimální plnění	DD (TD)				X			X
limit chybového stavu	DD	X			X			
limit baterie	DD (TD)	X	X	X	X	X	X	X

Tabulka 10.1: Příklad relevantních funkcí a dat.

10.6.5 Další aspekty

Nejsou.

10.6.6 Přiřazení tříd rizika

Podle rozhodnutí technické komise WELMEC WG 2 (22/23. 1. 2004) jsou všechna automatická vážicí zařízení zařazena do třídy B, a to nezávisle na typu (P nebo U).

Nicméně podle výsledku dotazníku skupiny WELMEC WG 7 (2004) byly stanoveny následující třídy rizika, které budou ještě předmětem jednání skupiny WG2:

- **třída rizika B pro přístroje typu P**
- **třída rizika C pro totalizéry typu P a ostatní AWI typu U**
- **třída rizika D pro totalizéry typu U.**

10.7 Taxametry

Taxametry jsou předmětem regulace ve smyslu směrnice MID. Požadavky specifické pro tyto typy měřicích přístrojů jsou uvedeny v dodatku MI-007, nebyly však brány v potaz, stejně jako nebyly brány v potaz ani žádné další normy.

10.7.1 Specifické normy, standardy a jiné normativní dokumenty

Evropská norma EN50148, která by se měla stát normativním dokumentem ve smyslu směrnice MID, nebyla pro tuto chvíli brána v potaz. Tato norma by se spolu s návodem vzniklým v rámci projektu MID-Procedures měla stát základem zde uvedených paragrafů. Kromě těchto dokumentů vzniká také doporučení sdružení OIML, ani to však není zatím ve stadiu, kdy by bylo možné jej použít jako normativní dokument.

10.7.2 Technický popis

Taxametr, tak jak je definován ve směrnici MID, měří čas, vzdálenost (na základě snímače, na který se nevztahuje směrnice MID) a počítá cenu podle daných tarifů.

V současnosti se jedná o jednoúčelové měřicí přístroje (typ P ve smyslu tohoto dokumentu), nicméně předpokládá se, že v budoucnosti budou vznikat i přístroje založené na univerzálních počítačích (typ U ve smyslu tohoto dokumentu).

10.7.3 Požadavky na software

Podle směrnice MID, přílohy MI-007, 9:
v případě, že napájení poklesne pod minimální hodnotu danou výrobcem, taxametr musí

- nadále pracovat správně nebo se vrátit po výpadku napájení do správné funkce beze ztráty dat, pokud se jedná o krátkodobý výpadek napájení, zejména vlivem startování motoru.
- skončit měření, pokud se jedná o dlouhodobý výpadek napájení.

Taxametr má funkci dlouhodobého uchovávání dat a data musí být uchovávána alespoň jeden rok (viz MI-007, odst. 15.2.)

Třída rizika B	Třída rizika C	Třída rizika D
<p>I7-1: Prostředky zálohování <i>Data relevantní z pohledu legální metrologie, jako jsou měřené hodnoty a stav měření, musí být v případě výpadku napájení zálohována.</i></p>		
<p>Specifikace:</p> <ol style="list-style-type: none"> 1) Data musí být zálohována v energeticky nezávislé paměti. 2) Systém obsahuje detektor úrovně napájení, který určuje, kdy je třeba zálohovat data. 3) Systém obsahuje prostředky na obnovení původního stavu po obnovení napájení. 		
<p>Potřebná dokumentace: Stručný popis dat, která jsou předmětem zálohování, a situace, kdy toto zálohování nastává.</p>		
<p>Validace: <i>Kontrola založená na dokumentaci</i></p> <ul style="list-style-type: none"> • Kontrolujeme, zda je zálohování realizováno přiměřeným způsobem. <p><i>Funkční kontrola</i></p> <ul style="list-style-type: none"> • Postačují běžné zkoušky reakce na chyby a vlivy prostředí v rámci schválení typu. 		
<p>Přijatelné řešení: Po 15 vteřinách výpadku napájení je vyvoláno přerušení a s ním související funkce, která uloží výsledky měření, stavové parametry a ostatní potřebná data do energeticky nezávislé paměti, např. EEPROM. Jakmile je napájení obnoveno, data jsou nahrána zpět do operační paměti přístroje a přístroj pokračuje v provozu.</p> <p><i>Poznámka: předpokládáme, že přerušení v důsledku výpadku napájení má takovou prioritu, že dokáže přerušit normální provoz, případně i uvíznutí programu v nekonečné smyčce.</i></p>		

10.7.4 Příklady softwaru a dat relevantních z pohledu legální metrologie

V následující tabulce jsou dány některé typické parametry taxametru:

parametr	chráněný	nastavitelný	poznámka
k-faktor	x		impulzy na km
tarif	x	x	měna/km
parametry rozhraní		x	baudrate atd.

10.7.5 Další aspekty

Doporučujeme, aby byl vytvořen normativní dokument pro generátory vzdálenosti. Předběžně uvažujeme o následujících požadavcích:

1. rozlišení generátoru vzdálenosti musí být stejné nebo vyšší než 2 metry,
2. generátor vzdálenosti musí pracovat nezávisle na rychlosti jízdy,
3. musí být známy charakteristiky vzhledem k rychlosti jízdy, napájení a podobným parametrům,
4. požadavky na testování budou předmětem dalších diskusí.

10.7.6 Přiřazení tříd rizika

Podle výsledku dotazníku skupiny WELMEC WG 7 (2004) byly stanoveny následující třídy rizika pro účely zkoušení taxametrů vybavených softwarem:

- **třída rizika C pro přístroje typu P**
- **třída rizika D pro přístroje typu U.**

10.8 Ztělesněné míry

Míry materiálu jsou předmětem regulace ve smyslu směrnice MID. Požadavky specifické pro tyto typy měřicích přístrojů jsou uvedeny v dodatku MI-008.

V současné době nejsou považovány za měřidla vybavené softwarem ve smyslu tohoto dokumentu.

10.9 Měřidla rozměrů

Měřidla rozměrů jsou předmětem regulace ve smyslu směrnice MID. Požadavky specifické pro tyto typy měřicích přístrojů jsou uvedeny v dodatku MI-009, nebyly však brány v potaz, stejně jako nebyly brány v potaz ani žádné další normy.

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

10.9.6 Přiřazení tříd rizika

Podle výsledku dotazníku skupiny WELMEC WG 7 (2004) byly stanoveny následující třídy rizika pro účely zkoušení měřidel rozměrů vybavených softwarem:

- **třída rizika B pro přístroje typu P**
- **třída rizika C pro přístroje typu U.**

10.10 Analyzátoři plynu

Analyzátoři plynu jsou předmětem regulace ve smyslu směrnice MID. Požadavky specifické pro tyto typy měřicích přístrojů jsou uvedeny v dodatku MI-010, nebyly však brány v potaz, stejně jako nebyly brány v potaz ani žádné další normy.

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

10.10.6 Přiřazení tříd rizika

Podle výsledku dotazníku skupiny WELMEC WG 7 (2004) byly stanoveny následující třídy rizika pro účely zkoušení měřidel rozměrů vybavených softwarem:

- **třída rizika B pro přístroje typu P**
- **třída rizika C pro přístroje typu U.**

11 DEFINICE TŘÍD RIZIKA

11.1 Obecný princip

Požadavky uvedené v tomto dokumentu jsou rozděleny podle tříd rizika (pojem „riziko“ se vztahuje pouze k softwaru v měřicích přístrojích). Každý zkoušený přístroj musí být jednoznačně do některé z uvedených tříd zařazen, aby bylo možné na něj aplikovat požadavky vyplývající z kapitol 5–10. Každá třída rizika odpovídá různým úrovním ochrany, zkoušení a shody, přičemž každý z těchto faktorů může mít tři stupně: nízký, střední a vysoký.

11.2 Popis úrovní ochrany, zkoušení a shody

Následující odstavec popisuje jednotlivé úrovně ochrany, zkoušení a shody:

Úrovně ochrany softwaru:

nízká: ochrana není zabezpečena žádným zvláštním způsobem,

střední: software je zabezpečen proti záměrným změnám prováděným jednoduchými a snadno dostupnými nástroji (např. textovými editory),

vysoká: software je zabezpečen proti záměrným změnám prováděným k tomu určenými sofistikovanými nástroji (diskové editory, vývojové nástroje atd.).

Úrovně zkoušení softwaru:

nízká: zkoušení měřidla je prováděno způsobem standardním pro běžné schválení typu, software není zvláštním způsobem zkoušen,

střední: kromě zkoušení měřidla způsobem standardním pro běžné schválení typu je software prověřován na základě jeho dokumentace. Ta zahrnuje popis softwarových funkcí, popis parametrů atd. Pro prokázání shody s dokumentací jsou prováděny praktické zkoušky vybraných funkcí,

vysoká: kromě zkoušení odpovídajícího střední úrovni je prováděna hloubková kontrola, obvykle na základě inspekce zdrojového kódu.

Úrovně shody softwaru:

nízká: funkčnost softwaru v každém přístroji se shoduje s dokumentací

střední: funkčnost softwaru se shoduje s dokumentací, některé části mohou být navíc při schválení prohlášeny za neměnné, tudíž je nemožné měnit bez souhlasu daného notifikovanou osobou. Tyto části musí být v každém přístroji stejné,

vysoká: veškerý software musí být identický se schváleným softwarem.

11.3 Rozdělení tříd rizika

Z 27 teoreticky možných permutací úrovní shody má pouze 4–5 praktický význam (třídy rizika B, C, D, E, případně F). Tyto třídy zahrnují všechny typy měřicích přístrojů, které pokrývá směrnice MID a poskytují dostatečný prostor pro další vývoj v budoucnosti. Třídy jsou definovány v níže uvedené tabulce:

třída rizika	úroveň ochrany	úroveň zkoušení	úroveň shody
A	nízká	nízká	nízká
B	nízká	střední	nízká
C	střední	střední	střední
D	vysoká	střední	střední
E	vysoká	vysoká	střední
F	vysoká	vysoká	vysoká

11.4 Interpretace tříd rizika

Třída rizika A: Vůbec nejnižší třída rizika. Neexistuje ochrana proti záměrné modifikaci softwaru a software je zkoušen jen jako součást měření při schválení typu celého zařízení. Shoda je požadována jen na úrovni dokumentace. V tuto chvíli se nepředpokládá, že by byl do této třídy zařazen nějaký typ přístroje, třída je definována jen pro případné budoucí využití.

Třída rizika B: Proti třídě A jsou ochrana i zkoušení softwaru požadovány na střední úrovni. Shoda je požadována jen na úrovni dokumentace stejně jako u třídy A.

Třída rizika C: Ve srovnání s třídou B je požadována shoda na střední úrovni. Některé části mohou být tedy při schvalování označeny za neměnné, zbytek pak musí vykazovat shodu na úrovni dokumentace. Požadavky na zkoušení a ochranu jsou stejné jako u třídy B.

Třída rizika D: Úroveň ochrany je proti třídě C zpřísněna na vysokou. I přestože úroveň zkoušení je stejná jako u třídy C, je nezbytné dokumentací doložit parametry a prostředky použité k zabezpečení této ochrany. Úroveň shody je stejná jako u třídy C.

Třída rizika E: Na rozdíl od třídy D je požadováno zkoušení na vysoké úrovni, ostatní požadavky jsou stejné.

Třída rizika F: Všechny požadavky jsou na nejvyšších úrovních. Obdobně jako u třídy A se momentálně nepředpokládá, že by byl do této třídy zařazen nějaký typ přístroje, třída je definována jen pro případné budoucí využití.

12 VZOR PROTOKOLU O VALIDACI

Následuje vzor protokolu o validaci, skládající se z hlavní části a dvou příloh. Hlavní část obsahuje obecný popis testovaného softwaru a musí být upraven podle konkrétního softwaru, který je zkoušen. Příloha 1 obsahuje dva checklisty, pomocí kterých by měl být usnadněn výběr příslušných částí tohoto dokumentu pro validaci softwaru. Příloha 2 obsahuje kontrolní seznamy pro jednotlivé bloky požadavků uvedené v tomto dokumentu. Doporučujeme je použít jak výrobci, tak zkoušejícímu, aby bylo ověřeno, že jsou splněny všechny požadavky.

V posledním odstavci této kapitoly jsou navíc uvedeny informace, které musí být součástí certifikátu schválení typu měřidla.

12.1 Vzor obecné části protokolu o validaci

Protokol o zkoušce č. XYZ122344
Průtokoměr Dynaflow, model DF100
Validace softwaru
(N příloh)

Poslání:

Směrnice MID (Measurement Instruments Directive) udává základní požadavky na měřidla používaná v Evropské unii. Software v měřicím přístroji byl validován, aby byla prokázána shoda s požadavky této směrnice.

Validace byla založena na použití dokumentu WELMEC MID Software Requirements Guide WELMEC Guide 7.2.. ve kterém jsou popsány základní požadavky na software v měřicích přístrojích. Tento protokol popisuje zkoušení softwaru, které bylo provedeno, aby byl prokázán soulad se směrnicí MID.

Klient:

Dynaflow
P. O. Box 1120333
100 Reykjavík
Iceland
Kontaktní osoba: Mr. Bjanur Sigfridson

Popis měřidla:

Průtokoměr Dynaflow DF 100 je měřicí přístroj určený k měření průtoku kapalin. Rozsah měření je 1–200 l/s. Základní funkce přístroje jsou následující:

- měření průtoku
- měření proteklého množství
- poskytnutí rozhraní k převodníku.

V souladu s WELMEC Guide 7.2 je průtokoměr popsán jako

- jednoúčelový měřicí přístroj
- přístroj obsahující dlouhodobé uchování dat.

Průtokoměr Dynaflow DF 100 je samostatný přístroj s integrovaným převodníkem. Měřený objem je indikován přímo na průtokoměru. Průtokoměr nemá prostředky pro komunikaci s jinými zařízeními.

Výrobce softwaru: Dynaflow, P.O. Box 1120333, 100 Reykjavík, Iceland.

Verze softwaru, která byla validována má označení V1.2c. Zdrojový kód se skládá z následujících souborů:

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

Validace byla provedena na základě následujících dokumentů:

- uživatelský manuál DF100
- manuál údržby DF100
- popis softwaru DF100 (interní dokument datovaný k 22. listopadu 2003)
- elektronické schéma DF100 (náčrt č. 222-31 datovaný k 15 říjnu 2003).

Přístroj byl přejat ke schválení do Národní zkušební laboratoře 25. listopadu 2003.

Zkoušení:

Validace byla provedena podle dokumentu WELMEC 7.2, vydání 1 (ke stažení na www.welmec.org).

Validace byla provedena v období 1.–23. prosince 2003. Kontrola návrhu přístroje byla provedena 3. prosince dr. K. Fehlerem v sídle firmy Dynaflow v Reykjavíku. Další zkoušení bylo provedeno v Národní zkušební laboratoři.

Byly validovány následující požadavky:

- specifické požadavky pro vestavěné měřicí přístroje (typ P)

P: rozšíření

L: dlouhodobé uchování dat.

Checklist, kterým byla tato konfigurace zvolena, je v příloze 1 tohoto dokumentu.

Přístroji byla přiřazena třída rizika C.

Byly použity následující metody validace:

- identifikace softwaru
- kompletnost dokumentace
- kontrola uživatelského manuálu
- funkční testování
- kontrola návrhu softwaru
- kontrola dokumentace
- analýza toku dat
- simulace vstupů.

Výsledek:

Následující požadavky dokumentu WELMEC 7.2 byly bezchybně splněny:

- P1, P2, P3, P5, P6, P7
(P4 se nevztahoval k tomuto softwaru)
- L1, L2, L3, L4, L5, L6, L7.

Kontrolní seznamy k požadavkům P jsou v příloze 2.1 tohoto protokolu, kontrolní seznamy k požadavkům L jsou v příloze 2.2 tohoto protokolu.

Při testování byly nalezeny dva příkazy nepopsané v uživatelském manuálu. Tyto příkazy byly zahrnuty do verze manuálu datované k 10. prosinci 2003.

Dále byla nalezena chyba, která omezovala počet dní měsíce února na 28 i v přestupných letech. Tato chyba se vyskytovala ve verzi V.1.2b a byla opravena ve verzi V.1.2c.

Software zařízení Dynaflo DF100 splňuje základní požadavky směrnice MID.

Národní metrologický institut
Oddělení validace SW

Dr. Kein Fehler
Technický manažer

Dr. Sans Probleme
Technický vedoucí

23. prosince 2003

12.2 Příloha 1 protokolu o validaci: Kontrolní seznamy pro výběr typu požadavků

První kontrolní seznam je určen k výběru základní konfigurace (P nebo U).

Pouze v případě, že všechny otázky jsou zodpovězeny stejně jako ve sloupci P, považujeme přístroj za jednoúčelový měřicí přístroj (typ P), v ostatních případech jej považujeme za přístroj typu U.

Kontrolní seznam pro výběr základní konfigurace			
		(P)	Poznámka
1	Je zařízení konstruováno jen pro účely měření?	(Ano)	
2	Je obecně použitelný software v zařízení dostupný uživateli?	(Ne)	
3	Pokud je možné přepnout zařízení do režimu nepodléhajícího kontrole, je zablokován přístup k prostředkům operačního systému?	(Ano)	
4	Jsou použité programy a prostředí neměnné?	(Ano)	
5	Existují v zařízení programovací nástroje?	(Ne)	
Zaškrtněte odpovídající políčka.			

Druhý kontrolní seznam je určen pro nalezení příslušných IT konfigurací:

Kontrolní seznam pro výběr IT konfigurace					
		ano	ne	n/a	Poznámka
L	Může zařízení dlouhodobě ukládat data na pevné nebo výměnné paměti?				
T	Má zařízení rozhraní pro příjem nebo odesílání dat z/do jiných přístrojů podléhajících kontrole?				
S	Obsahuje zařízení části softwaru nepodléhající kontrole, které by se měly po schválení měnit?				
D	Je možné a žádoucí stahovat software?				
Použijte požadavky na zaškrtnuté konfigurace.					

12.3 Příloha 2 protokolu o validaci: Kontrolní seznamy pro konkrétní technické požadavky

1. checklist pro zařízení typu P (základní požadavky)

Zařízení typu P						
	test		vyhověl	nevyhověl	n/a	poznámka
P1		Splňuje dokumentace požadavek P1?				
P2		Splňuje identifikace požadavek P2?				
P3		Je rozhraní pro zadávání příkazů vytvořeno tak, že zneumožňuje nepřipustné ovlivnění funkce softwaru?				
P4		Mohou být příkazy zadávány přes komunikační rozhraní a jsou zabezpečena proti nepřipustnému ovlivnění funkce softwaru?				
P5		Jsou data a software relevantní z pohledu legální metrologie chráněny proti náhodným změnám?				
P6		Je software relevantní z pohledu legální metrologie chráněn proti jeho změně nebo výměně?				
P7		Jsou parametry softwaru relevantní z pohledu legální metrologie chráněny proti neoprávněným změnám?				
V poznámce popište případné rozdíly proti požadavkům.						

2. checklist pro zařízení typu U (základní požadavky)

Zařízení typu U						
	test		vyhověl	nevyhověl	n/a	poznámka
U1		Splňuje dokumentace výrobce požadavek U1?				
U2		Je identifikace softwaru vytvořena podle požadavků U2?				
U3		Je rozhraní pro zadávání příkazů vytvořeno tak, že zneumožňuje nepřipustné ovlivnění funkce softwaru?				
U4		Mohou být příkazy zadávány přes komunikační rozhraní a jsou zabezpečena proti nepřipustnému ovlivnění funkce softwaru?				
U5		Jsou data a software relevantní z pohledu legální metrologie chráněny proti náhodným změnám?				
U6		Je software relevantní z pohledu legální metrologie chráněn proti jeho změně nebo výměně?				
U7		Jsou parametry softwaru relevantní z pohledu legální metrologie chráněny proti neoprávněným změnám?				
U8		Existují prostředky na zajištění autentičnosti softwaru a produkováných dat?				
U9		Je software navržen tak, že nemůže být jeho funkce ovlivněna jiným softwarem, který není předmětem kontroly z pohledu legální metrologie?				
<i>V poznámce popište případné rozdíly proti požadavkům.</i>						

3. checklist pro specifické požadavky rozšíření L

Rozšíření L						
	test		vyhověl	nevyhověl	n/a	poznámka
L1		Obsahují uložená data všechny informace potřebné k rekonstrukci původního měření?				
L2		Jsou uložená data chráněna proti neúmyslným změnám?				
L3		Jsou uložená data chráněna proti změnám jednoduchými nástroji (třídy rizika B a C) nebo sofistikovanými nástroji (třídy rizika D a E)?				
L4		Je možné k datům jednoznačně přiřadit konkrétní měření?				
L5		Třídy rizika B a C: jsou klíče použité k ochraně dat zabezpečeny proti odhalení jednoduchými nástroji? Třídy rizika D a E: jsou klíče použité k ochraně dat zabezpečeny proti odhalení sofistikovanými nástroji? Jsou použité metody shodné s metodami použitými při elektronických platbách? Může uživatel ověřit autentičnost veřejného klíče?				
L6		Kontroluje software, který načítá uložená data, zda nebyla neoprávněně nebo náhodně změněna? Existují prostředky zabráňující použití takových dat?				
L7		Jsou měřená data ukládána automaticky?				
L8		Má paměť vyhrazená k ukládání dat dostatečnou kapacitu?				
<i>V poznámce popište případné rozdíly oproti požadavkům.</i>						

4. checklist pro specifické požadavky rozšíření T

Rozšíření T						
	test		vyhověl	nevyhověl	n/a	poznámka
T1		Obsahují přenášená data všechny informace potřebné k rekonstrukci původního měření?				
T2		Jsou přenášená data chráněna proti neúmyslným změnám?				
T3		Jsou přenášená data chráněna proti změnám jednoduchými nástroji (třídy rizika B a C) nebo sofistikovanými nástroji (třídy rizika D a E)?				
T4		Je možné k datům jednoznačně přiřadit konkrétní měření?				
T5		Třídy rizika B a C: jsou klíče použité k ochraně dat zabezpečeny proti odhalení jednoduchými nástroji? Třídy rizika D a E: jsou klíče použité k ochraně dat zabezpečeny proti odhalení sofistikovanými nástroji? Jsou použité metody shodné s metodami použitými při elektronických platbách? Může uživatel ověřit autentičnost veřejného klíče?				
T6		Kontroluje software, který přijímá data, zda nebyla neoprávněně nebo náhodně změněna? Existují prostředky zabráňující použití takových dat?				
T7		Nemůže být proces měření ovlivněn zpožděním při přenosu?				
T8		Nemůže dojít ke ztrátě dat při přenosu?				
<i>V poznámce popište případné rozdíly proti požadavkům.</i>						

5. checklist pro specifické požadavky rozšíření S

Rozšíření S						
	test		vyhověl	nevyhověl	n/a	poznámka
S1		Zahrnuje software, který je předmětem kontroly z pohledu legální metrologie, všechny potřebné parametry?				
S2		Je zajištěno, že doplňující informace generovaná softwarem, který není předmětem kontroly z pohledu legální metrologie, nemůže být zaměněna s informací generovanou softwarem, který je předmětem kontroly z pohledu legální metrologie?				
S3		Je veškerá výměna dat mezi oběma částmi softwaru prováděna skrze ochranné rozhraní?				
<i>V poznámce popište případné rozdíly proti požadavkům.</i>						

6. checklist pro specifické požadavky rozšíření D

Rozšíření D						
	test		vyhověl	nevyhověl	n/a	poznámka
D1		Jsou stahování a následná kontrola softwaru prováděny automaticky?				
D2		Existují prostředky k ověření autentičnosti a schválení softwaru?				
D3		Existují prostředky pro kontrolu změn softwaru v průběhu stahování?				
D4		Je zajištěna možnost zjistit čas a další parametry stahování při zpětné kontrole?				
D5		Je zajištěno, aby stahování neproběhlo bez předchozího souhlasu uživatele?				
<i>V poznámce popište případné rozdíly proti požadavkům.</i>						

12.4 Informace, které by měly být součástí certifikátu schválení typu

Součástí certifikátu schválení typu měřidla by měl být výběr z informací získaných v rámci validace softwaru, který měřidlo obsahuje. Tento požadavek se týká následujících informací:

- odkazy na dokumentaci dodanou ke schválení typu,
- identifikace a popis hardwarových komponent, které souvisí se softwarovou funkcí měřidla,
- popis softwarového prostředí,
- popis modulů, které jsou předmětem kontroly z pohledu legální metrologie,
- popis a identifikace hardwarových a softwarových rozhraní podstatných pro chod softwaru,
- popis a identifikace umístění softwaru v měřidle (EEPROM, procesor, pevný disk), které musí být zabezpečeny úřední značkou,
- návod ke kontrole softwaru při ověření měřidla,
- návod ke kontrole záznamů událostí.

13 KŘÍŽOVÉ REFERENCE

13.1 Vztah tohoto dokumentu ke článkům směrnice MID

Požadavek	označení	článek/příloha MID	označení
	Typ P		
P1	dokumentace výrobce	AI-9.3, 12, čl.10	dokumentace, kontrola shody
P2	identifikace	AI-7.6, 8.3	vhodnost, ochrana před zneužitím
P3	vliv uživatelského rozhraní	AI-7.1	vhodnost
P4	vliv komunikačního rozhraní	AI-7.1, 8.1	vhodnost, ochrana před zneužitím
P5	ochrana před náhodnými změnami	AI-7.1, 7.2, 8.4	vhodnost, ochrana před zneužitím
P6	ochrana před záměrnými změnami	AI-7.1, 8.2, 8.3, 8.4	vhodnost, ochrana před zneužitím
P7	ochrana parametrů	AI-7.1, 8.2, 8.3, 8.4	vhodnost, ochrana před zneužitím
	Typ U		
U1	dokumentace výrobce	AI-9.3, 12, čl.10	dokumentace, kontrola shody
U2	identifikace	AI-7.6, 8.3	vhodnost, ochrana před zneužitím
U3	vliv uživatelského rozhraní	AI-7.1	vhodnost
U4	vliv komunikačního rozhraní	AI-7.1, 8.1	vhodnost, ochrana před zneužitím
U5	ochrana před náhodnými změnami	AI-7.1, 7.2, 8.4	vhodnost, ochrana před zneužitím
U6	ochrana před záměrnými změnami	AI-7.1, 8.2, 8.3, 8.4	vhodnost, ochrana před zneužitím
U7	ochrana parametrů	AI-7.1, 8.2, 8.3, 8.4	vhodnost, ochrana před zneužitím
U8	autentičnost softwaru a výsledků	AI-7.1, 7.2, 7.6, 8.3, 10.2, 10.3, 10.4	vhodnost, ochrana před zneužitím
U9	vliv jiného softwaru	AI-7.6	vhodnost

Požadavek	označení	článek/příloha MID	označení
	Rozšíření L		
L1	úplnost dat	AI-7.1, 8.4, 10.2	vhodnost, ochrana před zneužitím, indikace
L2	ochrana dat	AI-7.1, 7.2, 8.4	vhodnost, ochrana před zneužitím
L3	integrita dat	AI-7.1, 8.4	vhodnost, ochrana před zneužitím
L4	autentičnost dat	AI-7.1, 8.4, 10.2	vhodnost, ochrana před zneužitím, indikace
L5	utajení klíčů	AI-7.1, 8.4	vhodnost, ochrana před zneužitím
L6	získání uložených dat	AI-7.2, 10.1, 10.2, 10.3, 10.4	vhodnost, indikace
L7	automatické ukládání	AI-7.1, 8.4	vhodnost, ochrana před zneužitím
L8	kapacita paměti	AI-7.1	vhodnost
Lx	vše z rozšíření L	AI-11.1	další zpracování dat
	Rozšíření T		
T1	úplnost dat	AI-7.1, 8.4	vhodnost, ochrana před zneužitím
T2	ochrana dat	AI-7.1, 7.2, 8.4	vhodnost, ochrana před zneužitím
T3	integrita dat	AI-7.1, 8.4	vhodnost, ochrana před zneužitím
T4	autentičnost dat	AI-7.1, 8.4	vhodnost, ochrana před zneužitím
T5	utajení klíčů	AI-7.1, 8.4	vhodnost, ochrana před zneužitím
T6	zpracování poškozených dat	AI-7.1, 8.4	vhodnost, ochrana před zneužitím
T7	zpoždění při přenosu	AI-7.1, 8.4	vhodnost, ochrana před zneužitím
T8	dostupnost přenosu	AI-7.1, 8.4	vhodnost, ochrana před zneužitím

Požadavek	označení	článek/příloha MID	označení
	Rozšíření S		
S1	oddělení softwaru	AI-7.6, 10.1	vhodnost, indikace
S2	smíšená indikace	AI-7.1, 7.2, 7.6, 10.2	vhodnost, indikace
S3	ochranné rozhraní	AI-7.6	vhodnost
	Rozšíření D		
D1	mechanismus stahování	AI-8.2, 8.4	ochrana před zneužitím
D2	autentizace softwaru	AI-7.6, 8.3, 8.4, 12	vhodnost, ochrana před zneužitím,
D3	integrita softwaru	AI-7.1, 8.4	vhodnost, ochrana před zneužitím, testování shody
D4	návaznost softwaru	AI-7.1, 7.6, 8.2, 8.3, 12	vhodnost, ochrana před zneužitím
D5	souhlas ke stahování	AI-7.1, 7.6	vhodnost
	Rozšíření I		
I1-1 I2-1 I3-1 I4-1	detekce chyb	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	spolehlivost, specifické požadavky na měřidla
I1-2 I2-2 I3-2 I4-2	zálohování	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	spolehlivost, specifické požadavky na měřidla
I1-3 I2-3 I3-3 I4-3	obnova ze zálohy	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	specifické požadavky na měřidla
I1-4 I2-4 I3-4 I4-4	rozlišení	MI-002-5.3, MI-003-5.2	specifické požadavky na měřidla

Požadavek	označení	článek/příloha MID	označení
I1-5 I2-5 I3-5 I4-5	resetování kumulativních hodnot	AI-8.5	ochrana před zneužitím
I1-6 I2-6 I3-6 I4-6	indikace	AI-7.2, 10.5	vhodnost, indikace
I2-7	sledování životnosti baterie	MI-002-5.2	specifické požadavky na měřidla
I2-8	sledování přepočítávačů objemu plynu	MI-002-9.1	specifické požadavky na měřidla
I2-9	testování	MI-002-5.5	specifické požadavky na měřidla
I6-1	detekce chyb	MI-006-IV, MI- 006-V	specifické požadavky na měřidla
I6-2	zálohování	MI-006-IV, MI- 006-V	specifické požadavky na měřidla

13.2 Vztah článků směrnice MID k tomuto dokumentu

Článek MID	označení	poznámka	tento dokument – požadavek
1–3		se softwarem nesouvisí	
4(b)	definice, moduly	přenos dat, základní požadavky na komponenty	P, U
5–9		se softwarem nesouvisí	
10	dokumentace	obecný popis přístrojů, dokumentace, plány, výkresy, diagramy, umístění značek, rozhraní aj.	P1, U1
	Příloha I		
AI-1 - AI-5		se softwarem nesouvisí	
AI-6	spolehlivost	detekce chyb, zotavení, restart	Ix.1 – Ix.3
AI-7	vhodnost	nemožnost zneužití	P3–P7, U3–U8, L1–L5, L7, L8 T1–T8, S2, D3, D4
AI-8	ochrana před zneužitím		
AI-8.1		vliv připojených přístrojů	P4, U4
AI-8.2		zabezpečení	P6, P7, U6, U7, D1, D4
AI-8.3		identifikace	P2, P6, P7, U2, U6, U7, U8, D2, D4
AI-8.4		ochrana uložených a přenášených dat	P5–P7, U5–U7, L1–L5, T1–T8 D1–D3
AI-8.5		reset kumulativních hodnot	I1-5, I2-5, I3-5, I4-5

Článek MID	označení	poznámka	tento dokument – požadavek
AI-9	informace poskytovaná spolu s přístrojem		
AI-9.1		kapacita měření	L8
AI-9.2		se softwarem nesouvisí	
AI-9.3		instalace, rozhraní, připojení ostatních přístrojů	P1, U1
AI-9.4–AI-9.8		se softwarem nesouvisí	
AI-10	indikace		
AI-10.1		displej, tiskárna	U8, L6, S2
AI-10.2		smíšená indikace výsledků	U8, L1, L4, L6, S2
AI-10.3		čitelnost výsledků	U8, L6, S2
AI-10.4		zobrazení výsledků při obchodu	U8, S2
AI-10.5		zobrazení výsledků zákazníkovi	I1-6, I2-6, I3-6, I4-6
AI-11	další zpracování výsledků		
AI-11.1		ukládání hodnot	L1–L8
AI-11.2		ověřování měřených hodnot	L1, L6
AI-12	posouzení shody		P1, P2, U1, U2, D2, D4
	přílohy A1–H1		
A1-H1		se softwarem nesouvisí	
	příloha MI-001		
1–6		se softwarem nesouvisí	
7.1.1–2	ochrana před elmag. rušením	detekce chyb, záloha, obnovení	I1-1 až I1-3
7.1.3–9		se softwarem nesouvisí	

Článek MID	označení	poznámka	tento dokument – požadavek
	příloha MI-002		
1,2		se softwarem nesouvisí	
3.1	ochrana před elmag. rušením	detekce chyb, záloha, obnovení	I2-1 až I2-3
3.1.3–5.1		se softwarem nesouvisí	
5.2	vhodnost	doba životnosti baterie	I2-7
5.3	vhodnost	rozlišení	I2-4
5.4–8		se softwarem nesouvisí	
5.5	vhodnost	testovací prvek	I2-9
5.6–8		se softwarem nesouvisí	
9.1	konverze na objem, vhodnost	přepočítávače množství plynů	I2-8
9.2–10		se softwarem nesouvisí	
	příloha MI-003		
1– 4.2		se softwarem nesouvisí	
4.3	vliv elmag. pole	detekce chyb, záloha, obnovení	I3-1 až I3-3
5.1		se softwarem nesouvisí	
5.2	vhodnost	rozlišení	I3-4
5.3–3.7		se softwarem nesouvisí	
	příloha MI-004		
1–4.1		se softwarem nesouvisí	
4.2	vliv elmag. pole	detekce chyb, záloha, obnovení	I4-1 až I4-3
4.3–7		se softwarem nesouvisí	
	příloha MI-006		
IV,V	totalizéry	detekce chyb, záloha, obnovení	I6-1 až I6-2

14 LITERATURA

- [1] 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
- [2] Software Requirements and Validation Guide, Version 1.00, 29 October 2004, European Growth Network „MID-Software“, contract number G7RT-CT-2001-05064, 2004
- [3] Software Requirements on the Basis of the Measuring Instruments Directive, WEMEC 7.1, Issue 2, 2005

© Úřad pro technickou normalizaci, metrologii a státní zkušebnictví,
Gorazdova 24, 128 01 Praha 2, k volnému prohlížení a stažení
i na www.unmz.cz, náklad 450 ks. Praha 2006.
Nakladatelský servis: Bořivoj Kleník, PhDr. – Q-art.
Redakční uzávěrka: 30. 11. 2006. NEPRODEJNÉ