European Cooperation in
Legal Metrology (WELMEC)e. V.
Bundesallee 100
38116 Braunschweig
Germany

WELMEC Guide 7.2

Softwarová příručka

(SMĚRNICE MID 2014/32/EU)

Verze 2023

Pro informaci:

Tato příručka je k dispozici pracovní skupině pro měřicí zařízení (odborná skupina Evropské komise E01349) pro účely budoucího využití na evropských webových stránkách.

WELMEC e.V., Bundesallee 100, 38116 Braunschweig, Germany.
Phone: +49 531 592 1980 E-mail: secretary@welmec.org www.welmec.org

WELMEC e.V. je spolupráce mezi představiteli legální metrologie členských států Evropské unie a EFTA.
Tento dokument je jednou z mnoha příruček vydávaných WELMEC e.V s cílem poskytnout vodítko výrobcům měřidel a oznámeným subjektům odpovědným za posuzování shody výrobků. Příručky mají výhradně poradenský charakter a neukládají žádná restriktivní opatření ani dodatečné technické požadavky oproti těm, které jsou obsaženy v příslušných směrnicích EU. Alternativní přístupy mohou být přijatelné, ale návody uvedené v tomto dokumentu jsou považovány za stanovisko WELMEC e.V. jako nejlepší možná praxe, která by měla být následována.

Vydal:
Sekretariát WELMEC
E-mail : secretary@welmec.org
Web: www.welmec.org

WELMEC e.V., Bundesallee 100, 38116 Braunschweig, Germany.
Phone: +49 531 592 1980 E-mail: secretary@welmec.org www.welmec.org

Softwarová příručka (SMĚRNICE MID 2014/32/EU)

Obsah

Předmluva

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

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

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

Upozornění: Toto vydání příručky platí rovněž pro směrnici 2004/22/ES.

Úvod

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

Postupováním podle této příručky splníte požadavky směrnice MID na software měřicích přístrojů. Všechny notifikované osoby tuto příručku přijímají jako vyhovující výklad směrnice MID v otázkách týkajících se softwaru. Provázanost mezi požadavky uvedenými v tomto dokumentu a požadavky směrnice MID je znázorněna v křížových odkazech, které tvoří přílohu tohoto dokumentu (kapitola 13).

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

1 Terminologie

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

Přijatelné řešení (Acceptable solution): Návrh nebo princip softwarového modulu nebo hardwarové komponenty, nebo vlastnosti, která je považována za splnění určitého požadavku.

Poznámka: Přijatelné řešení poskytuje příklad toho, jak může být konkrétní požadavek splněn. Tím není dotčeno žádné jiné řešení, které by rovněž splňovalo tento požadavek.

Auditní stopa (Audit trail): Průběžná data obsahující časově označený záznam událostí, např. změny v hodnotách parametrů měřicího přístroje nebo aktualizace softwaru, nebo jiné činnosti, které mají právní význam a které jsou kritické pro metrologické charakteristiky.

Poznámka: Pokud jde o příklady událostí zaznamenaných v auditové stopě, viz Událost (Event).

Autentizace (Authentication): Proces kontroly deklarované nebo údajné identity uživatele, procesu, softwaru nebo měřicího přístroje.

Poznámka: To může být nezbytné při kontrole, zda stažený software pochází od vlastníka TEC.

Autenticita (Authenticity): Výsledek ověření pravosti (vyhověl nebo nevyhověl).

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

Jednoúčelový měřicí přístroj (typ P), (Built-for-purpose measuring instrument): Zařízení konstruováno pro konkrétní účel metrologického úkolu.

Poznámka 1: Zařízení postavené pro konkrétní účel nemusí obsahovat operační systém.

Poznámka 2: Pokud má operační systém, není přímo přístupný.

Komponenta kategorie 1 (Category 1 component): Komponenty, které jsou součástí měřicího procesu, tj. zpracovávají měřicí data k vytvoření a indikaci konečné hodnoty měřeného množství spolu s relevantními daty výsledku měření.

Komponenta kategorie 2 (Category 2 component): Komponenty, které dalším způsobem zpracovávají výsledek měření bez modifikace konečné hodnoty měřeného množství a souvisejících relevantních dat výsledku měření.

Certifikace klíčů (Certification of keys): Proces vazby hodnoty veřejného klíče k jednotlivci, organizaci nebo jiné entitě.

Kontrolní zařízení (Checking facility): Zařízení integrované do měřicího přístroje nebo komponenty, které umožňuje detekovat a reagovat na významné závady.

Poznámka: "reagovat na" se vztahuje na jakoukoli adekvátní reakci měřicího přístroje (světelný signál, akustický signál, prevence měřicího procesu atd.).

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

Komunikační rozhraní (Communication interface): Část přístroje, která umožňuje přenos informací mezi měřicími přístroji, komponentami měřicích přístrojů nebo jinými vnějšími systémy.

Poznámka 1: Komunikační rozhraní může být kabelové, optické, rádiové atd. a obvykle je navrženo tak, aby používalo konkrétní protokol.

Poznámka 2: Tato definice nezahrnuje komunikaci mezi softwarovými moduly uvnitř měřicího přístroje nebo stejné komponenty.

Komponenta (Component): Identifikovatelná hardwarová část měřicího přístroje nebo podsestavy, která plní konkrétní funkci nebo funkce a která může být odděleně vyhodnocena podle konkrétních metrologických a technických výkonnostních požadavků.

Poznámka: viz WELMEC Guide 8.8.

Důvěrnost (Confidentiality): Vlastnost, že informace nejsou zpřístupněny nebo zveřejněny neoprávněným jednotlivcům, subjektům nebo procesům.

Kryptografický certifikát (Cryptographic certificate): Soubor dat obsahující veřejný klíč náležející měřicímu přístroji, nebo komponentě nebo osobě s jedinečnou identifikaci subjektu, např. sériové číslo měřicího přístroje, jméno nebo osobní identifikační číslo (PIN) osoby, datum vypršení platnosti.

Kryptografické prostředky (Cryptographic means): Prostředky, jako je šifrování a dešifrování s cílem skrývat informace před neoprávněnými osobami, nebo hashe a elektronické podpisy k zajištění integrity a autenticity.

Datová doména (Data domain): Umístění v paměti, které každý program potřebuje pro zpracování dat.

Poznámka: Datové domény mohou náležet pouze jednomu softwarovému modulu nebo několika modulům.

Specifické parametry přístroje (Device-specific parameter): *Legálně relevantní parametry*, s hodnotou závislou na konkrétním přístroji, komponentě a/nebo softwarovém modulu či modulech podléhajících legální kontrole.

Poznámka: Specifické parametry přístroje zahrnují nastavení parametrů (např. úprava rozsahu nebo jiné nastavení či korekce) a konfiguraci parametrů (např. maximální hodnota, minimální hodnota, měřicí jednotky atd.).

Elektronický měřicí přístroj (Electronic measuring instrument): Měřicí přístroj určený k měření elektrické nebo neelektrické veličiny pomocí elektronických prostředků a/nebo vybavený elektronickými díly.

Poznámka: Pro účely příručky se považují pomocná zařízení, pokud podléhají metrologické kontrole, za součást měřicího přístroje.

Elektronický podpis (Electronic signature): Softwarový prostředek, který je přidán k softwaru nebo datům s účelem ověřit původ softwaru nebo dat, tj. prokázat jejich autenticitu, nebo zkontrolovat, že software nebo data zůstaly nezměněny, tj. prokázat jejich integritu.

Poznámka 1: Pro elektronické podepisování se obvykle používá veřejný klíčový systém, tj. pár klíčů, kde jen jeden musí zůstat soukromý/tajný; ten druhý může být veřejný.

Poznámka 2: Soukromý klíč se používá při podepisování softwaru nebo dat. Veřejný klíč se používá při ověřování softwaru nebo dat před použitím.

Poznámka 3: Ověřovací instance může vyžadovat kryptografický certifikát podepisující instance, aby měla jistotu o autenticitě veřejného klíče.

Událost (Event): Akce, která by mohla ovlivnit metrologická data a/nebo charakteristiky měřicího přístroje.

Poznámka: příklady takových událostí jsou změna legálně relevantního parametru nebo modifikace nebo aktualizace legálně relevantního softwaru.

Spustitelný kód (Executable code): Digitální informace nainstalované v měřicím přístroji nebo komponentě (EPROM, pevný disk atd.).

Poznámka: Tento kód je interpretován centrální procesorovou jednotkou (CPU) měřicího přístroje a převeden na určité logické, aritmetické, dekódovací nebo datové přenosové operace.

Hašovací funkce (Hash function): Matematická funkce, která mapuje hodnoty z velké (možná velmi velké) domény do menšího rozsahu.

Poznámka: "Dobrá" hašovací funkce je taková, jestliže jsou výsledky aplikace funkce na (velkou) sadu hodnot v doméně rovnoměrně rozloženy (a zdánlivě náhodně) přes rozsah.

Integrovaná paměť (Integrated storage): Neodnímatelná paměť, která je součástí měřicího přístroje nebo komponenty, např. RAM, EEPROM, pevný disk.

Integrita (Integrity): Vlastnost, že software, měřicí data a parametry se nezměnily.

Rozhraní (Interface): Společná hranice mezi dvěma funkčními jednotkami, definovaná různými charakteristikami týkajícími se funkcí, fyzických propojení, výměny signálů a dalších charakteristik jednotek, jak je vhodné.

Přerušitelné kumulativní měření (Interruptible cumulative measurement): Proces kumulativního měření množstevní hodnoty měřené veličiny, který lze během normálního provozu snadno a rychle zastavit.

Poznámka 1: Příklady zahrnují: a) : Diskontinuální součtové automatické váhy, b) výdejní stojan na pohonné hmoty.

Poznámka 2: Viz také nepřerušitelné měření.

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

Klíč (Key): Vhodné číslo nebo posloupnost znaků, které se používají k zakódování a/nebo dekódování informací.

Legálně relevantní (Legally relevant): Vlastnost, která je vyžadována k naplnění základních požadavků a/nebo má vliv na dodržení základních požadavků MID přílohy I a/nebo základních požadavků NAWID přílohy I a III.

Poznámka 1: Měřicí přístroj podrobený legální kontrole musí splňovat základní požadavky, MID viz článek 6 a NAWID článek, proto podle definice je tento měřicí přístroj legálně relevantní.

Poznámka 2: Pokud specifické přílohy MID stanoví základní požadavky na dílčí sestavy, pak dílčí sestavy, které jsou součástí legálně relevantního měřicího přístroje, jsou také legálně relevantní.

Poznámka 3: Další vysvětlení viz kapitola 15.

Maximálně přípustná chyba (měřicího přístroje) (**Maximum permissible error (of a measuring instrument):**): Krajní hodnota měřicí chyby ve vztahu k známé referenční

hodnotě veličiny, kterou povolují specifikace nebo předpisy pro dané měření, měřicí přístroj nebo měřicí systém.

Měřená hodnota veličiny (Measured quantity value): Hodnota veličiny vyjadřující výsledek měření.

Metadata měřené hodnoty veličiny (Measured quantity value metadata): Metadata související s měřenou hodnotou veličiny.

Měření (Measurement): Proces experimentálního získání jedné nebo více hodnot veličin, které lze rozumně připsat dané veličině.

Poznámka 1: Měření se nevztahuje na nominální vlastnosti.

Poznámka 2: Měření zahrnuje porovnání veličin nebo počítání entit.

Poznámka 3: Měření předpokládá soulad popisu veličiny se zamýšleným využitím výsledku měření, měřicím postupem a kalibrovaným měřicím systémem pracujícím dle specifikovaného měřicího postupu, včetně měřicích podmínek.

Poznámka 4: Kapitola 14 ilustruje pojmy a definice týkající se měřicího procesu a jejich použití v tomto dokumentu.

Měřicí data (Measurement data): Data používaná během měřicího procesu.

Poznámka: Měřicí data zahrnují naměřenou hodnotu veličiny, data relevantní pro výsledek měření a data měřicího procesu, viz kapitola 14.

Poznámka: Naměřená hodnota veličiny a data relevantní pro výsledek měření jsou obě součástí výsledku měření a společně s daty měřicího procesu tvoří měřicí data, viz kapitola 14.

Metadata o měření (Measurement metadata): Metadata související s měřicím procesem.

Poznámka: Metadata o měření zahrnují metadata naměřené hodnoty veličiny, metadata relevantní pro výsledek měření a metadata měřicího procesu.

Chyba měření (Measurement error): Naměřená hodnota veličiny mínus referenční hodnota veličiny.

Poznámka 1: Pojem 'chyba měření' lze použít jak a) pokud existuje jedna referenční hodnota veličiny, ke které se lze vztahovat, což nastává v případě kalibrace pomocí měřicího standardu s naměřenou hodnotou veličiny s zanedbatelnou měřicí nejistotou nebo pokud je dána konvenční hodnota veličiny, v takovém případě je chyba měření známa, a b) pokud se předpokládá, že měřená veličina je reprezentována unikátní skutečnou hodnotou veličiny nebo sadou skutečných hodnot veličiny se zanedbatelným rozsahem, v takovém případě chyba měření není známa.

Poznámka 2: Měření zahrnuje porovnání veličin nebo počítání entit.

Data měřicího procesu (Measurement process data): Data používaná během měřicího procesu k sestavení výsledku měření.

Poznámka: Příklady dat měřicího procesu zahrnují hodnoty měřicích parametrů, hodnoty nastavení spojení nebo hodnoty parametrů relace.

Informace o měřicím procesu (Measurement process information): Sada hodnot kvalitativních nebo kvantitativních proměnných reprezentujících měřicí proces.

Poznámka: Informace o měřicím procesu zahrnují data měřicího procesu a metadata měřicího procesu.

Metadata měřicího procesu (Measurement process metadata): Metadata související s měřicím procesem.

Poznámka: Příklady metadat měřicího procesu zahrnují formát měřicích parametrů, formát nastavení spojení nebo formát parametrů relace.

Výsledek měření (Measurement result): Soubor kvantitativních hodnot připisovaných měřené veličině spolu s dalšími dostupnými relevantními daty k výsledku měření.

Poznámka: Příklady relevantních dat k výsledku měření jsou značky a nápisy potřebné k informování uživatele o významu výsledku měření, viz MID, Příloha I, článek 10.2.

Poznámka: Příklady relevantních dat k výsledku měření zahrnují informace o původu měřicích dat potřebné k identifikaci konkrétní transakce, např. identifikace senzoru, viz MID, Příloha I, článek 11.1

Poznámka: Relevantní data k výsledku měření jsou také informace k identifikaci konkrétní transakce, např. číslo měření, datum a čas měření, viz MID, Příloha I, článek 11.1.

Poznámka: Pokud je výpočet ceny součástí legálně relevantního softwaru, jednotková cena a cena k zaplacení jsou součástí relevantních dat k výsledku měření, viz příslušné specifické přílohy směrnice MID a Příloha I směrnice NAWID.

Poznámka: Výsledek měření (včetně naměřené kvantitativní hodnoty) je používán pro legálně relevantní účely, např. uzavření transakce.

Relevantní data k výsledku měření (Measurement result relevant data): Data používaná během procesu sestavování výsledku měření.

Poznámka: Příklady relevantních dat k výsledku měření zahrnují digitální číslo nebo analogovou hodnotu pocházející ze senzoru nebo identifikaci měřicího přístroje, v případech, kdy je součástí výsledku měření, viz kapitola 14.

Relevantní informace k výsledku měření (Measurement result relevant information): Soubor hodnot kvalitativních nebo kvantitativních proměnných týkajících se výsledku měření.

Poznámka: Relevantní informace k výsledku měření zahrnují relevantní data k výsledku měření a relevantní metadata k výsledku měření.

Relevantní metadata k výsledku měření (Measurement result relevant metadata): Metadata související se sestavováním výsledku měření.

Poznámka: Příklady relevantních metadat k výsledku měření zahrnují formát digitálního čísla nebo analogové hodnoty pocházející ze senzoru, formát měřené kvantitativní hodnoty nebo formát ID měřicího přístroje, v případech, kdy je součástí výsledku měření.

Měřicí přístroj (Measuring instrument): Zařízení používané k měření samostatně nebo ve spojení s jedním nebo více doplňkovými zařízeními.

Metadata (Metadata): Data o datech nebo datových prvcích, včetně jejich popisů dat, a data o vlastnictví dat, přístupových cestách, přístupových právech a volatilitě dat.

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

Modul (Module): Softwarová jednotka, jako je program, podprogram, knihovna, parametr nebo datová sada a další objekty včetně jejich datových domén, které mohou být ve vztahu k dalším jednotkám.

Poznámka: Software měřicích přístrojů se skládá z jednoho nebo více modulů.

Nepřerušitelné kumulativní měření (Non-interruptible cumulative measurement): Kumulativní měřicí proces bez určitého konce, který nemůže být uživatelem/operátorem zastaven a znovu v něm pokračovat, aniž by došlo ke znehodnocení výsledku měření.

Poznámka 1: Příklady zahrnují: a) Kontinuální součtové automatické váhy, b) měřidla tepelné energie.

Poznámka 2: Viz také přerušitelné kumulativní měření.

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

Operační systém (Operating System): Software pro řízení provozu programu a pro poskytování služeb pro alokaci zdrojů, plánování úloh, řízení I/O a správu dat.

Poznámka 1: Jiné programy (jako editory, kancelářské programy atd.) určené pro jiné úkoly nejsou považovány za součást operačního systému.

Poznámka 2: Pro komponenty kategorie 1 nebo kompletní měřicí přístroje obvykle legálně relevantní části operačního systému zahrnují alespoň boot loader, jádro, rozhraní (hardware a meziprocesní komunikace), služby (na pozadí), správu uživatelských oprávnění, kryptografické knihovny a konfigurační soubory těchto částí.

Poznámka 3: Pro komponenty kategorie 2 obvykle legálně relevantní části operačního systému zahrnují alespoň rozhraní (hardware a meziprocesní komunikace), správu uživatelských oprávnění, kryptografické knihovny a konfigurační soubory těchto částí.

Ochranné rozhraní (Protective interface): Legálně relevantní softwarový modul, který zpracovává veškerý datový tok do legálně relevantního softwarového modulu/modulů za účelem zabránění nepřípustných vlivů.

Ochrana (Protection): Prostředek k ochraně měřicích dat, parametrů, měřicího přístroje, komponenty nebo softwarového modulu s cílem znemožnit nebo zviditelnit zásah.

Infrastruktura veřejného klíče (Public Key Infrastructure - PKI): Organizace zaručující důvěryhodnost systému s veřejným klíčem. Zahrnuje udělování a distribuci kryptografických certifikátů všem členům účastnícím se výměny informací.

Systém s veřejným klíčem (Public Key System PKS): Pár dvou různých klíčů, jeden se nazývá tajný klíč a druhý veřejný klíč. Pro ověření integrity a autenticity informací je pomocí hash funkce generován hash kód informace, který je zašifrován tajným klíčem odesílatele, čímž vzniká podpis, který je později příjemcem dešifrován pomocí veřejného klíče odesílatele.

Riziková třída (Risk class): Třída typů měřicích přístrojů s téměř identickým hodnocením rizik.

Plombování (Sealing): Prostředek určený k ochraně software, parametrů, měřicích dat, měřicího přístroje, komponenty nebo softwarového modulu před jakoukoliv modifikací, přenastavením, odstraněním komponent nebo softwarových modulů atd.

Poznámka: To může být dosaženo hardwarem, softwarem nebo kombinací obou.

Zabezpečení (Securing): Prostředek k zabránění neoprávněnému přístupu k hardware, software, parametrům nebo měřicím datům.

Poznámka: To může být dosaženo pomocí hesel.

Algoritmus podpisu (Signature algorithm): Kryptografický algoritmus, který zašifruje (kóduje) hash kód pomocí šifrovacího klíče a umožňuje dekódování zašifrovaného hash kódu, pokud je k dispozici odpovídající dekódovací klíč.

Významná závada (Significant defect): Incident, který má nežádoucí dopad na shodu měřicího přístroje nebo chybu.

Poznámka: Příklady významných závad zahrnují a) smazání auditní stopy, b) nepřípustné změny parametrů, c) neoprávněné aktualizace a d) náhodné změny software kvůli fyzikálním účinkům.

Stahování software(Software download): Proces automatického přenosu software do cílového měřicího přístroje nebo komponenty jakýmikoli technickými prostředky z místního nebo vzdáleného zdroje (např. výměnná úložná média, přenosný počítač, vzdálený počítač) prostřednictvím libovolných spojení (např. přímé linky, sítě).

Zkouška softwaru (Software examination): Technická operace, která spočívá v určení jedné nebo více vlastností software podle konkrétního postupu (např. analýza technické dokumentace nebo spuštění programu v kontrolovaných podmínkách).

Identifikace software (Software identification): Sekvence čitelných znaků (např. verze, kontrolní součet), která reprezentuje zvažovaný software nebo softwarový modul.

Poznámka: Identifikaci software lze zkontrolovat na přístroji během jeho používání.

Softwarové rozhraní (Software interface): Programový kód a vyhrazená datová doména; přijímání, filtrování nebo přenos dat mezi softwarovými moduly.

Poznámka 1: Softwarové rozhraní nemusí být nutně legálně relevantní.

Poznámka 2: Softwarové rozhraní je rozhraní mezi dvěma nebo více softwarovými moduly, které se používá k výměně dat a přenosu příkazů.

Separace software (Software separation): Oddělení software v měřicích přístrojích nebo komponentách, které lze rozdělit na legálně relevantní softwarové moduly a na softwarové moduly, které nejsou legálně relevantní.

Poznámka: Tyto moduly komunikují prostřednictvím ochranného rozhraní, viz S3.

Zdrojový kód (Source code): Počítačový program napsaný ve formě (programovacího jazyka), který je čitelný a upravitelný.

Poznámka: Zdrojový kód je kompilován nebo interpretován do spustitelného kódu.

Zařízení pro ukládání dat (Storage device): Zařízení používané pro ukládání měřicích dat, která jsou nezbytná pro sestavení výsledku měření a/nebo pro uchování výsledku měření aby byly k dispozici po dokončení měření pro pozdější legálně relevantní účely.

Podsestava (Sub-assembly): Hardwarové zařízení, které je jako takové uvedeno ve specifických přílohách přístroje a které funguje samostatně a tvoří měřící přístroj spolu s dalšími podsestavami, s nimiž je kompatibilní, nebo s měřícími přístroji, s nímž je kompatibilní [MID, čl. 4 odst. 2].

TEC (TEC): Certifikát schválení typu.

Časová značka (Time stamp): Jedinečná hodnota, např. v sekundách, nebo řetězec datum a čas označující datum a/nebo čas, kdy došlo k určitému incidentu (např. měření nebo událost).

Přenos naměřených dat (Transmission of measurement data): Elektronický přenos naměřených dat komunikačními linkami nebo jinými prostředky do přijímače.

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

Parametr specifický pro daný typ (Type-specific parameter): Legálně relevantní parametr, jehož hodnota závisí na typu přístroje, součásti a/nebo softwarového modulu, který podléhá legální kontrole.

Poznámka: Parametry specifické pro daný typ jsou součástí legálně relevantního softwaru.

Univerzální zařízení (Universal device): Zařízení, které není konstruováno pro konkrétní účel, ale které lze přizpůsobit legálně relevantnímu úkolu pomocí softwaru.

Uživatelské rozhraní (User interface): Rozhraní, které umožňuje výměnu informací mezi uživatelem/provozovatelem a měřicím přístrojem nebo jeho (hardwarovými) komponentami nebo softwarovými moduly.

Poznámka: Typickými příklady uživatelských rozhraní jsou spínače, klávesnice, myš, displej, monitor, tiskárna, dotyková obrazovka, softwarové okno na obrazovce včetně softwaru, který jej generuje.

Validace (Validation): Potvrzení přezkoušením a poskytnutím objektivního důkazu (např. informace, jejíž pravdivost lze dokázat skutečnostmi získanými pozorováním, měřením, zkouškou apod.), že byly splněny specifické požadavky na zamýšlené použití. V tomto případě jsou to požadavky uvedené ve směrnici MID[2].

Ověření (Verification): Poskytnutí objektivního důkazu, že daná položka splňuje stanovené požadavky.

Ověření měřicího přístroje (Verification of a measuring instrument): Postup hodnocení shody (jiný než hodnocení typu), který vyústí v připevnění ověřovací značky a/nebo vydání certifikátu o ověření.

2 Jak tuto příručku používat

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

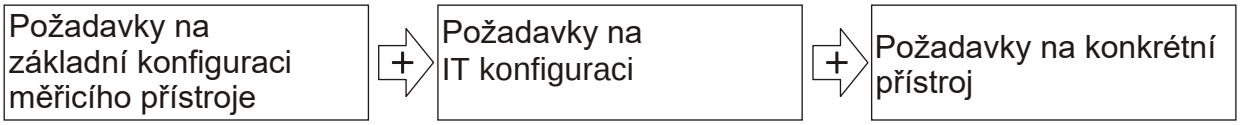
2.1 Celková struktura příručky

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

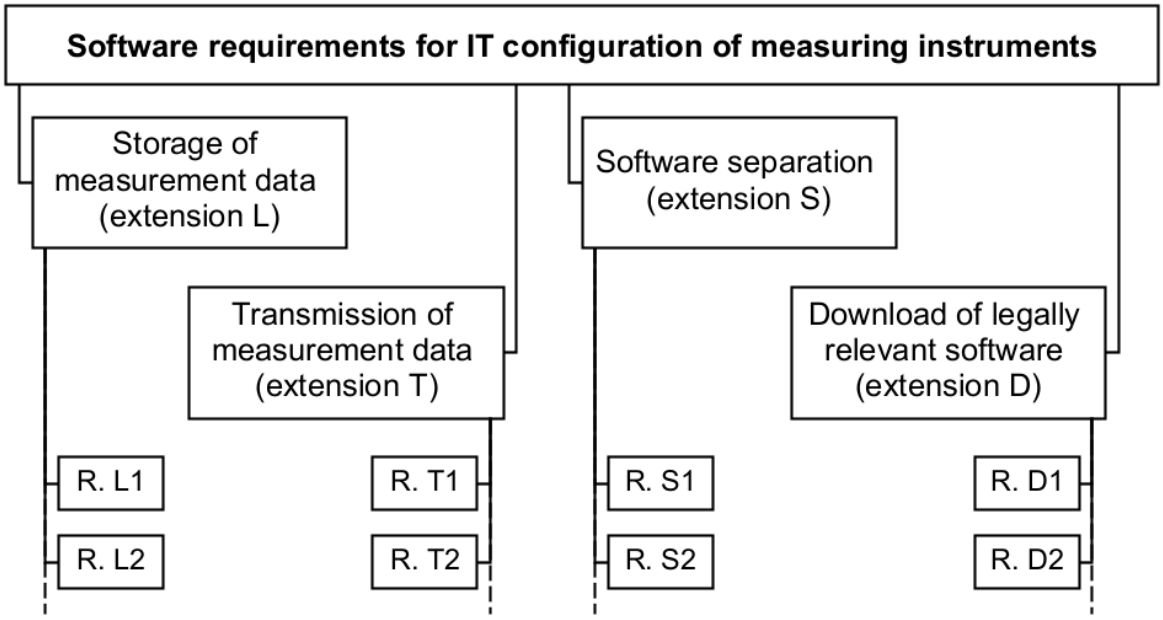
Příručka tedy obsahuje tři základní typy požadavků:

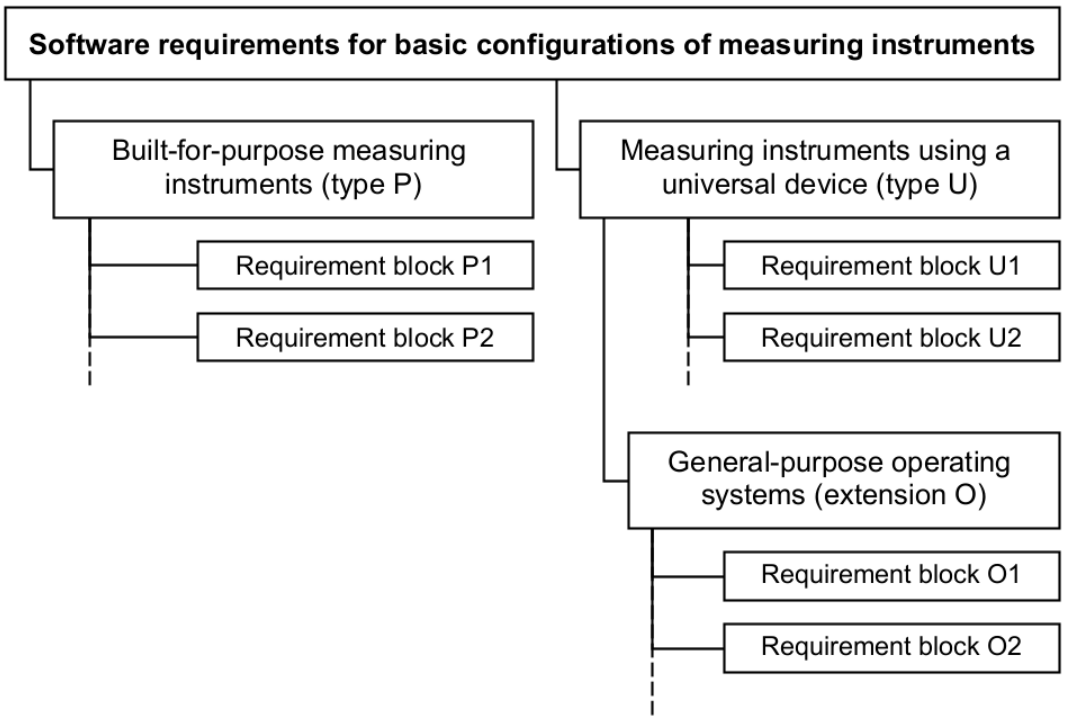
1. požadavky na dvě základní konfigurace měřicích přístrojů (tzv. přístroje typu P a typu U), a požadavky na operační systémy (označované jako rozšíření O),
2. požadavky na čtyři IT konfigurace (tzv. rozšíření L, T, S a D)
3. požadavky na konkrétní přístroje (tzv. rozšíření I.1, I.2 atd.)

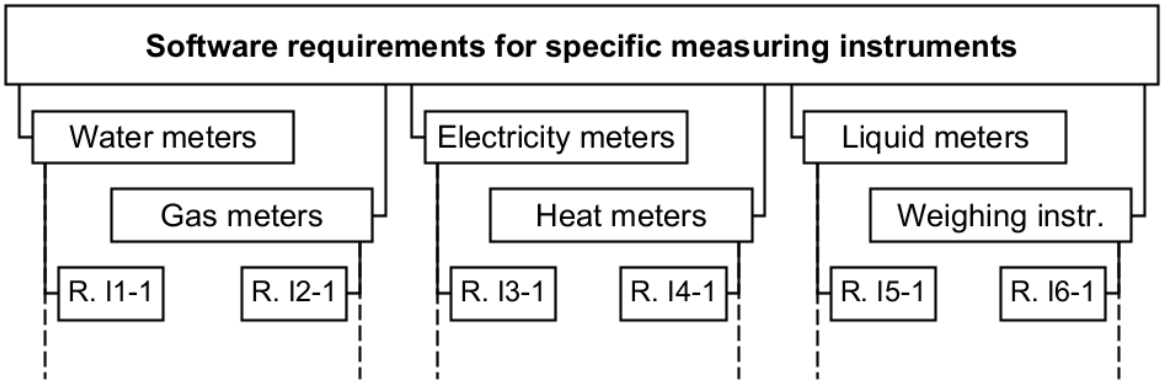
Požadavky prvního typu se vztahují na všechny měřicí přístroje. Pokud jde o operační systém a použitelnost příslušného rozšíření (O), viz podkapitola 2.2. Požadavky druhého typu se týkají následujících IT funkcí: dlouhodobého uložení naměřených dat (L), přenosu naměřených dat (T), stahování softwaru (D) a oddělení softwaru (S). Každou sadu požadavků je třeba aplikovat pouze tehdy, pokud daná funkce existuje. Posledním typem jsou požadavky na konkrétní přístroje. Jejich číslování je shodné s číslováním příloh s požadavky na jednotlivé přístroje ve směrnici MID. Postup aplikování požadavků vztahujících se na daný měřicí přístroj je schematicky znázorněn na obrázku **2-1**.



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


Software requirements for IT configuration of measuring instruments
Storage of measurement data (extension L)
Transmission of measurement data (extension T)
Software separation (extension S)
Download of legally relevant software (extension D)
R. L1
R. L2
R. T1
R. T2
R. S1
R. S2
R. D1
R. D2


Software requirements for basic configurations of measuring instruments
Built-for-purpose measuring instruments (type P)
Measuring instruments using a universal device (type U)
Requirement block P1
Requirement block P2
Requirement block U1
Requirement block U2
General-purpose operating systems (extension O)
Requirement block O1
Requirement block O2



Obrázek 2-2: Přehled souborů požadavků

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

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

2.2 Jak zvolit vhodné části příručky

Tuto přehlednou softwarovou příručku lze použít pro celou řadu měřicích přístrojů. Příručka má modulární podobu. Budete-li postupovat podle níže uvedených pokynů, snadno naleznete příslušné sady požadavků vztahující se na konkrétní přístroj. Přehled jednotlivých sad požadavků naleznete také na **obrázku 2-2**.

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

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

Použije se pouze jedna ze dvou sad požadavků pro základní konfigurace. Zvolte tedy typ základní konfigurace odpovídající danému přístroji: jednoúčelový měřicí přístroj se zabudovaným softwarem (typ P, viz kapitola 4) nebo přístroj využívající univerzální zařízení (typ U, viz kapitola 5). Pokud je vybrán typ U a přístroj je vybaven legálně relevantním operačním systémem, tj. operační systém se používá k naplnění základních požadavků MID nebo může ovlivnit soulad s požadavky, měla by být současně použito rozšíření pro operační systémy (rozšíření O). Pokud rozšíření O není aplikovatelné,

protože předpoklady stanovené v rozšíření neplatí, celý software přístroje by měl být považován za typ P. Pokud se nejedná o celý přístroj, ale pouze o jeho podsestavu nebo komponentu přístroje, rozhodněte se podle této podsestavy nebo komponenty. Vždy aplikujte kompletní sadu požadavků, která patří k příslušné základní konfiguraci a případně rozšíření O.

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

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

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

Za pomoci příslušného rozšíření I, vyberte pro daný druh měřicího přístroje příslušnou skupinu požadavků a aplikujte je.

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

Na základě definic uvedených v rozšíření I pro konkrétní měřicí přístroje zvolte třídu rizika. Třídy rizika jsou zde definovány jednotně pro každou třídu měřicích přístrojů, nebo podle dalšího členění do kategorií, rozsahu platnosti apod. Jakmile určíte příslušnou třídu rizika, je třeba zohledňovat pouze odpovídající požadavky a postup validace.

2.3 Jak pracovat se skupinami požadavků

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

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

Obrázek 2-3: Struktura bloku požadavků

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

Poznámky pro výrobce:

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

Poznámky pro notifikované osoby:

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

2.4 Jak pracovat s kontrolními seznamy

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

Postup:

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

3 Definice tříd rizika

3.1 Obecný princip

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

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

3.2 Popis úrovní ochrany před rizikovými faktory

Jednotlivé úrovně jsou definovány následujícím způsobem:

Úroveň zabezpečení softwaru

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

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

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

Úroveň přezkoušení softwaru

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

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

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

Úroveň shody softwaru

Nízká: Legálně relevantní software jednotlivých přístrojů se považuje za shodný s legálně relevantním softwarem zkoušeného typu, pokud funkce softwaru

odpovídají technické dokumentaci daného typu. Binární kód softwaru nemusí být totožný se softwarem daného typu.

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

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

3.3 Odvození tříd rizika

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

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

Tabulka 3-1: *Definice tříd rizika*

3.4 Popis jednotlivých tříd rizika

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

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

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

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

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

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

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

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

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

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

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

4.1 Technický popis

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

Vestavěný IT systém konktrétně vystihují následující body:

- Software je určen výhradně pro účely měření. Další funkce pro zabezpečení softwaru a dat, pro přenos dat a pro stahování softwaru jsou rovněž určeny výhradně pro účely měření.
- Uživatelské rozhraní slouží pouze k měření, tj. v běžném provozním režimu podléhá legální kontrole. Lze nicméně přepnout do provozního režimu, který nepodléhá legální kontrole.
- Může obsahovat operační systém (OS) nebo jeho subsystémy, pokud
    - veškerou komunikaci řídí legálně relevantní software,
    - neumožňuje nahrávání nebo pozměňování programů, parametrů nebo dat nebo spuštění programů,
    - jestliže neumožňuje změny prostředí legálně relevantní aplikace apod.

  Měla by být zároveň předem nastavena ochrana přístupu a neměla by vyplývat z dodatečné konfigurace příslušných komponent.
- Softwarové prostředí nelze měnit a neexistují žádné interní ani externí nástroje programování nebo pozměňování softwaru se statutem vestavěného softwaru. Stahování softwaru je možné, pouze pokud jsou dodrženy specifické požadavky rozšíření D (kapitola 10).

4.2 Specifické požadavky na přístroje typu P

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

Třída rizika B	Třída rizika C	Třída rizika D

P2: Označení softwaru

Legálně relevantní software musí být jasně označen. Označení musí být přístrojem trvale zobrazeno nebo musí být zobrazeno na příkaz nebo během používání.

Upřesnění:

1. Označení legálně relevantního softwaru může být samostatné nebo může být součástí strukturovaného označení. V druhém případě musí být možné zřetelně rozlišit označení legálně relevantního softwaru. Legálně relevantní softwarové identifikátory mohou být nezávislé nebo součástí dobře strukturovaných identifikátorů. Ve druhém případě musí být legálně relevantní softwarový identifikátor(y) jasně rozlišitelné.
2. . Pokud jsou různé verze softwaru platnými implementacemi téhož typu (např. pro nástroje rizikové třídy B), pak musí být legálně relevantní identifikátor(y) softwaru pro tyto verze stejný(é).
3. . Legálně relevantní softwarové identifikátory jsou typově specifické parametry.
4. . Legálně relevantní identifikátory softwaru musí být snadno zobrazitelné bez nutnosti použití dalšího nástroje.
5. Identifikátor(y) jsou zobrazené permanentně na zajištěném štítku nebo se zobrazí na příkaz či během spuštění.

Požadovaná dokumentace:

1. Dokumentace musí obsahovat (úplné) označení softwaru a popis, jak je tvořeno, jak je zabezpečeno, jak je možné označení zobrazit a jak je strukturováno, aby nemohlo dojít k záměně označení legálně relevantního softwaru s jinými označeními a aby bylo možné vyhodnotit jeho jednoznačnost.
2. V dokumentaci musí být uvedeno, na který legálně relevantní modul se vztahuje, který legálně relevantní softwarový identifikátor.

Postup validace:

Ověření na základě dokumentace:

Zkontrolujte, zda jsou v dokumentaci uvedeny všechny legálně relevantní identifikátory softwaru. Zkontrolujte, zda jsou legálně relevantní moduly jasně popsány tak, aby bylo možné opakovaně zjistit, který modul je zahrnut pod kterým softwarovým identifikátorem. Ověřte popis generování a zobrazení všech právně relevantních softwarových identifikátorů. Zkontrolujte, zda jsou všechny legálně relevantní softwarové identifikátory jedinečné (zejména v případech opakovaného posouzení). *Ověření funkčnosti:*

- Zkontrolujte, zda lze označení legálně relevantního softwaru zobrazit tak, jak je popsáno v dokumentaci.
- Zkontrolujte, zda je označení legálně relevantního softwaru zobrazené přístrojem shodné s označením uvedeným v dokumentaci.
- Zkontrolujte, zda lze jasně rozlišit označení legálně relevantního softwaru od ostatních označení.

Příklad přijatelného řešení:

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

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

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

Třída rizika B	Třída rizika C	Třída rizika D

P3: Vliv uživatelských rozhraní

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

Upřesnění:

1. Každý příkaz musí být jednoznačně přiřazen ke spuštění funkce nebo změně dat.
2. Nezdokumentované příkazy nesmí ovlivňovat legálně relevantní funkce, specifické parametry přístroje ani naměřená data.
3. Části softwaru zajišťující interpretaci příkazů jsou považovány za legálně relevantní software.

Požadovaná dokumentace:

Pokud přístroj umí přijímat příkazy, musí dokumentace zahrnovat:

- Popis příkazů a jejich vliv na legálně relevantní software, specifické parametry přístroje a naměřená data.
- Popis toho, jak jsou legálně relevantní software, specifické parametry přístroje a naměřená data chráněny před ovlivněním jinými vstupy.

Postup validace:

Ověření na základě dokumentace:

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

Ověření funkčnosti:

- Proveďte praktické testy (namátkovou kontrolu) zadáváním zdokumentovaných příkazů.
- Proveďte testy k vyloučení existence nezdokumentovaných příkazů.

Příklad přijatelného řešení:

Softwarový modul, který přijímá a interpretuje příkazy z uživatelského rozhraní. Tento modul patří k legálně relevantnímu softwaru. Dalším modulům legálně relevantního softwaru přeposílá pouze povolené příkazy. Všechny neznámé nebo nepovolené sekvence stisknutí přepínače nebo kláves jsou odmítnuty a nemají žádný vliv na legálně relevantní software, specifické parametry přístroje ani na naměřená data.

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D): Zdrojový kód legálně relevantního softwaru.

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

Ověření na základě zdrojového kódu:

- Ověřte návrh softwaru, zda je tok dat týkající se příkazů jednoznačně definován a realizován pouze legálně relevantním softwarem.
- Hledejte nepřípustný tok dat z uživatelského rozhraní do domén legálně relevantního softwaru, které mají být zabezpečeny.
- Ověřte správné dekódování příkazů (pomocí nástrojů nebo manuálně).
- Ověřte, zda zdrojový kód neobsahuje nedokumentované příkazy.

Třída rizika B	Třída rizika C	Třída rizika D

P4: Vliv komunikačních rozhraní

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

Upřesnění:

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

Požadovaná dokumentace:

Pokud má přístroj rozhraní, dokumentace musí obsahovat:

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

Postup validace:

Ověření na základě dokumentace:

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

Ověření funkčnosti:

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

Příklad přijatelného řešení:

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

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D): Zdrojový kód legálně relevantního softwaru.

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

Ověření na základě zdrojového kódu:

- Ověřte návrh softwaru, zda je tok dat týkající se příkazů legálně relevantního softwaru jednoznačně definován a zda je verifikovatelný.
- Hledejte nepřípustný tok dat z rozhraní do domén, které mají být zabezpečeny.
- Ověřte správné dekódování příkazů (pomocí nástrojů nebo manuálně).
- Ověřte, zda zdrojový kód neobsahuje nezdokumentované příkazy.

Třída rizika B	Třída rizika C	Třída rizika D

P5: Zabezpečení a ochrana legálně relevantního softwaru a specifických parametrů zařízení
Legálně relevantní software a specifické parametry přístroje musí být zabezpečeny proti náhodným či neúmyslným změnám.

Upřesnění:

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

Požadovaná dokumentace:

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

Postup validace:

Ověření na základě dokumentace:

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

Ověření funkčnosti:

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

Příklad přijatelného řešení:

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

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

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

Ověření na základě zdrojového kódu:

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

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">P6: Ochrana softwaru a naměřených dat
Legálně relevantní software a údaje o měření musí být chráněny proti úmyslným změnám.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Ochrana proti manipulaci přes uživatelské rozhraní – viz P3.
2. Ochrana proti manipulaci přes komunikační rozhraní – viz P4.
3. Naměřené údaje se považují za dostatečně chráněné, pokud je zajištěno, že je může zpracovávat pouze legálně relevantní software. Pokud neexistuje žádný legálně nerelevantní software, řeší to ochrana rozhraní v požadavcích P (P3, P4). V případě, že neexistuje legálně nerelevantní software, je dodatečná vnitřní ochrana proti vlivům z legálně nerelevantního softwaru zajištěna prostřednictvím rozšíření S.
4. Úložiště, která obsahují software a data měření, musí být chráněna proti výměně.</td></tr>
<tr><td></td><td colspan="2">Upřesnění:
5. K detekci změn softwaru je použit kontrolní součet nebo jiná alternativní metoda se stejnou úrovní požadavků.
6. Pro kontrolní účely musí být možno vypočítaný kontrolní součet nebo alternativní indikaci modifikace softwaru na příkaz zobrazit.
7. Kontrolní součet nebo alternativní indikace jsou vypočítávány z legálně relevantního softwaru. Software zajišťující výpočet kontrolních součtů nebo alternativních indikací je součástí legálně relevantního softwaru.
8. V případě aplikace kontrolního součtu, délka klíče tohoto algoritmu musí mít nejméně 4 byty (viz také rozšíření L a T).
9. Pokud jde o zacházení s klíči, viz také L5 a T5.</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Dokumentace musí obsahovat popis způsobů zabezpečení.</td></tr>
<tr><td colspan="3">• Popis prostředků zabezpečení softwaru , zejména metodu výpočtu kontrolního součtu a odpovídající nominální hodnotu kontrolního součtu nebo alternativní metodu včetně odpovídající nominální hodnoty.
• Popis metod k zabránění výměny paměti obsahující software.
• Popis programovacího režimu a jeho deaktivace, pokud je to relevantní.</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda jsou zdokumentované prostředky zabezpečení proti nepovolené výměně paměti, na níž je uložen legálně relevantní software a naměřená data, dostatečné.
• Ověřte, zda kontrolní součty / alternativní indikace pokrývají celý legálně relevantní software.

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

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D): Zdrojový kód legálně relevantního softwaru

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

Ověření na základě zdrojového kódu:

- Ověřte, zda jsou prostředky detekce záměrných změn dostatečné.

Třída rizika B	Třída rizika C	Třída rizika D
P7: Ochrana parametrů *Specifické parametry přístroje musí být po svém nastavení zabezpečeny proti nepřípustným změnám.*		
Upřesnění: 1. Určité specifické parametry zařízení může nastavit uživatel, za předpokladu, že jsou chráněny funkcí, která automaticky a nemazatelně zaznamenává jakoukoli úpravu legálně relevantního specifického parametru zařízení, např. auditní stopa. 2. Pokud je to nutné pro účely ověření měřicího přístroje, zobrazení nebo tisk aktuálních relevantních nastavení parametrů musí být možné. 3. Záznamy, které dokládají zásah, musí být na příkaz k dispozici prostřednictvím zobrazení nebo tisku.		
Požadovaná dokumentace: 1. Dokumentace musí popisovat specifické parametry přístroje, zda je lze nastavit, jak se nastavují a jak jsou zabezpečeny. 2. Dokumentace musí popisovat, jak lze specifické parametry zařízení zobrazit nebo vytisknout pro účely ověření měřicího přístroje. 3. Dokumentace musí popisovat, jak lze záznamy, které dokládají zásah, zobrazit nebo vytisknout.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda je po zabezpečení znemožněno provádět změny a úpravy specifických parametrů přístroje bez důkazu zjevného zásahu. • Ověřte, zda jsou zabezpečeny všechny příslušné parametry (specifikované v rozšíření I, pokud takové existují). • Ověřte, zda jsou zobrazeny nebo vytisknuty všechny záznamy, které dokládají zásah. *Ověření funkčnosti:* • Ověřte, zda jsou specifické parametry zařízení adekvátně chráněny. • Ověřte, zda lze specifické parametry zařízení zobrazit nebo vytisknout. • Ověřte, zda lze všechny záznamy, které dokládají zásah, zobrazit nebo vytisknout.		
Příklad přijatelného řešení: a) Parametry jsou zabezpečeny jednak zaplombováním přístroje nebo krytu paměti a dále přidružená zaplombovaná propojka nebo přepínač blokuje možnost zápisu do paměťového okruhu.		
b) *Specifické parametry zařízení jsou chráněny auditní stopou. Změny specifických parametrů zařízení jsou zaznamenány v auditní stopě. Jedná se o informační záznam uložený v nevolatilní paměti. Každý záznam je automaticky generován právně relevantním softwarem a obsahuje:* *• identifikátor parametru (např. název);* *• hodnotu parametru (aktuální nebo předchozí);* *• časové razítko změny.* *Auditní stopa nemůže být smazána ani změněna bez zničení pečetě. Obsah auditní stopy je zobrazen na displeji nebo vytisknut na příkaz.*		

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

Třída rizika C	Třída rizika D
P8: Zobrazení dat z měření *Musí být zaručena autenticita prezentovaných údajů z měření a způsob jejich zobrazení musí být jasný a doplněný všemi informacemi nezbytnými pro informování uživatele o významu výsledku.*	

Upřesnění:

1. Nesmí být možné podvodně simulovat (podvrhnout) legálně relevantní software pro zobrazení údajů z měření.
2. U každého zobrazovaného legálně relevantního údaje o měření musí být jasný jeho význam. Všechny zobrazované legálně relevantní údaje o měření musí být od sebe odlišitelné.
3. Zobrazené legálně relevantní údaje o měření musí být jasně odlišitelné od údajů, které nejsou legálně relevantní.
4. Zobrazené údaje o měření musí být doplněny všemi informacemi, které jsou nezbytné pro jejich interpretaci (např. množství, jednotka, číslo senzoru, hodnota dílku). Pokud jde o nezbytné informace, které mají být k údajům přiloženy, viz L1, T1. Číslo snímače (je-li nutné pro správnou interpretaci výsledku) je legálně relevantní parametr, který je třeba zajistit a chránit, viz P5/U5 a P7/U7.

Požadovaná dokumentace:

Pojmenování modulů, které zajišťují zobrazení legálně relevantních naměřených dat.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda lze zobrazení naměřených dat provádět pouze pomocí legálně relevantního softwaru.

Ověření funkčnosti:

- Ověřte, zda je jasný význam všech předložených legálně relevantních údajů o měření a zda je lze od sebe odlišit.
- Ověřte vizuálně, jestli jsou zobrazená naměřená data snadno odlišitelná od jiných zobrazovaných informací, které mohou být též zobrazeny.
- Ověřte vizuálně, zda jsou zobrazené údaje o měření doplněny všemi potřebnými informacemi.
- Pokud je to relevantní vizuálně zkontrolujte, že zobrazené naměřená data jsou korektně spjata s příslušným zdrojem.

Příklady přijatelných řešení:

1. Zobrazení neobsahuje legálně relevantní údaje, které jsou jasně odlišitelné od legálně relevantních údajů z měření.
2. Snímač zašifruje naměřená data pomocí klíče, který je znám legálně relevantnímu softwaru běžícímu na účelovém zařízení (např. tajné náhodné číslo). Pouze legálně relevantní software může data měření dešifrovat a používat, legálně relevantní moduly nebo součásti nikoli, protože klíč neznají. Požadavky na klíče viz rozšíření T.
3. Před odesláním dat z měření zdroj zahájí sekvenci „handshake“ s legálně relevantním softwarem v zařízení zabudovaném pro daný účel na základě tajných klíčů. Pouze v případě, že legálně relevantní software na účelovém zařízení komunikuje správně, odešle zdrojová jednotka svá naměřená data. Zpracování klíčů viz rozšíření T.

4. Klíč použitý v bodech 1 / 2 je vybrán a vložen do snímače a do softwaru jednoúčelového zařízení bez porušení plomby.	4. Klíč použitý v bodech 1 / 2 je možné vybrat a vložit do snímače a do softwaru jednoúčelového zařízení pouze po porušení plomby

5. Pokud zobrazená naměřená data nejsou explicitně spojena se senzorem, primární senzor přenáší data spolu se svou jednoznačnou identifikací. Všechna zobrazovaná naměřená data jsou označena identifikací příslušného senzoru. Identifikace každého senzoru je legálně relevantním parametrem, který lze i vyčíst na krytu senzoru.

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika C až D): Zdrojový kód legálně relevantního softwaru.

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

Ověření na základě zdrojového kódu:

- Ověřte, zda příslušný software generuje zobrazovaná data měření.
- Ověřte, zda jsou všechna přijatá opatření správná, aby byla zaručena zobrazení naměřených dat legálně relevantním softwarem.

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

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

4.1 Technický popis

Pro měřicí systém typu U jsou obvykle charakteristické následující konfigurace.

Konfigurace hardwaru

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

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

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

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

Konfigurace softwaru

e) Obvykle je využit operační systém.

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

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

Důsledky klasifikace rizik

Software měřicích přístrojů typu U je daleko otevřenější a přístupnější než software měřicích přístrojů typu P, a proto musí být u přístrojů tohoto typu lépe chráněna integrita softwaru. Ke kontrole integrity kódu softwaru je nutné používat zejména kontrolní součty a jiné ekvivalentní metody. Nízká úroveň shody (tj. pouze funkční shoda softwaru a technické dokumentace schvalovaného typu) nepředstavuje adekvátní způsob zajištění integrity softwaru, a tudíž nejnižší možnou třídou, do níž mohou přístroje typu U náležet, je třída rizika C.

4.2 Specifické požadavky na software přístrojů typu U

Třídy rizika C až E
U1: Dokumentace *Základní dokumentace musí kromě specifické dokumentace uvedené v některém z následujících požadavků obsahovat:* a. *Popis funkcí legálně relevantního softwaru, význam dat atd.* b. *Popis uživatelského rozhraní, menu a dialogů.* c. *Označení legálně relevantního softwaru* d. *Přehledné informace o hardwaru systému, zahrnující např. schéma topologického diagramu, typ počítače (počítačů), typ sítě,* e. *Pokud jde o dokumentaci konfigurace operačního systému, viz Rozšíření O.* f. *Operační manuál.*

Třída rizika C a D
U2: Označení softwaru *Legálně relevantní software musí být jasně označen. Označení musí být přístrojem trvale zobrazeno nebo musí být zobrazeno na příkazu nebo během používání.*
Upřesnění: 1. Označení legálně relevantního softwaru může být samostatné nebo může být součástí strukturovaného označení. 2. Pokud je označení legálně relevantního softwaru součástí celkového označení, musí být zřetelně rozlišitelné. 3. Označení každého legálně relevantního modulu, kterým je přístroj vybaven, musí být unikátní. 4. Zobrazit označení legálně relevantního softwaru musí být snadno proveditelné, bez nutnosti použít další nástroje. 5. Označení částí operačního systému je uvedena viz O6. Tyto upřesňující poznámky platí ve spojení s O6 pro identifikaci operačního systému. 6. Označení legálně relevantního softwaru je považováno za specifický parametr daného typu, který musí být náležitým způsobem zabezpečen (viz požadavky U5 a U6). Není-li označení neoddělitelně spojeno se samotným softwarem, jsou požadovány další prostředky zabezpečení. 7. Označení je (jsou) zobrazeno(a) permanentně nebo se zobrazí po zadání příkazu nebo při spuštění.
Požadovaná dokumentace: • Dokumentace musí obsahovat úplné označení softwaru a popis, jak je tvořeno, jak je zabezpečeno, jak je možné označení zobrazit, případně jak je strukturováno, aby bylo možné odlišit označení legálně relevantního softwaru od jiných označení.
Postup validace: *Ověření na základě dokumentace:* • Zkontrolujte, zda dokumentace obsahuje označení legálně relevantního softwaru. • Zkontrolujte, zda jsou všechny legálně relevantní moduly jasně popsány tak, aby bylo možné reprodukovat, který modul je zahrnut, pod kterým softwarovým identifikátorem. • Ověřte popis generování a vizualizace všech legálně relevantních softwarových identifikátorů. • Zkontrolujte, zda jsou všechny legálně relevantní identifikátory softwaru jedinečné (zejména v případech opakovaného přezkoušení). *Ověření funkčnosti:* • Označení softwaru lze zobrazit dle popisu v dokumentaci. • Předložená označení jsou identická s označeními uvedenými v dokumentaci. • Označení legálně relevantního softwaru je odlišitelné od jiných označení.
Příklad přijatelného řešení: a) kontrolní součet kódu programu. b) řetězec doplněný číslem verze, c) řetězec čísel, písmen, jiných znaků, Pokud se výrobce rozhodne pro smíšené označení legálně relevantního a legálně nerelevantního softwaru, pak lze označení jednoduše rozlišit zástupnými znaky v certifikátu schválení typu (TEC), např. „abc1.xx“, kde „abc1“ je označení legálně relevantního softwaru a „xx“ jsou zástupné znaky pro legálně nerelevantní software.

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

<table>
<tr><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="2">U3: Vliv uživatelských rozhraní
Příkazy zadané přes uživatelská rozhraní nesmí nepřípustně ovlivňovat legálně relevantní software, specifické parametry přístroje ani naměřená data.</td></tr>
<tr><td colspan="2">Upřesnění:
1. Každý příkaz musí být jednoznačně přiřazen ke spuštění funkce nebo změně dat.
2. Nezdokumentované příkazy nesmí ovlivňovat legálně relevantní funkce, specifické parametry přístroje ani naměřená data.
3. Příslušné moduly, které interpretují příkazy, jsou považovány za legálně relevantní.</td></tr>
<tr><td colspan="2">Požadovaná dokumentace:
Pokud přístroj dokáže přijímat příkazy, dokumentace musí zahrnovat:
• Popis příkazů a jejich vliv na legálně relevantní software, specifické parametry přístroje a naměřená data.
• Popis toho, jak jsou legálně relevantní software, specifické parametry přístroje a naměřená data zabezpečené před ovlivněním jinými vstupy.</td></tr>
<tr><td colspan="2">Postup validace:
Ověření na základě dokumentace:
• Zkontrolujte, zda jsou zdokumentované příkazy přípustné, tj. zda jejich vliv na legálně relevantní software, specifické parametry přístroje a naměřená data je povolený.
• Zkontrolujte prostředky zabezpečení před ovlivněním jinými příkazy.
Ověření funkčnosti:
• Proveďte praktické testy (namátkovou kontrolu) zadáváním zdokumentovaných příkazů.
• Vyzkoušejte některé kombinace kláves na klávesnici a zkontrolujte, zda nemají vliv na legálně relevantní software, specifické parametry přístroje a naměřená data.
• V případě otevřeného operačního systému s uzavřeným prostředím vyzkoušejte některé nezdokumentované standardní příkazy a ověřte, zda nejsou akceptovány.</td></tr>
<tr><td>Příklad přijatelného řešení:
• Modul v legálně relevantním softwaru odfiltrovává nepřípustné příkazy. Pouze tento modul přijímá příkazy a nelze ho obejít. Jakýkoliv falešný vstup je blokován.</td><td>Příklad přijatelného řešení:
• K používání měřicího systému jsou zřízeny pouze účty s omezenými oprávněními. Přístup k účtu administrátora je blokován dle požadavku U6.
• Uživatelský prostor je uzavřen, tj. uživatel nemůže načítat programy, psát programy ani zadávat příkazy operačnímu systému.</td></tr>
</table>

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

Třída rizika C	Třída rizika D

U4: Vliv komunikačních rozhraní

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

Upřesnění:

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

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

Požadovaná dokumentace:

Pokud má přístroj rozhraní, dokumentace musí obsahovat:

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

Postup validace:

Ověření na základě dokumentace:

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

Ověření funkčnosti:

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

Příklad přijatelného řešení:

- Legálně relevantní modul, který přijímá a interpretuje příkazy z rozhraní. Ostatním legálně relevantním modulům předává pouze povolené příkazy. Všechny neznámé nebo nepovolené příkazy jsou odmítnuty a nemají žádný vliv na legálně relevantní software, specifické parametry zařízení a naměřená data.
- Zásady operačního systému pro sériová připojení a nastavení brány firewall pro síťová připojení zabraňují nepřípustnému provedení příkazu, které by ovlivnilo legálně relevantní aplikaci.

Dodatky pro třídu rizika E

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

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

Ověření na základě zdrojového kódu:

- Ověřte návrh softwaru, zda je tok dat týkající se příkazů legálně relevantního softwaru jednoznačně definován a zda je verifikovatelný.
- Hledejte nepřípustný tok dat z uživatelského rozhraní do domén legálně relevantních dat, které mají být zabezpečeny.
- Ověřte správné dekódování příkazů pomocí nástrojů nebo manuálně.
- Ověřte, zda zdrojový kód neobsahuje nezdokumentované příkazy.

Třída rizika C	Třída rizika D

U5: Zabezpečení a ochrana legálně relevantního softwaru a specifických parametrů zařízení
Legálně relevantní software a specifické parametry přístroje musí být zabezpečeny proti náhodným či neúmyslným změnám.

Upřesnění:

1. Software musí být schopný detekovat změny způsobené fyzikálními vlivy (elektromagnetickým rušením, teplotou, vibracemi atd.).
2. Musí být implementovány prostředky ochrany proti neúmyslnému zneužití / nesprávnému použití uživatelskými rozhraními.
3. Náhodná modifikace legálně relevantního softwaru a specifických parametrů přístroje musí být pravidelně kontrolována kontrolními součty a jejich automatickým porovnáváním s uloženými nominálními hodnotami. Pokud porovnávané hodnoty nesouhlasí, je nutné reagovat způsobem odpovídajícím danému přístroji (např. zastavit měření, označení naměřených datt; viz rozšíření I)
   K odhalení změny stavu softwaru lze použít i alternativní metody.
4. Další ochranná opatření, která je třeba implementovat do operačního systému, viz O4.

Požadovaná dokumentace:

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

Postup validace:

Ověření na základě dokumentace:

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

Příklad přijatelného řešení:

- Aby se zabránilo zneužití operačního systému, přepsání nebo vymazání dat a programů: Je využito všech prostředků ochrany a práv na soukromí, které poskytuje operační systém nebo programovací jazyk.
- Veškerá uživatelská práva pro odstranění, přesun nebo změnu legálně relevantního softwaru jsou zrušena a přístup je řízen pomocí obslužných programů.
- Náhodná změna legálně relevantního softwaru a všech parametrů specifických pro zařízení se kontroluje výpočtem kontrolního součtu spustitelného kódu legálně relevantního softwaru a všech parametrů specifických pro zařízení, jeho porovnáním s nominální hodnotou a zahájením příslušných opatření, pokud byl legálně relevantní spustitelný kód a/nebo parametry specifické pro zařízení změněny, viz rozšíření I pro případné doporučení týkající se příslušných opatření.

Dodatky pro třídu rizika E

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

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

Ověření na základě zdrojového kódu:

- Ověřte, zda jsou prostředky detekce změn (chyb) dostatečné.
- Ověřte, zda jsou v kontrolním součtu zahrnuty všechny legálně relevantní moduly a všechny parametry specifické pro zařízení.

<table>
<tr><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="2">U6: Ochrana softwaru a naměřených dat
Legálně relevantní software a údaje o měření musí být chráněny proti úmyslným změnám.</td></tr>
<tr><td colspan="2">Upřesnění:
1. Údaje z měření se považují za dostatečně chráněné, pokud je zajištěno, že je může zpracovávat pouze legálně relevantní software. To je řešeno ochranou rozhraní v požadavcích U3 a U4. V případě softwaru, který není legálně relevantní, je dodatečná vnitřní ochrana proti vlivům ze strany softwaru, který není legálně relevantní, zajištěna prostřednictvím rozšíření S.
2. Úložiště, která obsahují software a data měření, musí být chráněna proti výměně.
3. Pro podporu detekce modifikací softwaru musí být k dispozici kontrolní součet nebo alternativní metoda se stejnou úrovní ochrany. Vypočtený kontrolní součet nebo alternativní údaj o modifikaci softwaru musí být viditelný na příkaz pro kontrolní účely.
4. Kontrolní součet nebo alternativní indikace se vypočítává z legálně relevantního softwaru. Software zajišťující výpočet kontrolních součtů nebo alternativních indikací je součástí legálně relevantního softwaru.
5. Další ochranná opatření, která je třeba implementovat do operačního systému, viz O4 a O7.
6. V případě aplikace kontrolního součtu, délka klíče tohoto algoritmu musí mít nejméně 4 byty.</td></tr>
<tr><td></td><td>7. Univerzální počítač lze obecně použít pouze tehdy, pokud je možné použít doplňkový hardware zajišťující dodatečné zabezpečení.
8. Při výběru vhodného algoritmu a minimální délky klíče musí být vzaty v úvahu požadavky a doporučení národních a mezinárodních institutů zodpovědných za bezpečnost dat.</td></tr>
<tr><td colspan="2">Požadovaná dokumentace:
• Popis prostředků zabezpečení softwaru a specifických parametrů přístroje, zejména popis metody výpočtu kontrolního součtu a nominálních hodnot nebo alternativní metody s odpovídajícím nominálním údajem.
• Popis metod zabezpečení velkokapacitních pamětí proti jejich výměně (pokud je tento požadavek relevantní).
• Popis zobrazení kontrolních součtů nebo alternativních indikací.</td></tr>
<tr><td colspan="2">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda jsou zdokumentované prostředky ochrany proti výměně paměťového zařízení, které obsahuje legálně relevantní software a údaje o měření, dostatečné.
• Ověřte, zda kontrolní součet (kontrolní součty) nebo alternativní údaj (alternativní údaje) obsahují legálně relevantní software.
• Ověřte, zda jsou opatření přijatá k zabránění modifikace nebo nahrazení legálně relevantního softwaru pomocí operačního systému dostatečná.

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

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

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

Třída rizika C	Třída rizika D

U7: Ochrana parametrů
Specifické parametry přístroje musí být zabezpečeny proti nepřípustným změnám.

Upřesnění:
1. Určité specifické parametry zařízení mohou být nastaveny uživatelem za předpokladu, že jsou chráněny zařízením, které automaticky a nesmazatelně zaznamenává jakoukoli úpravu právně relevantního specifického parametru zařízení, např. auditní stopou.
2. Je-li to nezbytné pro účely ověření měřicího přístroje, musí být možné zobrazit nebo vytisknout aktuální nastavení příslušného parametru.
3. Záznamy, které jsou důkazem zásahu, musí být na příkaz zpřístupněny prostřednictvím zobrazení nebo tisku.

Požadovaná dokumentace:
1. Dokumentace musí popisovat, jak jsou specifické parametry zařízení chráněny, zda je lze nastavit a jak se nastavují.
2. Dokumentace musí popisovat, jak lze zobrazit nebo vytisknout specifické parametry zařízení pro účely ověření měřicího přístroje.
3. Dokumentace musí popisovat, jak lze zobrazit nebo vytisknout záznamy, které poskytují důkaz o zásahu.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda je po nastavení znemožněno provádět změny a úpravy specifických parametrů přístroje.
- Ověřte, zda jsou zabezpečeny všechny příslušné parametry (uvedené v rozšíření I, pokud existují).
- Ověřte, zda jsou zobrazeny nebo vytištěny všechny záznamy, které poskytují důkaz o zásahu.

Ověření funkčnosti:

- Ověřte, zda jsou parametry specifické pro zařízení dostatečně chráněny.
- Ověřte, zda lze zobrazit nebo vytisknout parametry specifické pro zařízení.
- Ověřte, zda lze zobrazit nebo vytisknout všechny záznamy, které poskytují důkaz o zásahu.

Příklad přijatelného řešení:
- Parametry jsou zabezpečeny jednak zaplombováním přístroje nebo krytu paměti a dále přidružená zaplombovaná propojka nebo přepínač blokuje možnost zápisu do paměťového okruhu.
- Specifické parametry zařízení jsou chráněny auditní stopou. Změny specifických parametrů zařízení jsou zaznamenány v auditní stopě. Jedná se o informační záznam uložený v nevolatilní paměti. Každý záznam je automaticky generován legálně relevantním softwarem a obsahuje:
  - identifikátor parametru (např. název);
  - hodnotu parametru (aktuální nebo předchozí);
  - časové razítko změny.

Auditní stopa nemůže být smazána ani změněna bez zničení pečetě. Obsah auditní stopy je zobrazen na displeji nebo vytisknut na příkaz.

Dodatky pro třídu rizika E

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

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

Ověření na základě zdrojového kódu:
- Ověřte, zda jsou prostředky na ochranu parametrů dostatečné.

Třída rizika C	Třída rizika D
U8: Zobrazení dat z měření *Musí být zaručena autenticita zobrazených údajů z měření a způsob jejich zobrazení musí být jasný a doplněný všemi informacemi nezbytnými pro informování uživatele o významu výsledku.*	

Upřesnění:

1. Nesmí být možné podvodně simulovat (podvrhnout) legálně relevantní software pro zobrazení údajů z měření.
2. U každého zobrazovaného legálně relevantního údaje o měření musí být jasný jeho význam. Všechny zobrazované právně relevantní údaje o měření musí být od sebe odlišitelné.
3. Zobrazované legálně relevantní údaje o měření musí být jasně odlišitelné od údajů, které nejsou legálně relevantní.
4. Zobrazované údaje o měření musí být doplněny všemi informacemi, které jsou nezbytné pro jejich interpretaci (např. množství, jednotka, číslo senzoru, hodnota dílku). Pokud jde o nezbytné informace, které mají být k údajům přiloženy, viz L1, T1. Číslo snímače (je-li nutné pro správnou interpretaci výsledku) je legálně relevantní parametr, který je třeba zajistit a chránit, viz P5/U5 a P7/U7.

Požadovaná dokumentace:

Pojmenování modulů, které umožňují zobrazení legálně relevantních údajů z měření.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda lze zobrazení naměřených dat provádět pouze pomocí legálně relevantního softwaru.
- Ověřte, zda mohou být naměřená data zobrazována pouze legálně relevantním softwarem.
- Pokud zdroj zobrazených naměřených dat není implicitně identifikovatelný či ověřitelný ověřte, zda zdroj těchto dat je identifikován a indikován legálně relevantním softwarem.

Ověření funkčnosti:

- Ověřte, zda je význam všech předložených legálně relevantních údajů o měření jasný a zda je lze od sebe odlišit.
- Ověřte vizuálně, jestli jsou zobrazovaná naměřená data snadno odlišitelná od jiných zobrazovaných informací, které mohou být též zobrazeny.
- Ověřte vizuálně, zda jsou prezentované údaje o měření doplněny všemi potřebnými informacemi.
- Pokud je to relevantní vizuálně zkontrolujte, že zobrazovaná naměřená data jsou korektně spjata s příslušným zdrojem.

Příklady přijatelných řešení:

1. Snímač zašifruje naměřená data pomocí klíče, který je znám legálně relevantnímu softwaru běžícímu na účelovém zařízení (např. tajné náhodné číslo). Pouze legálně relevantní software může data měření dešifrovat a používat, legálně relevantní moduly nebo součásti nikoli, protože klíč neznají. Požadavky na klíče viz rozšíření T.
2. Před odesláním dat z měření zdroj zahájí sekvenci „handshake“ s legálně relevantním softwarem v zařízení zabudovaném pro daný účel na základě tajných klíčů. Pouze v případě, že legálně relevantní software na účelovém zařízení komunikuje správně, odešle zdrojová jednotka svá naměřená data. Zpracování klíčů viz rozšíření T.

3. Klíč použitý v bodech 1 / 2 je vložen do snímače a do softwaru jednoúčelového zařízení bez porušení plomby.	3. Klíč použitý v bodech 1 / 2 je možné vložit do snímače a do softwaru jednoúčelového zařízení pouze po porušení plomby

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika C až D): Zdrojový kód legálně relevantního softwaru.
Postup validace (kromě postupu požadovaného pro třídy rizika C až D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda zobrazená naměřená data generuje legálně relevantní software. • Ověřte, zda jsou všechna přijatá opatření správná, aby byla zaručena zobrazení naměřených údajů legálně relevantním softwarem.

6. Rozšíření O: operační systémy pro obecné použití

Specifické požadavky této kapitoly se uplatňují pouze v případě, že operační systém na součásti měřicího přístroje je legálně relevantní, tj. operační systém se používá k plnění základních požadavků MID nebo může ovlivnit soulad s požadavky. Jedná se o doplněk k specifickým požadavkům na software pro měřicí přístroje používající univerzální zařízení (požadavky typu U). Tyto požadavky nemusí být uplatňovány u měřicích přístrojů typu P.

6.1 Technický popis

Software je popsán jako operační systém pro všeobecné účely, pokud systémové zdroje měřicího přístroje (CPU, paměť, rozhraní) jsou tímto softwarem spravovány a jsou poskytnuty legálně relevantní aplikaci. Kromě toho má operační systém schopnost více uživatelů a režim správy (operační systém pro více uživatelů). Jakýkoliv operační systém pro všeobecné účely, který byl vyhodnocen dle tohoto rozšíření, musí splňovat následující předpoklady:

- musí být prokázáno, že se používá,
- musí být vhodný pro všeobecný účel,
- musí být technicky nejmodernější[2] a
- nesmí být vyvinut výrobcem měřicího přístroje, dílčí sestavy nebo výrobcem komponentu. Výrobce nebo producent však může přispět k OS pokud jde o ovladače nebo moduly, které jsou speciálně naprogramovány pro legálně relevantní úkol, za předpokladu, že jsou splněny požadavky O6 a O7, tj. ovladače nebo moduly, které jsou speciálně naprogramovány pro legálně relevantní úkol, musí mít vlastní identifikaci a ochranu.

V tomto případě může být softwarové zkoušení operačního systému pro všeobecné účely omezeno na zkoušení legálně relevantní konfigurace na základě požadavků v Rozšíření O. Každé z implementovaných ochranných opatření lze kombinovat s opatřeními na hardwarové úrovni nebo na úrovni legálně relevantní aplikace.

6.2 Aplikace požadavků na komponenty

S ohledem na volně dostupné operační systémy rozlišuje toto rozšíření dvě kategorie komponent měřicích přístrojů, viz definice komponent kategorií 1 a 2 v kapitole 1.

Tato kapitola se vztahuje pouze na komponenty měřicího přístroje, které lze hodnotit samostatně za podmínek uvedených v průvodci WELMEC 8.8. V případě kompletního přístroje se uplatní požadavky komponenty kategorie 1.

Pro komponenty z kategorie 2:

- O2 se neuplatňuje.
- O3, O4 a O5 se uplatňují v plném rozsahu.
- O1, O6 a O7 se vztahují na konfiguraci/nastavení OS.

V tomhle případějsou možné pravidelné aktualizace operačního systému, pokud neovlivní konfiguraci. Technické pracovní skupiny mohou rozhodnout, které komponenty kategorie 2 (pokud jsou nějaké) mohou být předmětem této výjimky.

[2] tj. byly použity opravy všech známých chyb a zranitelností.

U některých typů operačních systémů může aktualizace vést k zásadním změnám, které ovlivní i konfiguraci (např. hlavní aktualizace verze ve Windows nebo v běžné distribuci Linuxu založené na Debianu). V takovém případě by výše uvedená výjimka neplatila.

6.3 Specifické požadavky na operační systémy pro obecné použití

<table>
<tr><th>Třída rizika C</th><th>Třída rizika D</th><th>Třída rizika E</th></tr>
<tr><td colspan="3">O1: Ochrana hardwaru
Hardwarová část, na které běží legálně relevantní operační systém, musí být chráněna proti úmyslným změnám.</td></tr>
<tr><td colspan="3">Upřesnění:
1.U komponent kategorie 1 a kompletních přístrojů musí být legálně relevantní operační systém chráněn proti vyjmutí nebo výměně.
2.Hardwarová rozhraní, která by mohla ovlivnit operační systém, musí být buď odpojena od napájení, vyřazena z provozu operačním systémem, chráněna hardwarovou plombou nebo vázána na ochranné rozhraní (viz O5).
3.Rozhraní s přímým přístupem do paměti musí být chráněna hardwarovou plombou.
4.Operační systém musí používat ochranu paměti, aby zabránil získání citlivého kryptografického materiálu.</td></tr>
<tr><td colspan="2">Požadovaná dokumentace:
• Seznam všech komponent operačního systému.
• Popis ochranných opatření pro hromadná úložiště.
• Popis ochranných opatření hardwarových rozhraní.</td><td>Požadovaná dokumentace (kromě dokumentace pro rizikovou třídu C):
• Pokud se používá kryptografický materiál: Popis ochranných opatření pro volatilní paměť a paměťová zařízení.</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda jsou zdokumentovány všechny komponenty s legálně relevantním operačním systémem.
• Ověřte, zda jsou všechna hardwarová rozhraní chráněná nebo nezbytná pro legálně relevantní výměnu dat, v takovém případě musí být vybavena ochranným rozhraním, viz U4.
• Ověřte, zda jsou všechna opatření na ochranu paměti, hromadných úložišť a hardwarových rozhraní účinná a adekvátní.</td></tr>
<tr><td colspan="2"></td><td>Ověření na základě konfiguračních souborů:
• Ověřte, zda konfigurace operačního systému pro ochranu paměti odpovídá opatřením popsaným v dokumentaci.
Ověření funkčnosti:
• Ověřte, zda jsou dodatečná ochranná opatření pro legálně relevantní operační systém a kryptografický materiál efektivní.</td></tr>
<tr><td colspan="3">Příklad přijatelného řešení:
• Kryt měřicího přístroje je fyzicky chráněn plombami, aby se zabránilo výměně hromadných úložišť, nebo jsou hromadná úložiště během používání opatřena zaplombovanými přípojkami.
• Hardwarová plomba je použita k zajištění toho, aby nemohlo dojít k výměně nebo vyjmutí hromadného úložiště, na kterém se nachází legálně relevantní operační systém.</td></tr>
<tr><td colspan="2"></td><td>• Kryptografický materiál, například hesla, je uložen v samostatné hardwarové komponentě, která je chráněna proti přístupu prostřednictvím operačního systému.</td></tr>
</table>

<table>
<tr><th>Třída rizika C</th><th>Třída rizika D</th><th>Třída rizika E</th></tr>
<tr><td colspan="3">O2: Bootovací proces
U komponent kategorie 1 a kompletních přístrojů musí konfigurace bootovacího procesu poskytovat stejně nakonfigurované prostředí pro spuštění legálně relevantního softwaru.</td></tr>
<tr><td colspan="3">Upřesnění:
1.Proces bootování operačního systému musí být jednoznačný a reprodukovatelný.
2.Do postupu pro spuštění univerzálního zařízení musí být zahrnuta legálně relevantní softwarová aplikace
3.Bootovací konfigurace musí být chráněna proti změnám.
4.Na konci bootovacího procesu se vytvoří důvěryhodný řetězec nad jednotlivými součástmi bootovacího procesu.
5.Zpracování důvěryhodného řetězce může být přerušeno, pokud je zachována integrita důvěryhodného řetězce.
6. Bootování přes otevřená rozhraní je zakázáno.</td></tr>
<tr><td></td><td colspan="2">7. Proces bootování musí být zajištěn odpovídajícími prostředky v závislosti na úrovni ochrany</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
• Informace o konfiguraci bootování operačního systému (např. paměťové médium, oddíly, parametry jádra).
• Popis ochranných opatření pro bootovací proces.
• Popis struktury řetězce důvěryhodnosti.
• Popis bootovacího prostředí operačního systému pro legálně relevantní software.</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda je konfigurace bootovacího procesu chráněna proti nepřípustným změnám.
• Ověřte, zda se operační systém při každém bootování spustí do stejného zabezpečeného prostředí legálně relevantní software.
• Ověřte, zda nedochází k nezdokumentovaným přerušením bootovacího procesu.
• Ověřte, zda je zakázáno bootování přes otevřená rozhraní.</td></tr>
<tr><td></td><td colspan="2">Ověření na základě konfiguračních souborů:
• Ověřte, zda jsou použitá kryptografická opatření účinná a zda odpovídají požadavkům nebo doporučením vnitrostátních a mezinárodních institucí odpovědných za bezpečnost dat.
Ověření funkčnosti:
• Ověřte, zda je konfigurace boot loaderu jednoznačná.
• Ověřte, zda je možné bootovat operační systém prostřednictvím otevřených rozhraní.</td></tr>
<tr><td colspan="3">Příklad přijatelného řešení:
• Bootovací konfigurace (BIOS) byla zabezpečena silným heslem. Integrita bootloaderu a legálně relevantních částí operačního systému je kontrolována pomocí kontrolního součtu.
• Modul TPM (trusted platform module) ověřuje elektronický podpis bootloaderu, bootloader pak ověřuje operační systém, který následně ověřuje a spouští legálně relevantní aplikace.</td></tr>
<tr><td></td><td colspan="2">• Zabezpečené bootování: Boot loader může načíst pouze podepsané jádro (kernel). Před bootováním operačního systému se ověří elektronický podpis jádra.</td></tr>
</table>

<table>
<tr><th>Třída rizika C</th><th>Třída rizika D</th><th>Třída rizika E</th></tr>
<tr><td colspan="3">O3: Systémové prostředky
Konfigurace operačního systému musí zajistit dostatek prostředků pro provoz legálně relevantní aplikace.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Operační systém by měl být nakonfigurován co možná nejvíce omezeně.
2. Prostředky legálně relevantní softwarové aplikace nejsou snižovány pod nezbytné minimum jiným softwarem (legálně relevantním i legálně nerelevantním).</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
• Informace o konfiguraci nainstalovaných částí operačního systému.</td></tr>
<tr><td></td><td colspan="2">• Informace o probíhajících procesech během používání měřicího přístroje</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda jsou nainstalované části operačního systému vhodné a dostatečně nakonfigurované pro zajištění provozu měřicího přístroje.</td></tr>
<tr><td colspan="3">Ověření funkčnosti:
• Ověřte, zda export běžících procesů odpovídá dokumentaci.
• Výrobce prostřednictvím ukazatele využití systému ověří, zda jsou během používání k dispozici dostatečné systémové prostředky pro legálně relevantní aplikaci.</td></tr>
<tr><td colspan="3">Příklad přijatelného řešení:
• Pomocí správy balíčků operačního systému výrobce odstraní všechny nepotřebné programy.
• Výrobce omezí dobu běhu pro legálně nerelevantní úlohy.
• Hierarchie přerušení je navržena tak, aby nedocházelo k nežádoucím vlivům.</td></tr>
</table>

Třída rizika C	Třída rizika D	Třída rizika E

O4: Ochrana během používání

Operační systém musí být nakonfigurován tak, aby legálně relevantní software nemohl být nepřípustně ovlivňován funkcemi operačního systému nebo jiným softwarem.

Upřesnění:

1. Úkoly správy legálně relevantního softwaru (aplikace a operační systém) musí být zabezpečeny.
2. Ovládání přístupu musí být nakonfigurováno tak, aby nebylo možné nepřípustně ovlivnit zamýšlené použití.
3. Přístupová oprávnění musí být pravidelně kontrolována legálně relevantním operačním systémem.
4. Operační systém musí být nakonfigurován tak, aby zabránil odstranění legálně relevantního softwaru.
5. Připojení přídavných zařízení nesmí mít nepřípustný vliv na operační systém ani na nastavení konfigurace.

Požadovaná dokumentace:

- Seznam připojených nebo připojitelných úložných médií s jejich atributy a zásadami pro omezení jejich použití.
- Popis správy řízení přístupu uživatelů a ochrany účtu správce.
- Popis provozního režimu grafického uživatelského rozhraní.
- Popis připojení přídavných zařízení.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda je používání legálně relevantní aplikace je odděleno od správy systému, tj. zda legálně relevantní aplikace nemůže měnit žádnou legálně relevantní správu/konfiguraci operačního systému.
- Ověřte, zda jsou bezpečnostní opatření účtu správce dostatečná a zda neexistuje druhý účet s nepřípustnými právy správce.
- Ověřte, zda z připojeného paměťového média nelze spustit nepřípustný software.
- Ověřte, zda nelze vyvolat prostřednictvím vstupních zařízení (např. klávesových zkratek) nebo uživatelského prostředí nepřípustné funkce operačního systému.
- Ověřte, zda řízení aplikace umožňuje spouštění pouze legálně relevantního softwaru, pokud nebylo zavedeno oddělení softwaru.
- Ověřte, zda připojení přídavných zařízení neovlivňuje nepřípustným způsobem legálně relevantní operační systém nebo konfigurační nastavení.
- Ověřte, zda nelze resetovat nebo změnit právně relevantní nastavení operačního systému.

Ověření funkčnosti:

- Ověřte, zda je účet správce během používání uzamčen.
- Ověřte, zda byly deaktivovány všechny nepřípustné klávesové zkratky.
- Ověřte, zda není možné opustit nebo změnit provozní režim grafického uživatelského rozhraní.
- Ověřte, zda je účinná kontrola aplikací a zásad pro paměťová média a přídavná zařízení.
- Ověřte, zda se po restartu zachovají legálně relevantní nastavení.

Ověření na základě konfiguračních souborů:

Ověřte, zda:

- uživatelská a skupinová oprávnění, účet správce,
- konfigurace řízení aplikace,
- připojených úložných médií a také diskových oddílů nebo médií s atributy přístupu,
- zásady pro úložná média a přídavná zařízení,

odpovídají informacím uvedeným v dokumentaci a jsou správně nakonfigurovány.

Příklad přijatelného řešení: • Všechny legálně relevantní úlohy jsou v počítači sdruženy do jedné dynamicky propojitelné knihovny. • Kryptografické prostředky zajišťují, že pouze legálně relevantní dynamicky propojitelná knihovna může komunikovat se senzorem připojeným k počítači. • Okno zobrazující legálně relevantní údaje je generováno a řízeno postupy v legálně relevantní dynamicky propojitelné knihovně. • Během měření tyto procedury cyklicky kontrolují, zda je příslušné okno stále nahoře nad všemi ostatními otevřenými okny; pokud tomu tak není, procedury jej umístí nahoru, zatímco prioritizace procesů zajišťuje, aby ostatní I/O zařízení trvale nebránila procesoru.	**Příklad přijatelného řešení:** • Operační systém disponuje zabezpečeným účtem správce pro úlohy správy a také uživatelským účtem s omezenými právy pro použití během měření. • Operační systém se při každém bootovaní nastaví do režimu kiosku, v němž jsou přístupné pouze legálně relevantní aplikace. Klávesové zkratky byly omezeny na legálně relevantní použití. • Přístup k vyměnitelným médiím a přídavným zařízením byl omezen pomocí skupinových zásad. • V systému nejsou žádné adresáře s právy pro zápis a spouštění souborů • Účet správce byl trvale deaktivován.

<table>
<tr><th>Třída rizika C</th><th>Třída rizika D</th><th>Třída rizika E</th></tr>
<tr><td colspan="3">O5: Ochranné rozhraní
Funkce operačního systému přístupné přes otevřená rozhraní nesmí nepřípustně ovlivňovat legálně relevantní software, legálně relevantní parametry nebo údaje o měření.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Komunikace s legálně relevantním operačním systémem musí probíhat prostřednictvím ochranných rozhraní.
2. V případě separace softwaru v operačním systému platí rozšíření S a rozšíření T pro otevřené sítě pro přenos legálně relevantních dat měření prostřednictvím ochranných rozhraní operačního systému.
3. Pokud konfigurace operačního systému zajišťuje, že komunikačním partnerem připojeným k otevřenému rozhraní může být pouze certifikovaná součást a spojení je chráněné, není nutná žádná další kontrola rozhraní.</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
• Popis konfigurace operačního systému pro otevřená hardwarová a softwarová rozhraní a způsob jejich ochrany.
• Seznam otevřených hardwarových a softwarových rozhraní, která nejsou konfigurována operačním systémem.
• Seznam všech přijímaných příkazů a jejich vlivu pro všechna otevřená rozhraní spravovaná operačním systémem.</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda otevřená rozhraní nemají nepřípustný vliv na legálně relevantní operační systém, jeho konfiguraci, legálně relevantní softwarovou aplikaci, legálně relevantní parametry nebo naměřená data.</td></tr>
<tr><td colspan="2"></td><td>Ověření na základě konfiguračních souborů:
Pro následující otevřená rozhraní se ověří, zda je zabráněno nepřípustnému ovlivnění:
• síťová rozhraní (otevřené a uzavřené porty, používané protokoly a příkazy, zásady),
• sériová rozhraní (příkazový interpret aplikace, zásady pro řízení uživatelských účtů
• softwarová rozhraní operačního systému (příkazy pro řízení přístupu).
Kromě toho se ověří zda jsou použitá kryptografická opatření účinná a zda odpovídají požadavkům nebo doporučením vnitrostátních a mezinárodních institucí odpovědných za bezpečnost údajů.

Ověření funkčnosti:
• Ověřte účinnost konfigurace otevřených sériových rozhraní.
• Ověřte účinnost konfigurace otevřených síťových rozhraní.</td></tr>
<tr><td colspan="3">Příklad přijatelného řešení:
• Všechna hardwarová rozhraní s výměnou měřených dat se konfigurují prostřednictvím operačního systému (síťový firewall, zásady USB).</td></tr>
<tr><td colspan="2"></td><td>Příklad přijatelného řešení:
• Používání bezpečnostních protokolů IT (VPN, PISEC) pro otevřené sítě.</td></tr>
</table>

Třída rizika C	Třída rizika D	Třída rizika E

O6: Identifikace operačního systému a jeho konfigurace

Operační systém a jeho konfigurace musí být identifikovatelné. Identifikace operačního systému a identifikace konfigurace operačního systému musí být zobrazena na příkaz nebo během provozu.

Upřesnění:

1. Pokud jsou legálně relevantní software a účet měřicí úlohy chráněny specifickou konfigurací operačního systému, musí mít příslušné konfigurační soubory vlastní identifikátor.
2. Identifikace zahrnuje moduly (moduly jádra, ovladače, knihovny) operačního systému, které byly upraveny nebo specificky naprogramovány pro legálně relevantní úlohu.

Požadovaná dokumentace:

- Obecné informace o operačním systému (výrobce, distribuce, název produktu, verze jádra).
- Informace o identifikaci modulů operačního systému nakonfigurovaných pro legálně relevantní úkol.
- Informace týkající se identifikace upravených nebo přidaných modulů operačního systému vyvinutých vlastními prostředky pro legálně relevantní úkol.
- Seznam všech používaných identifikátorů a popis způsobu jejich vytvoření, jejich označení a způsobu jejich odlišení od identifikátorů, které nejsou legálně relevantní.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda byly zdokumentovány všechny identifikátory legálně relevantní konfigurace operačního systému.
- Ověřte, zda byly zdokumentovány všechny identifikátory upravených nebo přidaných modulů.
- Ověřte, zda jsou všechny identifikátory operačního systému jednoznačné a zda je pokrytí legálně relevantních modulů operačního systému úplné a srozumitelné.
- Ověřte, zda je vytvoření, uvedení a ochrana identifikátorů, jakož i jejich odlišení od jiných legálně nerelevantních identifikátorů, plně zdokumentováno a zda nejsou mezi nimi rozpory.

Ověření funkčnosti:

- Ověřte označení identifikátorů operačního systému a porovnejte je s dokumentací.

Příklad přijatelného řešení:

- Identifikátor se skládá z názvu výrobce operačního systému, názvu produktu a verze operačního systému. Alternativně se používá název a verze distribuce a verze jádra
- Kromě toho jsou moduly operačního systému nakonfigurované pro legálně relevantní úlohu identifikovány pomocí kontrolního součtu.

<table>
<tr><th>Třída rizika C</th><th>Třída rizika D</th><th>Třída rizika E</th></tr>
<tr><td colspan="3">O7: Ochrana operačního systému
Operační systém musí být chráněn proti úmyslným změnám.</td></tr>
<tr><td colspan="3">Upřesnění:

1. Moduly operačního systému (moduly jádra, ovladače, knihovny), které jsou speciálně naprogramovány pro legálně relevantní úkol, mají vlastní ochranu.
2. Ochranná opatření pro operační systém musí kompletně pokrývat všechny legálně relevantní moduly. Výjimkou může být zahrnutí konfigurace bootloaderu do ochranného opatření namísto samotného bootloaderu, pokud není součástí systémových souborů operačního systému.
3. Pokud se používá kontrolní součet nebo rovnocenné ochranné opatření, měly by být vypočteny pomocí operačního systému. Vypočtený kontrolní součet nebo rovnocenné ochranné opatření musí být uvedeno operačním systémem nebo legálně relevantní aplikací.
4. Integrita legálně relevantního operačního systému se pravidelně kontroluje. Pokud kontrola integrity selže, je nutné provést adekvátní opatření, která jsou pro daný přístroj vhodná.
5. Tento požadavek se netýká aktualizací legálně relevantních modulů operačního systému. Tyto aktualizace spadají do rozšíření D.</td></tr>
<tr><td colspan="2"></td><td>6. Kontrolní součet se získá pomocí kryptograficky silných metod.</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
• Dokumentace ochranných opatření operačního systému.
• Popis metod pro vytvoření a uvedení ochranných opatření
• Kompletní seznam legálně relevantních modulů operačního systému</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
• Zkontrolujte, zda jsou všechny legálně relevantní moduly operačního systému dostatečně pokryty ochrannými opatřeními.
• Zkontrolujte, zda je vytvoření a uvedení ochranných opatření plně zdokumentováno a zda neobsahuje žádné nesrovnalosti.
Ověření funkčnosti:
• Pokud byl použit kontrolní součet: Ověřte, zda údaj o kontrolním součtu pro legálně relevantní moduly operačního systému (viz definice pro kategorie 1 a 2) a porovnejte jej s referenčními hodnotami uvedenými v dokumentaci.
• Pokud byla použita alternativní opatření: Zkontrolujte prototyp a porovnejte jej s dokumentací.</td></tr>
<tr><td colspan="2"></td><td>• Ověřte, zda jsou použitá kryptografická opatření účinná a zda odpovídají požadavkům nebo doporučením vnitrostátních a mezinárodních institucí odpovědných za bezpečnost dat.</td></tr>
<tr><td colspan="3">Příklad přijatelného řešení:
• Linux: Kontrolní součet zahrnující zavaděč, jádro a adresář apod.
• Windows: Kontrolní součet zahrnující části systémového adresáře, části exportovaného registru a části nastavení zásad týkajících se uživatelských oprávnění, brány firewall, USB atd.</td></tr>
<tr><td>• Kontrolní součet je CRC32.</td><td colspan="2">• Kontrolní součet je hodnota SHA (bezpečný hashovací algoritmus) o délce doporučené agenturou ENISA.</td></tr>
</table>

7. Rozšíření L: Uložení naměřených dat

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

Uložení zahrnuje dobu od okamžiku, kdy je měření fyzicky dokončeno, do okamžiku, kdy jsou dokončeny všechny procesy, které má provést legálně relevantní software. Může se také vztahovat na dlouhodobé uložení výsledku měření, aby byl k dispozici po dokončení měření pro pozdější legálně relevantní účely.

7.1 Technický popis

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

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

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

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

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

Tabulka 7-1: Technický popis pamětí pro dlouhodobé uložení dat

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

7.2 Specifické požadavky na software pro uložení dat

Třída rizika B	Třída rizika C	Třída rizika D
L1 Úplnost uložených naměřených dat *Ukládaná naměřená data musí být doplněna všemi náležitými informacemi potřebnými pro legální účely.* **Upřesnění:** 1. Musí být možné zpětně dohledat měření, při němž uložená naměřená data vznikla. 2. Uložená naměřená data musejí být dostačující pro kontrolu faktur. 3. Druh požadované informace se může odvíjet od typu přístroje. 4. Předpokladem splnění tohoto specifického požadavku je označení každého jednotlivého uloženého bloku dat.		
Požadovaná dokumentace: Popis všech položek bloku dat.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda blok dat obsahuje všechny informace potřebné pro legálně relevantní účely.		
Příklad přijatelného řešení: • Blok dat, který je z legálního a metrologického hlediska úplný, musí být tvořen následujícími položkami: º naměřené hodnoty s dostatečným rozlišením º jednotka měření º cena za jednotku nebo cena k zaplacení (je-li relevantní) º datum a čas měření (je-li relevantní) º označení přístroje º místo měření (je-li relevantní) • Data jsou uložena ve stejném rozlišení, hodnotách, jednotkách atd., jako je indikováno při měření nebo je vytištěno na dodacím dokladu.		

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

Třída rizika B	Třída rizika C	Třída rizika D

L2: Zabezpečení a ochrana uložených dat měření
Uložená naměřená data musí být chráněna proti náhodným a neúmyslným změnám.

Upřesnění:

1. Uložená naměřená data musí být doplněna dalšími redundantními informacemi, které umožní softwaru, který data načítá, vyhodnocuje a indikuje nebo jinak zpracovává, ověřit, že uložená naměřená data nebyla změněna fyzikálními vlivy (elektromagnetickým rušením, teplotou, vibracemi atd.).
2. Musí být zavedeny prostředky k zabezpečení dat měření tak, aby nemohla být změněna a mohla být vymazána pouze za následujících podmínek:
   a. Data měření, která se skládají z mezihodnoty měřené veličiny, viz kapitola 14, nemohou být vymazána uživatelem, ale mohou být automaticky vymazána, pokud další modul nebo komponenta uvede správné dokončení očekávaných činností, které se provádějí.
   b. U měřicích přístrojů jiných než měřidel spotřeby lze výsledek měření vymazat po uplynutí doby, po kterou lze požadovat předložení trvalého dokladu. Předpisy týkající se minimální doby uchovávání výsledků měření jsou ponechány na národních předpisech, a proto jsou mimo rámec této příručky.
   c. U měřidel spotřeby nesmí být celkové naměřené množství nikdy vymazánotj. tyto registry musí být chráněny hardwarovou plombou proti vynulování. Dalšíinformace jsou uvedeny v příručkách WELMEC 11.1, 11.3 a 13.1.

Požadovaná dokumentace:

- Metoda, jakým způsobem je provedeno zabezpečení proti neúmyslným změnám a vymazání a jak může vyhledávací software ověřit integritu naměřených dat.// Praktické namátkové kontroly, které ukazují, že výsledky měření lze vymazat pouze po splnění podmínek a v případě ručního vymazání, zda bylo úspěšně aplikováno bezpečnostní opatření, např. zda bylo předloženo heslo.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda je implementována metoda na detekci náhodných změn dat.
- Ověřte, zda tato metoda pokrývá všechna data.
- Ověřte, zda nemůže dojít k přepsání nebo vymazání naměřených dat, pokud nejsou splněny všechny podmínky, a v případě ručního mazání pouze po úspěšném absolvování bezpečnostního opatření, např. po zadání hesla.

Ověření funkčnosti:

- Proveďte praktické namátkové testy, které prokáží, že výsledky měření lze vymazat pouze po splnění podmínek a v případě ručního vymazání, zda bylo úspěšně aplikováno bezpečnostní opatření, např. zda bylo zadáno heslo.

Příklad přijatelného řešení:

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

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

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">L3: Ochrana uložených dat měření
Uložená naměřená data musí být chráněna proti záměrným změnám.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Musí být aplikovány prostředky ochrany proti záměrným změnám, které lze provést snadno dostupnými ovládacími softwarovými nástroji.
2. Uložená data musí být doplněna dalšími kontrolními informacemi umožňujícími ověření jejich integrity, a to při jejich vyčtení, vyhodnocení, zobrazení či jiném zpracování.</td></tr>
<tr><td colspan="2"></td><td>3. Prostředky zabezpečení musí rovněž zabránit záměrným změnám, které lze provést speciálními sofistikovanými softwarovými nástroji.
4. Při výběru vhodného algoritmu a minimální délky klíče musí být vzaty v úvahu požadavky a doporučení národních a mezinárodních institutů zodpovědných za bezpečnost dat.
5. I když bude algoritmus a klíč splňovat vysokou úroveň ochrany, technické řešení standardního osobního počítače tento stupeň ochrany nebude naplňovat, pokud nebudou existovat dostatečné prostředky ochrany pro programy, které podepisují nebo verifikují přenášená data (viz základní požadavky U pro univerzální počítače – poznámka k požadavku U6 - třída rizika D).</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Metoda, jakým způsobem je realizována ochrana proti nepřípustným úmyslným změnám a jak může načítací software ověřit integritu naměřených dat.</td></tr>
<tr><td colspan="2">Postup validace:
Ověření na základě dokumentace:
• V případě použití kontrolního součtu nebo elektronického podpisu:
• Ověřte, zda je kontrolní součet nebo elektronický podpis generován z celého bloku dat.
• Ověřte, zda legálně relevantní software, který čte data a vypočítává kontrolní součet nebo dešifruje elektronický podpis, skutečně porovnává vypočtené hodnoty s nominálními.
• Ověřte, zda jsou neveřejné údaje (např. počáteční hodnota klíče, pokud je použita) zabezpečeny proti odhalení jednoduchými nástroji.</td><td>Postup validace (kromě postupu požadovaného pro třídy rizika B a C):
Ověření na základě dokumentace:
• Ověřte, zda přijatá opatření odpovídají nejnovějším požadavkům na vysoký stupeň ochrany.</td></tr>
</table>

Příklad přijatelného řešení: • Modul ukládacího zařízení vypočítá CRC-32 souboru dat a připojí jej k souboru dat. Pro tento výpočet používá tajnou počáteční hodnotu. Tato počáteční hodnota je použita jako klíč a uložena jako konstanta ve spustitelném kódu. Čtecí modul má tuto počáteční hodnotu rovněž uloženou ve svém spustitelném kódu. Před použitím datové sady vypočítá čtecí modul kontrolní součet a porovná jej s kontrolním součtem uloženým v datové sadě. Pokud se obě hodnoty shodují, datová sada není zfalšovaná. V opačném případě modul předpokládá falzifikaci a datovou sadu zahodí a označí, že naměřená data jsou poškozená.	**Příklad přijatelného řešení:** • Legálně relevantní ukládací modul vygeneruje elektronický podpis pro uložený soubor dat. Ten je připojen k uložené datové sadě. Soukromý a veřejný klíč použitý pro podepisování se generují v hardwarovém bezpečnostním modulu, který chrání soukromý klíč před manipulací nebo čtením a exportuje veřejný klíč. Čtecí modul ověří elektronický podpis pomocí veřejného klíče, aby zkontroloval pravost a integritu datové sady. K prokázání původu datové sady potřebuje čtecí modul vědět, zda veřejný klíč skutečně patří ukládajícímu modulu. Proto se veřejný klíč zobrazuje na displeji měřicího přístroje a může být jednorázově zaregistrován, např. spolu se sériovým číslem přístroje při jeho ověřování v terénu. V případě nesrovnalosti modul přepokládá falšování a sadu dat vyřadí a oznámí, že naměřená data jsou poškozená.
Dodatky pro třídu rizika E	
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D): Zdrojový kód legálně relevantního softwaru.	
Postup validace (kromě postupu požadovaného pro třídu rizika D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda jsou prostředky zajištění integrity dostatečné a zda jsou správně implementovány.	

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

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D): Zdrojový kód legálně relevantního softwaru.
Postup validace (kromě postupu požadovaného pro třídu rizika D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda jsou soubory naměřených dat správně sestaveny a spolehlivě vysledovány zpět k měřicímu přístroji a měření.

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">L5: Ochrana důvěrných informací
Důvěrné informace musí být chráněny před změnami, uchovávány v tajnosti a chráněny před zveřejněním.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Přístup ke čtení důvěrných informací má pouze legálně relevantní software.
2. Prostředky ochrany musí zajistit, aby nebylo možné provádět žádné změny snadno dostupnými a zvládnutelnými softwarovými nástroji.
3. V závislosti na způsobu ochrany se důvěrné informace mohou skládat z klíčů, generátorových polynomů, počátečních vektorů / počátečních hodnot atd.</td></tr>
<tr><td colspan="2"></td><td>4. Prostředky zabezpečení musí rovněž zabránit záměrným změnám, které lze provést speciálními sofistikovanými softwarovými nástroji
5. Technické řešení na bázi standardního osobního počítače není pro zajištění vysokého stupně ochrany dostatečné bez odpovídajících hardwarových prostředků ochrany klíče a dalších tajných údajů (viz základní požadavky pro univerzální počítače, U6).</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Popis správy tajných informací a prostředků pro utajení klíčů a dalších informací.</td></tr>
<tr><td colspan="2">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda nelze tajné informace odhalit.</td><td>Postup validace (kromě postupu požadovaného pro třídy rizika B a C):
Ověření na základě dokumentace:
• Ověřte, zda přijatá opatření odpovídají nejnovějším požadavkům na vysoký stupeň ochrany.</td></tr>
<tr><td colspan="2">Příklad přijatelného řešení:
Tajný klíč a související informace jsou uloženy v binárním a zašifrovaném formátu ve spustitelném kódu legálně relevantního softwaru. Software nenabízí žádné funkce pro prohlížení nebo úpravu těchto dat a volatilní paměť je chráněna konfigurací operačního systému, aby se zabránilo načtení citlivého kryptografického materiálu, viz O1.</td><td>Příklad přijatelného řešení:
Tajný klíč je uložen v části hardwaru, kterou lze fyzicky zaplombovat. Software nemá žádné nástroje umožňující zobrazení či editaci těchto údajů.</td></tr>
</table>

<table>
<tr><th>Dodatky pro třídu rizika E</th></tr>
<tr><td>Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D):
Zdrojový kód legálně relevantního softwaru.</td></tr>
<tr><td>Postup validace (kromě postupu požadovaného pro třídu rizika D):
Ověření na základě zdrojového kódu:
• Ověřte, zda jsou správně implementována opatření přijatá pro správu tajných informací.</td></tr>
</table>

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">L6: Načtení, ověření a zobrazení uložených dat
V případě, že se údaje z měření používají pro legálně relevantní účely, musí existovat legálně relevantní komponenta nebo modul pro načítání, ověřování, manipulaci a zobrazení uložených naměřených dat.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Legálně relevantní software musí být schopen načítat, ověřovat, zpracovávat a zobrazovat uložené údaje o měření. Požadavky týkající se prezentace dat měření viz P8/U8.
2. Načtená naměřená data musejí být ověřena.
3. V případě nesrovnalosti nesmí být naměřená data použita pro další legálně relevantní účely. Zaregistrují se jako neplatné. Tento registr se považuje za relevantní údaje o výsledku měření.
4. Na zobrazených nebo vytištěných naměřených údajích musí být uvedena případná nesrovnalost naměřených údajů.</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
• Popis funkcí softwaru načítajícího data.
• Popis způsobu ověřování naměřených dat.
• Popis, jak jsou poškozená data označena a zobrazena.</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda je software načítající data schopen data správně zobrazit.
Ověření funkčnosti:
• Proveďte praktické namátkové testy k ověření, zda jsou při načtení zobrazeny všechny potřebné informace.</td></tr>
<tr><td colspan="2">Příklad přijatelného řešení:
Legálně relevantní modul ukládacího zařízení vypočítá CRC32 datové sady a připojí ji k datové sadě, viz L3. Pro tento výpočet používá tajnou počáteční hodnotu. Tato počáteční hodnota je použita jako klíč a uložena jako konstanta ve spustitelném kódu. Čtecí modul má tuto počáteční hodnotu rovněž uloženou ve svém spustitelném kódu. Před použitím datové sady čtecí modul vypočítá kontrolní součet a porovná jej s kontrolním součtem uloženým v datové sadě. Pokud se obě hodnoty shodují, datová sada není falšována. V opačném případě modul předpokládá falšování a sadu dat vyřadí, označí sadu dat jako poškozenou a uvede, že data měření jsou poškozená.</td><td>Příklad přijatelného řešení:
• Legálně relevantní ukládací modul vygeneruje elektronický podpis pro uložený soubor dat. Ten je připojen k uložené datové sadě. Soukromý a veřejný klíč používaný pro podepisování se generují v hardwarovém bezpečnostním modulu, který chrání soukromý klíč před manipulací nebo čtením a exportuje veřejný klíč. Čtecí modul ověřuje elektronický podpis pomocí veřejného klíče, aby zkontroloval pravost a integritu datové sady. K prokázání původu datové sady potřebuje čtecí modul vědět, zda veřejný klíč skutečně patří ukládajícímu modulu. Proto je veřejný klíč zobrazen na displeji měřicího přístroje a může být jednorázově zaregistrován, např. spolu se sériovým číslem přístroje při jeho ověřování v terénu.
• V případě nesrovnalosti modul předpokládá falšování a sadu dat vyřadí a označí sadu dat jako poškozenou a uvede, že data měření jsou poškozená.</td></tr>
</table>

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

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

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

Třída rizika B	Třída rizika C	Třída rizika D
L8: Kapacita paměti a kontinuita *Kapacita paměti pro dlouhodobé uložení dat musí být pro zamýšlené účely dostatečná.*		
Upřesnění: 1. Pokud je paměť plná nebo je-li paměť z přístroje vyjmuta či odpojena, operátor je o tom informován prostřednictvím výstrahy. 2. Musí být zajištěno, že lze přepsat pouze zastaralá data. 3. Minimální doba uložení naměřených dat a požadovaných informací se řídí národní legislativou, a proto se jimi tato příručka nezabývá. 4. Musí být zpřístupněny informace o kapacitě paměti.		
Požadovaná dokumentace: • Kapacita paměti, popis správy uložených naměřených dat. • Popis chování zařízení, pokud je úložiště plné nebo odstraněné.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda dokumentace obsahuje údaje o kapacitě paměti nebo formulaci jejího výpočtu. • Ověřte, zda před koncem doby uložení dat stanovené a zdokumentované výrobcem nemůže dojít k přepsání dat. *Ověření funkčnosti:* • Ověřte, zda se zobrazí varování, že je paměť plná nebo že byla odejmuta, pokud je to relevantní.		
Příklad přijatelného řešení: • Měření, která lze snadno a rychle přerušit: Když je paměť nedostupná před dokončením měření: Měřicí přístroj disponuje dostatečně velkou dočasnou pamětí pro uložení aktuální operace. Nelze následně zahájit další měření a hodnoty uložené v dočasné paměti jsou uchovány do chvíle, než mohou být přeneseny do archivní paměti. • Měření, která nelze přerušit: Kumulativní údaje jsou vyčteny a přeneseny do paměti později, když je tato paměť opět k dispozici. • Naměřená data jsou po prověření jejich stáří (příslušná doba uložení se řídí národní legislativou) automaticky přepsána. Před přepsáním dat je uživatel vyzván o povolení data vymazat a data jsou mazána počínaje nejstaršími.		

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

8 Rozšíření T: Přenos naměřených dat komunikačními sítěmi

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

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

8.1Technický popis

V následující tabulce jsou popsány dvě síťové konfigurace.

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

Tabulka 8-1: Technický popis komunikačních sítí.

8.2 Specifické požadavky na software pro přenos naměřených dat

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

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

Třída rizika B	Třída rizika C	Třída rizika D

T2: Zabezpečení a ochrana přenášených dat měření

Přenášená data měření musí být zabezpečena proti neúmyslným a náhodným změnám.

Upřesnění:

1. Musí být zavedeny prostředky pro zabezpečení přenášených naměřených dat proti neúmyslným změnám a pro zjištění změny nebo ztráty přenášených naměřených dat.

Požadovaná dokumentace:

Popis metod používaných k zabezpečení přenášených naměřených dat a k detekci chyb přenosu nebo ztráty přenášených naměřených dat.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda je zavedena metoda zabezpečení přenášených naměřených dat a detekce chyb přenosu nebo ztráty přenášených naměřených dat..

Příklad přijatelného řešení:

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

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

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

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">T3: Ochrana přenášených naměřených dat
Přenášená naměřená data musí být chráněna proti záměrným změnám.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Tento požadavek se vztahuje pouze na otevřené sítě, nikoliv na sítě uzavřené.
2. Musí být aplikovány prostředky ochrany proti záměrným změnám, které lze provést snadno dostupnými ovládacími softwarovými nástroji.</td></tr>
<tr><td colspan="2"></td><td>3. Prostředky zabezpečení musí rovněž zabránit záměrným změnám, které lze provést speciálními sofistikovanými softwarovými nástroji.
4. Při výběru vhodného algoritmu a minimální délky klíče musí být vzaty v úvahu požadavky a doporučení národních a mezinárodních institutů zodpovědných za bezpečnost dat.
5. Aby byla zajištěna vysoká úroveň zabezpečení, je nutné aplikovat odpovídající prostředky ochrany softwaru, který podepisuje či verifikuje přenášená data (např. prostředky hardwarové) (viz také kapitola 5 pro software univerzálních počítačů, požadavek U6, upřesňující poznámka 6 pro třídu rizika D).</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Popis metody zabezpečení.</td></tr>
<tr><td colspan="3">Postup validace:
Ověření na základě dokumentace:
Zkontrolujte, zda byla zvolena vhodná metoda.</td></tr>
<tr><td colspan="2">Příklad přijatelného řešení:
• Modul vysílajícího zařízení vypočítá CRC-32 souboru dat a připojí jej k souboru dat. Pro tento výpočet používá tajnou počáteční hodnotu. Tato počáteční hodnota je použita jako klíč a uložena jako konstanta ve spustitelném kódu. Přijímací modul má tuto počáteční hodnotu rovněž uloženou ve svém spustitelném kódu. Před použitím datové sady přijímací modul vypočítá kontrolní součet a porovná jej s kontrolním součtem uloženým v datové sadě. Pokud se obě hodnoty shodují, datová sada není zfalšovaná. V opačném případě modul předpokládá falšování a datovou sadu vyřadí a požádá o opětovné zaslání dat.</td><td>Příklad přijatelného řešení:
• Legálně relevantní vysílací modul vygeneruje elektronický podpis pro přenášený soubor dat. Ten je připojen k přenášenému souboru dat. Soukromý a veřejný klíč použitý pro podepisování se generují v hardwarovém bezpečnostním modulu, který chrání soukromý klíč před manipulací nebo čtením a exportuje veřejný klíč. Přijímací modul ověří elektronický podpis pomocí veřejného klíče, aby zkontroloval pravost a integritu datové sady. K prokázání integrity a autenticity datové sady musí přijímací modul vědět, zda veřejný klíč skutečně patří vysílajícímu modulu. Proto je veřejný klíč zobrazen na displeji měřicího přístroje a může být jednorázově zaregistrován, např. spolu se sériovým číslem přístroje při jeho ověřování v terénu. V případě nesrovnalosti přijímací modul datovou sadu vyřadí a znovu požádá o opětovné zaslání dat.</td></tr>
<tr><th colspan="3">Dodatky pro třídu rizika E</th></tr>
<tr><td colspan="3">Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D):
Zdrojový kód legálně relevantního softwaru.</td></tr>
<tr><td colspan="3">Postup validace (kromě postupu požadovaného pro třídy rizika B až D):
Ověření na základě zdrojového kódu:
• Ověřte, zda jsou správně provedena opatření pro zajištění integrity přenášených dat měření.</td></tr>
</table>

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

<table>
<tr><th>Dodatky pro třídu rizika E</th></tr>
<tr><td>Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D):
Zdrojový kód legálně relevantního softwaru.</td></tr>
<tr><td>Postup validace (kromě postupu požadovaného pro třídy rizika B až D):
Ověření na základě zdrojového kódu:
• Ověřte, zda jsou správně provedena opatření přijatá k zajištění dohledatelnosti přenášených naměřených dat.</td></tr>
</table>

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">T5: Ochrana důvěrných informací
Důvěrné informace musí být chráněny před změnami, uchovávány v tajnosti a chráněny před zveřejněním.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Přístup ke čtení důvěrných informací má pouze legálně relevantní software.
2. Prostředky ochrany musí zajistit, aby nebylo možné provádět žádné změny snadno dostupnými a zvládnutelnými softwarovými nástroji.
3. V závislosti na způsobu ochrany se důvěrné informace mohou skládat z klíčů, generátorových polynomů, počátečních vektorů / počátečních hodnot, atd.</td></tr>
<tr><td colspan="2"></td><td>4. Prostředky zabezpečení musí rovněž zabránit záměrným změnám, které lze provést speciálními sofistikovanými softwarovými nástroji
5. Technické řešení na bázi standardního osobního počítače není pro zajištění vysokého stupně ochrany dostatečné bez odpovídajících hardwarových prostředků ochrany klíče a dalších tajných údajů (viz základní požadavky pro univerzální počítače, U6).</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Popis správy tajných informací a prostředků pro utajení klíčů a dalších informací.</td></tr>
<tr><td colspan="2">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda nelze tajné informace odhalit.</td><td>Postup validace (kromě postupu požadovaného pro třídy rizika B a C):
Ověření na základě dokumentace:
• Ověřte, zda přijatá opatření odpovídají nejnovějším požadavkům na vysoký stupeň ochrany.</td></tr>
<tr><td colspan="2">Příklad přijatelného řešení:
Tajný klíč a související informace jsou uloženy v binárním a zašifrovaném formátu ve spustitelném kódu legálně relevantního softwaru. Software nenabízí žádné funkce pro prohlížení nebo úpravu těchto dat a volatilní paměť je chráněna konfigurací operačního systému, aby se zabránilo načtení citlivého kryptografického materiálu, viz O1.</td><td>Příklad přijatelného řešení:
Tajný klíč je uložen v části hardwaru, kterou lze fyzicky zaplombovat. Software nemá žádné nástroje umožňující zobrazení či editaci těchto údajů.</td></tr>
</table>

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

Třída rizika B	Třída rizika C	Třída rizika D

T6: Příjem, ověřování a zpracování přenesených naměřených dat

V případě, že se údaje z měření používají pro legálně relevantní účely, musí existovat legálně relevantní komponenta nebo modul pro načítání, ověřování, manipulaci a zobrazení uložených naměřených dat.

Upřesnění:

1. Legálně relevantní software musí být schopen načítat, ověřovat, zpracovávat a zobrazovat uložené údaje o měření. Požadavky týkající se prezentace dat měření viz P8/U8.
2. Načtená naměřená data musejí být ověřeny.
3. V případě nesrovnalosti nesmí být naměřená data použita pro další legálně relevantní účely. Zaregistrují se jako neplatné. Tento registr se považuje za relevantní údaje o výsledku měření.
4. Na zobrazených nebo vytištěných naměřených údajích musí být uvedena případná nesrovnalost naměřených údajů.

Požadovaná dokumentace:

- Popis funkcí softwaru načítajícího data.
- Popis způsobu ověřování naměřených dat.
- Popis jak jsou označena poškozená data.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda jsou detekována poškozená naměřená data a že nejsou akceptována a jsou podle toho nahrazena správnými nebo registrovanými daty

Ověření funkčnosti:

- Ověřte, zda jsou detekována poškozená naměřená data a že nejsou akceptována a jsou podle toho nahrazena správnými nebo registrovanými daty

Příklad přijatelného řešení:

Legálně relevantní modul vysílajícího zařízení vypočítá CRC32 datové sady a připojí ji k datové sadě, viz T2 a T3. Pro tento výpočet používá tajnou počáteční hodnotu. Tato počáteční hodnota je použita jako klíč a uložena jako konstanta ve spustitelném kódu. Přijímací modul má tuto počáteční hodnotu rovněž uloženou ve svém spustitelném kódu. Před použitím datové sady přijímací modul vypočítá kontrolní součet a porovná jej s kontrolním součtem uloženým v datové sadě. Pokud se obě hodnoty shodují, datová sada není zfalšovaná. V opačném případě modul předpokládá falšování a datovou sadu vyřadí a požádá o opětovné zaslání dat.

Příklad přijatelného řešení:

- Legálně relevantní odesílající software vytvoří elektronický podpis pro přenášený soubor dat. Ten je připojen k přenášenému souboru údajů, viz T2 a T3. Přijímací modul ověří elektronický podpis pomocí veřejného klíče, aby zkontroloval pravost a integritu datové sady. K prokázání původu datové sady potřebuje přijímací modul vědět, zda veřejný klíč skutečně patří odesílajícímu modulu. Veřejný klíč je proto předem umístěn na displeji měřicího přístroje a může být jednorázově zaregistrován, např. spolu se sériovým číslem přístroje při jeho ověřování v terénu. V případě nesrovnalosti přijímací modul datovou sadu vyřadí a požádá o opětovné zaslání dat.

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

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

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

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

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

9 Rozšíření S: Oddělení softwaru

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

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

9.1 Technický popis

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

9.2 Specifické požadavky na software v případě oddělení softwaru

Třída rizika B	Třída rizika C	Třída rizika D
S1: Realizace oddělení softwaru *Část softwaru obsahující legálně relevantní software a parametry musí být jednoznačně oddělená od ostatních částí softwaru.*		
Upřesnění: 1. Samotné ochranné rozhraní (viz S3) je legálně relevantní. 2. Pokud jde o určení, zda je či není legálně relevantní software, parametry nebo údaje, viz kapitola 15.		
Požadovaná dokumentace: Pojmenování všech modulů, které tvoří legálně relevantní software.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda je pojmenování správné a seznam modulů kompletní.		
Příklad přijatelného řešení:		

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D): Zdrojový kód legálně relevantního softwaru.
Postup validace (kromě postupu požadovaného pro třídy rizika B až D)**:** *Ověření na základě zdrojového kódu:* • Ověřte (např. analýzou toku dat pomocí nástrojů nebo ručně), zda jsou všechny moduly, které se podílejí na zpracování naměřených dat, registrovány jako legálně relevantní software.

Třída rizika B	Třída rizika C	Třída rizika D

S2: Smíšená indikace

Legálně relevantní údaj musí být generován legálně relevantním softwarem a musí být jasně odlišitelný od legálně nerelevantního údaje.

Upřesnění: ---

1. Legálně relevantní zobrazení musí být chráněno proti vlivu legálně nerelevantního softwaru, viz S1.
2. Legálně relevantní software musí generovat legálně relevantní indikaci a nesmí umožnit legálně nerelevantnímu softwaru přístup k naměřeným datům až po zobrazení výsledku měření.
3. Legálně relevantní údaj se uvede tak, aby bylo zřejmé, že se jedná o legálně relevantní údaj.
4. Legálně relevantní zobrazení musí být viditelné ihned po zahájení měření a až do zobrazení výsledku měření. Uživatel tak může zkontrolovat, zda údaj obsahuje potřebné údaje o měření, např. jednotkovou cenu. Další pokyny v případě provozního systému viz O8.

Požadovaná dokumentace:

- Pojmenování modulů, které umožňují prezentaci legálně relevantních údajů z měření.
- Popis způsobu, jak je zabráněno tomu, aby k naměřeným datům před zobrazením výsledku měření měl přístup software, který není legálně relevantní.
- Popis způsobu, jakým lze rozlišit legálně relevantní zobrazení od zobrazení, které není legálně relevantní.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, zda software, který není legálně relevantní, nemá přístup k naměřeným datům před jejich zobrazením.

Ověření funkčnosti:

- Prostřednictvím vizuální kontroly posuďte, zda jsou legálně relevantní údaje jasně odlišitelné od údajů, které nejsou legálně relevantní.

Příklad přijatelného řešení:

- Legálně relevantní údaj je zobrazen ve vyhrazené části displeje, která je pod kontrolou legálně relevantního softwaru. Technická opatření vyžadovaná od aplikace jsou:

a. Do doby, než jsou údaje o měření zobrazeny, nemají moduly, které nejsou legálně relevantní, žádný přístup k naměřeným datům.

b. Aplikace se pravidelně aktualizuje. Související modul kontroluje, zda je aplikace viditelná, dokud není měření ukončeno. Zpracování dat měření se zastaví vždy, když je tato aplikace zavřená nebo není zcela viditelná.

- Legálně relevantní údaj se zobrazuje v okně, které je pod kontrolou legálně relevantního softwaru. Toto okno je vždy nahoře. Viz rozšíření O4.

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

Třída rizika B	Třída rizika C	Třída rizika D

S3: Ochranné rozhraní

Interakce a výměna dat mezi legálně relevantním a legálně nerelevantním softwarem se provádí výhradně prostřednictvím ochranného rozhraní, které je plně pod kontrolou legálně relevantního softwaru.

Upřesnění:

1. Tento požadavek se vztahuje na všechny typy interakcí a výměn dat mezi legálně relevantním a legálně nerelevantním softwarem.
2. Veškerá komunikace musí být výhradně realizována přes definované ochranné rozhraní.
3. Přípustné jsou pouze takové interakce a toky dat, které nemají nepřípustný vliv na proces měření, zejména na legálně relevantní software, specifické parametry přístroje a naměřená data.
4. Plánování a průběh procesu měření nesmí být ovlivněny softwarem, který není legálně relevantní.
5. V případě separace softwaru v legálně relevantním operačním systému viz O4.
6. Ochranné rozhraní mezi legálně relevantním a legálně nerelevantním softwarem musí být co nejmenší a nesmí obsahovat žádné zbytečné funkce. Musí být plně pod kontrolou legálně relevantního softwaru.

Požadovaná dokumentace: Popis softwarového rozhraní

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

Postup validace:

Ověření na základě dokumentace:

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

Příklad přijatelného řešení:

- Legálně nerelevantní software je uzavřen v knihovně pro výpočet legálně nerelevantních údajů. Legálně relevantní software tak má plnou kontrolu nad všemi interakcemi s legálně nerelevantním softwarem. Každé volání legálně relevantního softwaru do knihovny včetně přenášených dat je zdokumentováno. Žádný přenos dat nemá nepřípustný vliv na legálně relevantní software.

Dodatky pro třídu rizika E

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

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

Ověření na základě zdrojového kódu:

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

10 Rozšíření D: Stahování legálně relevantního softwaru

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

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

10.1 Technický popis

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

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

Tabulka 10-1: Technický popis konfigurací pro automatické stahování softwaru.

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

10.2 Specifické požadavky na software

Třída rizika B	Třída rizika C	Třída rizika D

D1: Mechanismus stahování

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

Upřesnění:

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

Požadovaná dokumentace:

Dokumentace musí popisovat způsob implementace podmínek uvedených v části Upřesnění.

Postup validace:

Ověření na základě dokumentace:

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

Ověření funkčnosti:

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

Příklad přijatelného řešení:

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

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

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

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

Dodatky pro třídu rizika E

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

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

Ověření na základě zdrojového kódu:

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

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

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

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

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

<table>
<tr><th>Třída rizika B</th><th>Třída rizika C</th><th>Třída rizika D</th></tr>
<tr><td colspan="3">D4: Návaznost stahovaného legálně relevantního softwaru
Za účelem následných kontrol musí být v přístroji zajištěna odpovídajícími technickými prostředky zpětná návaznost a dohledatelnost stahovaných legálně relevantních softwarů.</td></tr>
<tr><td colspan="3">Upřesnění:
1. Musí být zaznamenána a zabezpečena všechna relevantní data umožňující dohledat stahování nebo pokus o stahování softwaru. Patří k nim např. datum a čas stahování, označení softwaru, původ přenosu, oznámení o úspěšnosti přenosu.
2. Zaznamenaná data musejí být dostupná po adekvátní dobu (délka této doby je určena nařízeními mimo rámec MID).
3. Zaznamenaná data musí být na vyžádání zobrazena.
4. Prostředky a záznamy sloužící k dohledatelnosti jsou součástí legálně relevantního softwaru, a jako takové musejí být náležitým způsobem chráněny.</td></tr>
<tr><td colspan="3">Požadovaná dokumentace:
Dokumentace musí popisovat:
• způsob implementace a zabezpečení prostředků návaznosti a dohledatelnosti,
• strukturu záznamů,
• způsob, jak lze zaznamenané informace zobrazit</td></tr>
<tr><td colspan="2">Postup validace:
Ověření na základě dokumentace:
• Ověřte, zda implementované prostředky dohledatelnosti splňují podmínky uvedené v části Upřesnění.
Ověření funkčnosti:
• Ověřte funkčnosti prostředků při stahování softwaru.</td><td>Postup validace (kromě postupu požadovaného pro třídy rizika B a C):
Ověření na základě dokumentace:
• Ověřte, zda přijatá opatření odpovídají nejnovějším požadavkům na vysoký stupeň ochrany.</td></tr>
<tr><td colspan="3">Příklad přijatelného řešení:
• Auditní stopa: Měřicí přístroj je vybaven záznamníkem událostí, který automaticky zaznamenává minimálně datum a čas stahování, označení stahovaného legálně relevantního softwaru, označení vysílací strany a záznam o úspěšnosti procesu. Záznam o úspěšnosti stahování se vytvoří při každém pokusu o stažení softwaru bez ohledu na jeho výsledek.
• Po dosažení limitu kapacity záznamníku auditní stopy musí technologické prostředky zabránit dalšímu stahování softwaru. Auditní stopu lze vymazat pouze po porušení plomby. Umístit novou plombu je oprávněn pouze kontrolní úřad.</td></tr>
<tr><td colspan="2"></td><td></td></tr>
</table>

Dodatky pro třídu rizika E
Požadovaná dokumentace (kromě dokumentace pro třídy rizika B až D): Zdrojový kód legálně relevantního softwaru
Postup validace (kromě postupu požadovaného pro třídu rizika D)**:** *Ověření na základě zdrojového kódu:* • Ověřte, zda jsou prostředky sledování procesů stahování dostatečné. • Ověřte, zda jsou prostředky zabezpečení uložených dat dostatečné.

11 Rozšíření I: Požadavky na software přístrojů konkrétního typu

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

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

Rozšíření I by v tuto chvíli mělo představovat první návrh, jenž bude příslušnými odbornými pracovními skupinami WELMEC v budoucnu dále doplňován. Má proto otevřenou strukturu - vytváří jakousi kostru, která je s výjimkou přiřazení tříd rizika vyplněna pouze částečně (např. u měřičů spotřeby a automatických vážicích přístrojů). Na základě zkušeností a rozhodnutí příslušných pracovních skupin WELMEC může být toto rozšíření použito i pro jiné přístroje MID (a také pro přístroje, které v této směrnici nejsou zahrnuté) podle získaných zkušeností a rozhodnutí přijatých příslušnými pracovními skupinami WELMEC.

11.1 Struktura

Existují různé aspekty softwaru specifické pro daný typ měřicího přístroje, které může být třeba zvážit. Tyto aspekty by měly být systematicky řešeny následujícím způsobem: Každá podkapitola týkající se konkrétního přístroje by měla být rozdělena do následujících kategorií.

11.1.1 Specifické předpisy, normy a další normativní dokumenty

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

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

11.1.2 Technický popis

V tomto oddílu mohou být uvedeny následující informace:

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

Popis by měl zahrnovat:

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

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

11.1.3 Specifické požadavky na software

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

11.1.4 Příklady legálně relevantních parametrů, funkcí a dat

V tomto oddílu mohou být uvedeny příklady

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

11.1.5 Další vlastnosti

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

11.1.6 Přiřazení třídy rizika

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

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

11.2 Vodoměry

11.2.1 Zvláštní předpisy, normy a jiné normativní dokumenty

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

Doporučení a normy organizace OIML nebyly zohledněny.

11.2.2 Technický popis

11.2.2.1 Konfigurace hardwaru

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

11.2.2.2 Konfigurace softwaru

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

11.2.2.3 Princip měření

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

Měření objemu nelze opakovat.

11.2.2.4 Detekce a řešení chyb

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

11.2.3 Specifické požadavky na software (vodoměry)

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

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

Třída rizika B	Třída rizika C	Třída rizika D
I1-3: Doplňkové funkce[3] *Doplňkové funkce, např. předplatné nebo intervalové měření[4], by neměly ovlivnit legálně relevantní měřicí funkce specifikované v MID, Příloha III Vodoměry (MI-001).*		
Upřesnění: • Doplňkové funkce jsou povoleny za předpokladu, že neovlivňují legálně relevantní měřicí funkce specifikované v MID, Příloha III Vodoměry (MI-001).		
Požadovaná dokumentace: Viz S1 až S3.		
Postup validace: Viz S1 až S3.		
Příklad přijatelného řešení: Viz S1 až S3.		

Třída rizika B	Třída rizika C	Třída rizika D
I1-4: Prostředky zálohování *Musí existovat prostředky zajišťující pravidelnou zálohu naměřených dat, jako jsou naměřené hodnoty a současný stav procesu. Tato data musejí být uložena v energeticky nezávislé paměti.*		
Upřesnění: Pokud jsou pro zajištění obnovy po chybě použity prostředky zálohování, musí být vypočten takový minimální interval ukládání dat, který zajistí, že nebude překročena kritická hodnota.		
Požadovaná dokumentace: • Stručný popis toho, jaká data jsou zálohována a kdy se zálohování provádí. • Výpočet takového minimálního intervalu pro ukládání dat, že není překročena kritická hodnota změny.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda jsou naměřená data uložena v energeticky nezávislé paměti a zda je lze obnovit. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Naměřená data jsou zálohována dle potřeby.		

[3] Vždy by měl vzít výrobce v úvahu národní požadavky týkající se doplňkových funkcí.
[4] Další doporučení k intervalovému měření poskytuje WELMEC Guide 13.3.

Třída rizika B	Třída rizika C	Třída rizika D
I1-5: Stahování softwaru *Během instalace softwaru nesmí být měřicí proces pozastaven celkově déle než 1 minutu. V případě, že proces instalace zabírá více než 1 minutu, musí být přijata další opatření (např. instalace probíhá v režimu nízké spotřeby energie).*		
Upřesnění: • Pokud je realizováno stahování softwaru kromě požadavků D1, D2, D3 a D4 aplikujte i tento požadavek. • Tento dodatečný požadavek přináší ujištění, že aplikace běžící v reálném čase nejsou přerušeny moc dlouho.		
Požadovaná dokumentace: Viz D1, D2, D3 a D4..		
Postup validace: *Viz D1, D2, D3 a D4..*		
Příklad přijatelného řešení: Viz D1, D2, D3 a D4.		

Třída rizika B	Třída rizika C	Třída rizika D
I1-6: MID Příloha I, 8.5 (zamezení vynulování naměřených kumulativních dat) *Údaje o celkovém spotřebovaném objemu nebo údaje, z nichž lze celkový spotřebovaný objem odvodit, které se částečně či plně využívají k výpočtu ceny k zaplacení, musí být u přístrojů na měření spotřeby chráněny proti vynulování během provozu.*		
Upřesnění: • Kumulativní registry měřicího přístroje lze vynulovat před provedením procedury posouzení shody. Během procesu schvalování typu dle příloh D, F či H1 musí být vodoměry zabezpečeny všemi prostředky, jak je specifikováno v TEC. Tato zajištění jsou takového rázu, že není možno vynulovat naměřené kumulativní hodnoty bez evidence tohoto zásahu. • Totalizéry kumulativních registrů měřidla mohou být vynulovány před dokončením příslušné procedury posouzení shody. Během procesu schvalování typu dle příloh D, F či H1 musí být vodoměry zabezpečeny všemi ochrannými prostředky specifikovanými v TEC, které postkytují záznam o intervenci do registrů měřidla po provedení vynulování kumulativních naměřených dat. Není dovoleno vynulovat kumulativní registry v době používání v distribuční síti. NB: viz ISO 4064 bod 6.8.2. – Zařízení s elektronickou plombou		
Požadovaná dokumentace: Dokumentace prostředků zabezpečení proti vynulování ukazatelů objemu.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda je operace vynulování kumulativních legálně relevantních naměřených hodnot zajištěna a že očekávaná zabezpečení poskytují záznam o intervenci. *Ověření funkčnosti:* • Ověřte správnou funkci aplikovaných zabezpečení, viz také P3/U3 a P4/U4.		
Příklad přijatelného řešení: Registr pro celkové naměřené množství musí být chráněn hardwarovou plombou. Ostatní registry, např. pro denní či noční tarif, mohou být chráněny stejnými prostředky jako parametry (viz P7/U7), přičemž musí být dostupný celkový (úhrnný kumulativní) registr chráněný hardwarovou plombou. Pro další informace viz WELMEC Guide 11.1/13 and ISO 4064 článek 6.8.2. – elektronická plomba.		

Třída rizika B	Třída rizika C	Třída rizika D
I1-7: MID-Příloha I, článek 10.5 (Čtení naměřených dat) *Naměřené výsledky, které slouží jako základ pro stanovení ceny, mohou pocházet z různých registrů a jsou aktivovány na dálku, dle času či jinými způsoby. Každý registr reprezentuje celkové množství odpovídající jedné fakturovací sazbě. Musí být možné zobrazit hodnoty na displeji periodicky či na požádání přes uživatelské rozhraní.*		
Upřesnění: • Kumulativní registry či celkové registry měřidla mohou být vynulovány před provedením posouzení shody. Během procesu posouzení shody dle příloh D, F či H1 musí být měřidla spotřeby vybavena všemi zajištěními, jak je specifikováno výrobcem a je specifikováno v TEC. Tato zajištění musí být takového rázu, že není možno vynulovat naměřená kumulativní data bez důkazu tohoto zásahu.. • Pokud je dosaženo maximálního indikovatelného množství, měření bude pokračovat a indikace bude běžet od nuly, viz I1-9.		
Požadovaná dokumentace: Dokumentace, popisující jak je možno získat naměřená data, které slouží jako základ pro stanovení ceny.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte správné zacházení s naměřenými daty. *Ověření funkčnosti:* • Potvrďte správnou funkci zacházení s naměřenými daty.		
Příklad přijatelného řešení: Pokud je měřidlo navrženo tak, že načítá množství definovaná v MID (MI-001) v různých registrech, musí být možné zobrazit celkové množství každého registru na displeji pomocí uživatelského rozhraní měřidla (viz P3/U3, např. tlačítek měřidla) a stejně tak i zobrazit právě aktuální registr. Je též možné zobrazit výsledky na několika displejích, periodicky či na požádání přes uživatelské rozhraní. Avšak při zobrazení těchto hodnot musí být jasné, jak se který registr zobrazuje (na kterém displeji), v tomto ohledu nesmí dojít k nejednoznačnosti. Pokud je potřeba může být na vodoměru umístěn doplňující popis vysvětlující rozdílné registry či indikaci v testovacím režimu (viz I1-9)		

Třída rizika B	Třída rizika C	Třída rizika D
I1-8: Ochrana proti záměrným změnám u vodoměrů typu P (s mechanickým čítačem) *Vypočítané výsledky kontrolního součtu či alternativní indikace sloužící k detekci modifikace softwaru musí být možné pro kontrolní účely na příkaz zobrazit, viz P6. Jako výjimka pro vodoměry typu P s mechanickým čítačem je akceptovatelné, aby hodnota kontrolního součtu či alternativní indikace byla uvedena na štítku měřidla, a to pokud jsou splněny následující podmínky A, B a C:* *A. Uživatelské rozhraní nenabízí prostředek k aktivaci zobrazení hodnoty kontrolního součtu či alternativní indikace modifikace softwaru na displeji nebo displej přístroje technicky neumožňuje tyto hodnoty zobrazit (mechanický čítač).* *B. Přístroj nemá žádné rozhraní, kterým by identifikaci softwaru mohl sdělit.* *C. Na vyrobeném přístroji již není možné software měnit nebo je změna softwaru možná pouze v kombinaci s výměnou hardwaru nebo jeho části.*		
Upřesnění: • Výrobce hardwaru nebo příslušné hardwarové části zodpovídá za to, že je označení softwaru správně uvedeno na příslušném hardwaru. • Dále platí všechna další upřesnění požadavků P6.		
Požadovaná dokumentace: • Viz P6.		
Postup validace: *Ověření na základě dokumentace:* • Viz P6. *Ověření funkčnosti:* • Viz P6		
Příklad přijatelného řešení: Hodnota kontrolního součtu či alternativní indikace sloužící k detekci modifikace softwaru vytištěná na štítku přístroje.		

Třída rizika B	Třída rizika C	Třída rizika D

I1-9: Počet míst

Displej pro zobrazení celkového množství musí mít dostatečný počet míst. Dle ISO 4064, část 1 počet míst indikace závisí na trvalém průtoku Q3:

Trvalý průtok Q3 [m3/h]	*Minimální rozsah indikace [m3]*
Q3 ≤ 6,3	*9 999*
6,3 < Q3 ≤ 63	*99 999*
63 < Q3 ≤ 630	*999 999*
630 < Q3 ≤ 6300	*9 999 999*

Také, dle ISO 4064 část 1 rozsah indikace má splňovat následující požadavky:

- *Dělení ověřovací stupnice musí být dostatečně malé, aby bylo zajištěno, že chyba rozlišení indikačního zařízení nepřekročí 0,25 % pro třídu přesnosti 1 a 0,5 % pro třídu přesnosti 2 při ob-jemu proteklého během 90 min při minimálním průtoku Q1.*
- *Lze použít další ověřovací prvky za předpokladu, že nejistota odečtu není větší než 0,25 % testovaného objemu pro měřidla třídy přesnosti 1 a 0,5 % testovaného objemu pro měřidla třídy přesnosti 2 a že je kontrolováno správné fungování registru.*

Vyhovění článku 7.6 a 10.5 přílohy I směrnice 2014/32/EU (MID):

Měřidlo musí být navrženo tak, aby po uvedení na trh a do provozu umožňovalo kontrolu měření. Pokud je třeba, musí být součástí měřidla i zvláštní zařízení nebo programové vybavení pro tuto kontrolu. Také měřidlo, které lze odečítat na dálku, musí být v každém případě vybaveno metrologicky kontrolovanou indikační jednotkou, která je pro zákazníka přístupná bez pomoci jakéhokoli nástroje. Pokud je dosaženo maximální hodnoty indikovaného množství, indikace bude pokračovat a bude zobrazovat hodnotu od nuly kubických metrů.

Upřesnění: Dle ISO 4064 část 1:

- Indikační zařízení vodoměru musí poskytovat snadno čitelnou, spolehlivou a jednoznačnou vizuální indikaci indikovaného objemu. Kombinované měřidlo může mít dvě indikační zařízení, jejichž součet poskytuje indikovaný objem.
- Každé indikační zařízení musí poskytovat prostředky pro vizuální, jednoznačné ověřovací testy a kalibraci.
- Vizualizace ověřovaného displeje může mít buď nepřetržitý či přerušovaný pohyb.

Požadovaná dokumentace:

- Popis displeje a jeho menu.
- Popis vizuálního ověření displeje a vysvětlení, jak zrealizovat toto ověření.

Postup validace:

Ověření funkčnosti:

- Zkontrolujte, zda rozsah displeje pro zobrazení celkového množství má dostatečný počet míst.
- Iniciujte vizuální ověření displeje a
  - zkontrolujte, zda rozlišení splňuje požadavky
  - zkontrolujte, zda je speciální vybavení či software pro takovouto kontrolu součástí zařízení (je-li relevantní)

Příklad přijatelného řešení:

Displej vodoměru má dostatečný rozsah pro zobrazení hodnoty celkového množství vyhovující oběma podmínkám s požadovaným rozlišením. Zařízení je vybaveno přepínacími módy pro zobrazení hodnot celkového množství se správným rozlišením a zobrazení “test módu” s doplňujícími informacemi pro ověření. Tyto módy je možno zobrazit těmito prostředky:

- přes uživatelské rozhraní měřidla (viz P3/U3, např.: tlačítky na měřidle) nebo
- cyklickým průchodem přes jednotlivé módy zobrazení.

Avšak při používání více módů zobrazení musí být zřejmé, který displej je primární a musí být jasné, jak vyčíst hodnoty a nesmí dojít k nejednoznačnostem s ohledem k rozdílným módům zobrazení (viz I1-7).

Poznámka: Není ve shodě se základními požadavky směrnice 2014/32/EU (MID), článkem 7.6 Přílohy I, pokud organizace provádějící ověření, dozorový orgán či oznámený subjekt musí žádat výrobce o speciální zařízení či software.

Třída rizika B	Třída rizika C	Třída rizika D
I1-10: Test displeje *Pro ověření správné funkčnosti všech segmentů displeje, je třeba, aby bylo možné spustit test displeje.*		
Upřesnění: Test displeje musí být ve shodě s ISO 4064: • Měřidlo musí poskytnout možnost vizuální kontroly celého displeje s následujícími náležitostmi: 1) sedmi-segmentový displej: zobrazit všechny elementy (např. “osmičkový” test); 2) sedmi-segmentový displej: vynulování všech prvků (“mezerový” test); 3) grafický displej: ekvivalentní test demonstrující, že chyba displeje nezpůsobí mylnou interpretaci výsledku • Každý krok sekvence musí trvat aspoň 1 s..		
Požadovaná dokumentace: Popis testu displeje a objasnění, jak iniciovat tento test.		
Postup validace: Iniciujte test displeje a zkontrolujte, zda je možné vizuálně celý displej zkontrolovat.		
Příklad přijatelného řešení: Test displeje je iniciován speciálním příkazem uživatelského rozhraní (viz P3/U3, např.: tlačítky přístroje) nebo je součástí cyklické procedury, která zobrazuje rozdílné módy zobrazení.		

11.2.4 Příklady legálně relevantních parametrů, funkcí a dat

Přístup k prostředkům pro úpravu softwaru, a/nebo nastavení parametrů, které ovlivňují stanovení výsledků měření, musí být zabezpečen.[5]

Parametr	Chráněný	Nastavitelný	Poznámka
Kalibrační faktor	x		
Linearizační faktor	x		
Legálně relevantní konfigurace registrů	X		
Nastavení: • Korekce • Interpolace křivky	X		
Další relevantní parametry, které ovlivňují či by mohly ovlivnit výsledek měření	X		
Stahování legálně relevantního softwaru	x		

11.2.5 Přiřazení třídy rizika

Následující třída rizika je považována za vhodnou a měla by být použita, pokud jsou prováděny zkoušky softwaru založené na této příručce pro (softwarově řízený) vodoměr:

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

[5] Další pokyny týkající se zajištění vodoměru jsou uvedeny v příručce WELMEC Guide 13.3.

11.3 Plynoměry a přepočítávače množství plynu

11.3.1 Zvláštní předpisy, normy a jiné normativní dokumenty

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

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

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

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

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

11.3.2 Technický popis

11.3.2.1 Konfigurace hardwaru

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

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

11.3.2.2 Konfigurace softwaru

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

11.3.2.3 Princip měření

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

Měření objemu je neopakovatelné.

11.3.2.4 Detekce a řešení chyb

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

• Po prodělaném rušení musí být plynoměr opět:

- navrácen do provozu v mezích MPE a
- mít zabezpečeny všechny měřicí funkce a
- musí umožnit obnovu všech hodnot naměřených bezprostředně před rušením.

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

- Elektronické přepočítávací zařízení musí být schopno detekovat, že pracuje mimo provozní rozsah(y) uvedený výrobcem pro parametry, které jsou relevantní pro přesnost měření. V takovém případě přepočítávací zařízení musí zastavit načítání přepočítaného množství a může sčítat separátně přepočítané množství za dobu, kdy zařízení pracuje mimo provozní rozsah(y).

  Viz článek 9.1 směrnice MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002).

11.3.3 Specifické požadavky na software

11.3.3.1 Plynoměry a přepočítávače objemu

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

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

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

Třída rizika B	Třída rizika C	Třída rizika D
I2-4: Doplňkové funkce[6] *Doplňkové funkce, např. předplatné nebo intervalové měření[7], by neměly ovlivnit legálně relevantní měřicí funkce specifikované v MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002).*		
Upřesnění: • Doplňkové funkce jsou povoleny za předpokladu, že neovlivňují legálně relevantní měřicí funkce specifikované v MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002).		
Požadovaná dokumentace: Viz S1 až S3.		
Postup validace: Viz S1 až S3.		
Příklad přijatelného řešení: Viz S1 až S3.		

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

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

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

Třída rizika B	Třída rizika C	Třída rizika D
I2-7: MID-Příloha I, článek 10.5 (Čtení naměřených hodnot) *A. Naměřené hodnoty, které slouží jako základ pro stanovení ceny, mohou pocházet z různých registrů, které jsou aktivovány dálkově, dle času či jinými způsoby. Každý registr reprezentuje celkové množství odpovídající jedné fakturovací sazbě. Je třeba, aby měřidlo zobrazovalo hodnoty každého registru periodicky či na požádání přes uživatelské rozhraní.*		
Upřesnění: Kumulativní registry měřidla mohou být vynulovány před provedením posouzení shody. Během procesu posouzení shody dle příloh D, F či H1 musí být měřidla spotřeby vybavena všemi zajištěními, jak je specifikováno výrobcem a je specifikováno v TEC. Tato zajištění musí být takového rázu, že není možno vynulovat naměřené kumulativní hodnoty bez evidence tohoto zásahu.		
Požadovaná dokumentace: Dokumentace popisující, jak je možno získat naměřené hodnoty, které slouží jako základ pro stanovení ceny.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte správné zacházení s naměřenými hodnotami. *Ověření funkčnosti:* • Potvrďte správnou funkci zacházení s naměřenými hodnotami.		
Příklad přijatelného řešení: Pokud je měřidlo navrženo tak, že počítá množství definovaná v MID, Příloze IV Plynoměry a přepočítávače množství plynu (MI-002) v různých registrech, musí být možné zobrazit celkové množství každého registru na displeji pomocí uživatelského rozhraní (viz tento dokument, např. tlačítek měřidla) a stejně tak i zobrazit právě aktuální registr. Akceptovatelné je též zobrazení výsledků rozdílných registrů na několika displejích, periodicky či na požádání přes uživatelské rozhraní. Avšak při zobrazení těchto hodnot musí být jasné, který registr se, jak zobrazuje (na kterém displeji), v tomto ohledu nesmí dojít k nejednoznačnosti.		

Třída rizika B	Třída rizika C	Třída rizika D

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

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

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

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

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

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

Upřesnění:

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

Požadovaná dokumentace:

- Viz P6.

Postup validace:

Ověření na základě dokumentace:

- Viz P6.

Ověření funkčnosti:

- Viz P6.

Příklad přijatelného řešení:

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

Třída rizika B	Třída rizika C	Třída rizika D

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

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

Upřesnění:

Požadovaná dokumentace:

Dokumentace vnitřní reprezentace čítače.

Postup validace:

Ověření na základě dokumentace:

- Ověřte, že je počet míst dostatečný – že po uplynutí 8000 hodin provozu při průtoku Q_{max} se čítač nevrátí na svou počáteční hodnotu.

Příklad přijatelného řešení:

Typické hodnoty plynoměrů používaných v domácnostech jsou: Q_{max} = 6 m^3/h. Požadovaný rozsah je tedy 48 000 m^3, tedy zobrazení 5 číslic (současné mechanické i elektronické plynoměry jsou schopny zobrazit až 99 999 m^3, což je pro tento typ měřidla více než adekvátní).

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

11.3.3.2 Plynoměry

Třída rizika B	Třída rizika C	Třída rizika D
I2-11: MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002), článek 5.5 Testovací prvek plynoměru *Plynoměr musí být vybaven testovacím prvkem umožňujícím provádění testů v přiměřeném čase.*		
Upřesnění: Testovací prvek urychlující časově náročné procesy testování se obvykle používá k testování před instalací a běžným provozem. V testovacím režimu se musí používat stejné čítače a stejné části softwaru, které budou použity v běžném režimu provozu.		

Požadovaná dokumentace: Dokumentace testovacího prvku a návod na spuštění testovacího režimu.
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda lze všechny časově náročné procesy testování plynoměru provést prostřednictvím testovacího prvku.
Příklad přijatelného řešení: Pro testovací účely musí přírůstek testovacího prvku či pulzu nastat nejméně každých 60 sekund při Q_{min}, viz WELMEC Příručka 11.1, odstavec 2.4.4. Časovou základnu vnitřních hodin lze zrychlit. Procesy, které trvají např. týden, měsíc nebo dokonce rok a způsobují přetečení čítačů, lze otestovat v testovacím režimu za pouhé minuty až hodiny..

11.3.3.3 Elektronický přepočítávač

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

B	Třída rizika C	Třída rizika D
I2-13: MID, Příloha IV Plynoměry a přepočítávače množství plynu (MI-002), článek 9.1 Elektronický přepočítávač *V elektronických přepočítávačích množství plynu musí být přepočítávací číslo přepočítáváno v intervalu, který nepřekračuje 1 min u teplotního přepočítávače, a v intervalu nepřekračujícím 30 s u ostatních typů přepočítávačů.* *Avšak pokud z plynoměru nepřijde žádný signál objemu* *- po dobu delší než 1 min pro teplotní přepočítávače; nebo* *- po dobu delší než 30 s pro ostatní typy;* *přepočet není až do dalšího obdržení signálu vyžadován.*		
Upřesnění:		

Požadovaná dokumentace: Dokumentace sekvence přepočtu.
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda jsou přijatá opatření přiměřená.
Příklad přijatelného řešení:

11.3.4 Příklady legálně relevantních parametrů, funkcí a dat

Přístup k prostředkům pro modifikaci legálně relevantního softwaru, nastavení a/nebo parametrům majícími vliv na výsledky měření musí být zabezpečen.[8]
U plynoměrů například ale nejenom:

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

U přepočítávačů například ale nejenom:

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

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

mohly ovlivnit výsledek měření			
Stahování legálně relevantního softwaru	X		

11.3.5 Přiřazení třídy rizika

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

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

11.4 Elektroměry k měření činné energie

11.4.1 Zvláštní předpisy, normy a jiné normativní dokumenty

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

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

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

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

11.4.2 Technický popis

11.4.2.1 Konfigurace hardwaru

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

11.4.2.2 Konfigurace softwaru

Každý typ měřidla je specifický, ale obvykle se očekává, že se bude řídit doporučeními uvedenými v hlavní části této příručky

11.4.2.3 Princip měření

Elektroměry k měření činné energie průběžně kumulativně měří objem spotřebované energie. Přístroj zobrazuje celkové množství spotřebované energie. Při měření se využívají různé principy transdukce a multiplikace.
Měření energie nelze opakovat.

11.4.2.4 Detekce a řešení chyb

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

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

11.4.3 Specifické požadavky na software)

Třída rizika B	Třída rizika C	Třída rizika D
I3-1: MID, příloha V Měřiče aktivní elektrické energie (MI-003), článek 4.3.1 Obnova po chybě *Software se musí po chybě v důsledku rušení dokázat vrátit do běžného provozu.*		
Upřesnění:		
Požadovaná dokumentace: Stručný popis mechanismu obnovy po chybě a vysvětlení jak a kdy je tento mechanismus spuštěn. Krátký popis souvisejících testů provedených výrobcem.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda realizace obnovy po chybě probíhá náležitým způsobem. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Cyklicky vykonávaný podprogram mikroprocesoru nuluje hlídací mechanismus hardwaru, a brání tak jeho spuštění. Pokud některá funkce nebyla vykonána nebo pokud dokonce dojde k uvíznutí mikroprocesoru v jakékoliv nekonečné smyčce, nedojde k vynulování hlídacího mechanismu a hlídací mechanismus se tedy po určité době spustí.		

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

Třída rizika B	Třída rizika C	Třída rizika D
I3-3: Doplňkové funkce[9] *Doplňkové funkce, např. předplatné nebo intervalové měření, [10]by neměly ovlivnit legálně relevantní měřicí funkce specifikované v MID, Příloha V Elektroměry k měření činné energie (MI-003).*		
Upřesnění: Doplňkové funkce jsou povoleny za předpokladu, že neovlivňují legálně relevantní měřicí funkce specifikované v MID, Příloha V Elektroměry k měření činné energie (MI-003).		
Požadovaná dokumentace: Viz S1 až S3.		
Postup validace: *Viz S1 až S3.*		
Příklad přijatelného řešení: Viz S1 až S3.		

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

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

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

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

Třída rizika B	Třída rizika C	Třída rizika D
I3-7: MID-Příloha I, článek 10.5 (Čtení naměřených hodnot) *Naměřené hodnoty, které slouží jako základ pro stanovení ceny, mohou pocházet z různých registrů, které jsou aktivovány dálkově, dle času či jinými způsoby. Každý registr reprezentuje celkové množství odpovídající jedné fakturovací sazbě. Musí být možné zobrazit hodnoty na displeji periodicky či na požádání přes uživatelské rozhraní.*		
Upřesnění: Kumulativní registry měřidla mohou být vynulovány před provedením posouzení shody. Během procesu posouzení shody dle příloh D, F či H1 musí být měřidla spotřeby vybavena všemi zajištěními, jak je specifikováno výrobcem a je specifikováno v TEC. Tato zajištění musí být takového rázu, že není možno vynulovat naměřená kumulativní data bez evidence tohoto zásahu.		
Požadovaná dokumentace: Dokumentace popisující, jak je možno získat naměřené hodnoty, které slouží jako základ pro stanovení ceny.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte správné zacházení s naměřenými hodnotami. *Ověření funkčnosti:* • Potvrďte správnou funkci zacházení s naměřenými hodnotami.		
Příklad přijatelného řešení: Pokud je měřidlo navrženo tak, že načítá množství definovaná v MID, Příloze V Elektroměry k měření činné energie (MI-003) v různých registrech, musí být možné zobrazit celkové množství každého registru na displeji pomocí uživatelského rozhraní (viz tento dokument, např. tlačítek měřidla) a stejně tak i zobrazit právě aktuální registr. Je též možné zobrazit výsledky na několika displejích, periodicky či na požádání přes uživatelské rozhraní. Avšak při zobrazení těchto hodnot musí být jasné, který registr se, jak zobrazuje (na kterém displeji), v tomto ohledu nesmí dojít k nejednoznačnosti.		

Třída rizika B	Třída rizika C	Třída rizika D

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

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

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

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

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

Upřesnění:

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

Požadovaná dokumentace:

- Viz P6.

Postup validace:

Ověření na základě dokumentace:

- Viz P6

Ověření funkčnosti:

- Viz P6.

Příklad přijatelného řešení:

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

Třída rizika B	Třída rizika C	Třída rizika D

I3-9: MID, Příloha V Elektroměry k měření činné energie (MI-003), článek 5.2 počet míst

Čítač zobrazující celkové množství energie musí být tvořen takovou dostatečně dlouhou řadou číslic, aby se nemohl vrátit na původní hodnotu dříve než po 4000 hodinách provozu elektroměru při maximální kapacitě ($I = I_{max}$, $U = U_n$ and $PF = 1$).

Upřesnění:

Požadovaná dokumentace:

Dokumentace vnitřní reprezentace čítače elektrické energie a pomocných veličin.

Postup validace:

Ověření na základě dokumentace:

Ověřte, zda je počet míst dostatečný (vnitřní a na displeji).

Příklad přijatelného řešení:

Typické hodnoty třífázových elektroměrů jsou: P_{max} (4000h) = 3*60 A * 230 V * 4000h / 1000 = 165600 kWh. To vyžaduje zobrazení přinejmenším 6 číslic.

11.4.4 Příklady legálně relevantních parametrů, funkcí a dat

Přístup k prostředkům pro modifikaci legálně relevantního softwaru, nastavení a/nebo parametrům majícími vliv na výsledky měření musí být zabezpečen.[11]

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

11.4.5 Přiřazení třídy rizika

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

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

.

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

11.5 Měřidla tepelné energie

11.5.1 Zvláštní předpisy, normy a jiné normativní dokumenty

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

11.5.2 Technický popis

11.5.2.1 Konfigurace hardwaru

Měřidla tepelné energie jsou přístroje pro měření tepelné energie přenesené nosičem tepla. Měřidlo tepelné energie je buď samostatný přístroj, nebo kombinovaný přístroj tvořený několika podsestavami (modulární přístup), např. snímačem spotřeby, dvojicí tepelných čidel a přepočítávací jednotkou tak, jak je uvedeno ve směrnici MID, odst. 4(b). Měřidlo může být rovněž kombinací těchto dvou typů. Samostatné části měřidla tepelné energie, které mají vyhodnocovací jednotku (obsahující software) jsou též předmětem procesu validace.

11.5.2.2 Konfigurace softwaru

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

11.5.2.3 Princip měření

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

11.5.2.4 Detekce a řešení chyb

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

- musí vrátit do fungování v rámci MPE a
- musí mít všechny měřicí funkce ochráněny a
- musí být schopno obnovy všech naměřených dat přítomných těsně před rušením“ (viz EN 1434-4:2015 kapitola 7)

11.5.3 Specifické požadavky na software (měřidla tepelné energie)

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

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

Třída rizika B	Třída rizika C	Třída rizika D
I4-3: Doplňkové funkce[12] *Doplňkové funkce, např. předplatné nebo intervalové měření, [13]by neměly ovlivnit legálně rele-vantní měřicí funkce specifikované v MID, Příloha V Elektroměry k měření činné energie (MI-003).*		
Upřesnění: Doplňkové funkce jsou povoleny za předpokladu, že neovlivňují legálně relevantní měřicí funkce specifikované v MID, Příloha V Elektroměry k měření činné energie (MI-003).		
Požadovaná dokumentace: Viz S1 až S3.		
Postup validace: *Viz S1 až S3.*		
Příklad přijatelného řešení: Viz S1 až S3.		

Třída rizika B	Třída rizika C	Třída rizika D
I4-4: Prostředky zálohování *Musí existovat prostředky zajišťující pravidelnou zálohu naměřených dat, jako jsou naměřené hodnoty a současný stav procesu. Tato data musejí být uložena v energeticky nezávislé paměti.*		
Upřesnění: Intervaly uložení musí být dostatečně krátké, aby byl rozdíl mezi aktuálními a uloženými kumulativními hodnotami malý.		
Požadovaná dokumentace: Stručný popis toho, jaká data jsou zálohována a kdy se zálohování provádí. Výpočet maximální chyby, k níž může při zálohování kumulativních hodnot dojít.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda jsou naměřená data uložena v energeticky nezávislé paměti a zda je lze obnovit. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Naměřená data jsou zálohována dle potřeby.		

Třída rizika B	Třída rizika C	Třída rizika D
I4-5: Stahování softwaru *Během instalace softwaru nesmí být měřicí proces pozastaven celkově déle než 1 minutu.* *V případě, že proces instalace zabírá více než 1 minutu, musí být přijata další opatření (např. instalace probíhá v režimu nízké spotřeby energie).*		
Upřesnění: • Pokud je realizováno stahování softwaru kromě požadavků D1, D2, D3 a D4 aplikujte i tento požadavek. • Tento dodatečný požadavek přináší ujištění, že aplikace běžící v reálném čase nejsou přerušeny moc dlouho.		
Požadovaná dokumentace: Viz D1.		
Postup validace: Viz D1.		
Příklad přijatelného řešení: Viz D1.		

[12] Vždy by měl vzít výrobce v úvahu národní požadavky týkající se doplňkových funkcí.
[13] Další doporučení k intervalovému měření poskytuje WELMEC Guide 13.3.

Třída rizika B	Třída rizika C	Třída rizika D
I4-6: MID Příloha I, 8.5 (Zamezení vynulování naměřených kumulativních dat) *Údaje o celkovém spotřebovaném objemu nebo údaje, z nichž lze celkový spotřebovaný objem od-vodit, které se částečně či plně využívají k výpočtu ceny k zaplacení, musí být u přístrojů na měření spotřeby chráněny proti vynulování během provozu.*		
Upřesnění: • Kumulativní registry měřicího přístroje lze vynulovat před provedením procedury posouzení shody. Během procesu schvalování typu dle příloh D, F či H1 musí být měřidla spotřeby zabezpečena všemi prostředky, jak je specifikováno výrobcem a je specifikováno v TEC. Tato zajištění jsou takového rázu, že není možno vynulovat naměřená kumulativní data bez evidence tohoto zásahu. • Totalizéry kumulativních registrů měřidla mohou být vynulovány před dokončením příslušné procedury posouzení shody. Během procesu schvalování typu dle příloh D, F či H1 musí být měřidla tepelné energie zabezpečeny všemi ochrannými prostředky specifikovanými v TEC, které poskytují záznam o intervenci do registrů měřidla po provedení vynulování kumulativních naměřených dat. Není dovoleno vynulovat kumulativní registry v době používání v distribuční síti. NB: viz EN 1434-1:2015 bod 5.10 – Specifické požadavky na registrační zařízení		
Požadovaná dokumentace: Dokumentace ochranných prostředků proti vynulování energetických registrů.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda je operace vynulování kumulativních legálně relevantních naměřených dat zajištěna a že očekávaná zabezpečení poskytují záznam o intervenci. *Ověření funkčnosti:* • Ověřte správnou funkci aplikovaných zabezpečení, viz také P3/U3 a P4/U4.		
Příklad přijatelného řešení: Registr pro celkové naměřené množství musí být chráněn hardwarovou plombou. Ostatní registry, např. pro denní či noční tarif, mohou být chráněny stejnými prostředky jako parametry (viz P7/U7), přičemž musí být dostupný celkový (úhrnný kumulativní) registr chráněný hardwarovou plombou. Pro další informace viz WELMEC Guide 13.1.		

Třída rizika B	Třída rizika C	Třída rizika D

I4-7: MID-Příloha I, článek 10.5 (Čtení naměřených hodnot)

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

Upřesnění:

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

Požadovaná dokumentace:

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

Postup validace:

Ověření na základě dokumentace:

- Ověřte správné zacházení s naměřenými hodnotami.

Ověření funkčnosti:

- Potvrďte správnou funkci zacházení s naměřenými hodnotami.

Příklad přijatelného řešení:

Pokud je měřidlo navrženo tak, že načítá množství definovaná v MID, Příloze VI Měřidla tepelné energie (MI-004) v různých registrech, musí být možné zobrazit celkové množství každého registru na displeji pomocí uživatelského rozhraní (viz P3/U3, např. tlačítek měřidla) a stejně tak i zobrazit právě aktuální registr. Je též možné zobrazit výsledky na několika displejích, periodicky či na požádání přes uživatelské rozhraní. Avšak při zobrazení těchto hodnot musí být jasné, jak se který registr zobrazuje (na kterém displeji), v tomto ohledu nesmí dojít k nejednoznačnosti.

Pokud je potřeba může být na měřidle tepelné energie umístěn doplňující popis vysvětlující rozdílné registry či indikaci v testovacím režimu (viz I1-9).

Třída rizika B	Třída rizika C	Třída rizika D
I4-8: Ochrana proti záměrným změnám u elektroměrů k měření činné energie typu P s mechanickým čítačem *Vypočítaný výsledek kontrolního součtu či alternativní indikace sloužící k detekci modifikace softwaru musí být možné pro kontrolní účely na příkaz zobrazit, viz P6. Jako výjimka pro elektroměry k měření činné energie typu P s mechanickým čítačem je akceptovatelné, aby hodnota kontrolního součtu či alternativní indikace byla uvedena na štítku měřidla, a to, pokud jsou splněny následující podmínky A, B a C:* *A. Uživatelské rozhraní nenabízí prostředek k aktivaci zobrazení hodnoty kontrolního součtu či alternativní indikace modifikace softwaru na displeji nebo displej přístroje technicky neumožňuje tyto hodnoty zobrazit (mechanický čítač).* *B. Přístroj nemá žádné rozhraní, kterým by identifikaci softwaru mohl sdělit.* *C. Na vyrobeném přístroji již není možné software měnit nebo je změna softwaru možná pouze v kombinaci s výměnou hardwaru nebo jeho části..*		
Upřesnění: • Výrobce zodpovídá za to, že hodnota kontrolního součtu či alternativní indikace modifikace softwaru je na příslušném hardwaru správně uvedena. • Dále aplikujte všechna další upřesnění požadavků P6.		
Požadovaná dokumentace: • Viz P6.		
Postup validace: *Ověření na základě dokumentace:* • Viz P6 *Ověření funkčnosti:* • Viz P6.		
Příklad přijatelného řešení: Hodnota kontrolního součtu či alternativní indikace sloužící k detekci modifikace softwaru vytištěná na štítku přístroje.		

Třída rizika B	Třída rizika C	Třída rizika D
I4-9: Počet míst *Ve shodě s EN1434-1:2015 odstavcem 6.3.7:* *Displej zobrazující celkové množství tepla musí být schopný zaregistrovat minimálně, bez přetečení, množství tepla odpovídající přenesu tepla při kontinuálním provozu po dobu 3 000 hodin v horním kvadrantu tepelné energie. Množství tepla, měřeno měřidlem tepelné energie, pracující v horním kvadrantu tepelné energie po dobu 1 hodiny musí odpovídat minimálně jedné číslici nejmenšího rozlišení displeje.* *Vyhovění článku 7.6 a 10.5 přílohy I směrnice 2014/32/EU (MID):* *Měřidlo musí být navrženo tak, aby po uvedení na trh a do provozu umožňovalo kontrolu měření. Pokud je třeba, musí být součástí měřidla i zvláštní zařízení nebo programové vybavení pro tuto kontrolu. Také měřidlo, které lze odečítat na dálku, musí být v každém případě vybaveno metrologicky kontrolovanou indikační jednotkou, která je pro zákazníka přístupná bez pomoci jakéhokoli nástroje.* *Pokud je dosaženo maximální hodnoty indikovaného množství tepla, indikace bude pokračovat a bude zobrazovat hodnotu od nuly kubických metrů, viz též I1-9 (Počet míst)* *Poznámka: měřidlo tepla může být čten jako měřidlo tepelné energie. .*		
Upřesnění: • Pro testování musí být výstupní signál ve shodě s EN1434-2 odstavec 5.3. • Indikační zařízení měřidla tepelné energie musí poskytovat snadno čitelnou, spolehlivou a jednoznačnou vizuální indikaci indikovaného množství. Kombinované měřidlo může mít dvě indikační zařízení, jejichž součet poskytuje indikované množství. • Každé indikační zařízení musí poskytovat prostředky pro vizuální, jednoznačné ověřovací testy a kalibraci. • Vizualizace ověřovaného displeje může mít buď nepřetržitý či přerušovaný pohyb.		
Požadovaná dokumentace: • Dokumentace vnitřního zobrazení počítadla energie, snímače teploty a průtokoměrů. • Popis displeje a jeho menu. • Popis vizuálního ověření displeje a vysvětlení, jak zrealizovat toto ověření.		

Postup validace:
Ověření na základě dokumentace:
• Zkontrolujte, zda je rozsah dostačující (interní i displeje).
Ověření funkčnosti:
• Zkontrolujte, zda rozsah displeje pro zobrazení celkového množství má dostatečný počet míst.
• Iniciujte vizuální ověření displeje a
  • zkontrolujte, zda rozlišení splňuje požadavky
  • zkontrolujte, zda je speciální vybavení či software pro takovouto kontrolu součástí zařízení (jeli relevantní)		

Příklad přijatelného řešení: Displej měřidla tepelné energie má dostatečný rozsah pro zobrazení hodnoty celkového množství vyhovující oběma podmínkám s požadovaným rozlišením. Zařízení je vybaveno přepínacími módy pro zobrazení hodnot celkového množství se správným rozlišením a zobrazení “test módu” s doplňujícími informacemi pro ověření. Tyto módy je možno zobrazit těmito prostředky: • přes uživatelské rozhraní měřidla (viz P3/U3, např.: tlačítky na měřidle) nebo • cyklickým přepínáním různých režimů zobrazení. Avšak při používání více módů zobrazení musí být zřejmé, který displej je primární a musí být jasné, jak vyčíst hodnoty a nesmí dojít k nejednoznačnostem s ohledem k rozdílným módům zobrazení (viz I1-7). *Poznámka*: Není ve shodě se základními požadavky směrnice 2014/32/EU (MID), článkem 7.6 Přílohy I, pokud organizace provádějící ověření, dozorový orgán či oznámený subjekt musí žádat výrobce o speciální zařízení či software.		

Třída rizika B	Třída rizika C	Třída rizika D
I4-10: Test displeje *Pro ověření správné funkčnosti všech segmentů displeje, je třeba, aby bylo možné spustit test displeje.*		
Upřesnění: Test displeje je: • Měřidlo musí poskytnout možnost vizuální kontroly celého displeje s následujícími náležitostmi: 1) sedmi-segmentový displej: zobrazit všechny elementy (např. “osmičkový” test); 2) sedmi-segmentový displej: vynulování všech prvků (“mezerový” test); 3) grafický displej: ekvivalentní test demonstrující, že chyba displeje nezpůsobí mylnou interpretaci výsledku • Každý krok sekvence musí trvat aspoň 1 s.		
Požadovaná dokumentace: Popis testu displeje a objasnění jak iniciovat tento test.		
Postup validace: Iniciujte test displeje a zkontrolujte, zda je možné vizuálně celý displej zkontrolovat.		
Příklad přijatelného řešení: Test displeje je iniciován speciálním příkazem uživatelského rozhraní (viz P3/U3, např.: tlačítky přístroje) nebo je součástí cyklické procedury, která zobrazuje rozdílné módy zobrazení. .		

11.5.4 Příklady legálně relevantních parametrů, funkcí a dat

Přístup k prostředkům umožňujícím modifikaci softwaru, nastavení a/nebo parametrům, které ovlivňují výsledky měření, musí být zabezpečen.[14]

Parametr	Chráněný	Nastavitelný	Poznámka
Kalibrační faktor	x		
Linearizační faktor	x		
Legálně relevantní konfigurace registrů	X		
Další relevantní para-metry, které ovlivňují či by mohly ovlivnit výsledek měření – jednotka měřené energie (MWh, GJ), instalace senzoru průtoku (přímá či zpětná větev teplotního obvodu)	X		
Stahování legálně relevantního softwaru	X		

11.5.5 Přiřazení třídy rizika

Následující třídy rizika jsou považovány za odpovídající a měly by být aplikovány při zkouškách softwaru měřidel tepelné energie (řízených softwarem) dle této příručky:

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

[14] Další doporučení k zabezpečení měřidel tepelné energie poskytuje WELMEC Guide 13.3.

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

Měřicí systémy pro kontinuální a dynamické měření množství jiných kapalin než vody podléhají požadavkům směrnice MID. Zvláštní požadavky této kapitoly vycházejí pouze z přílohy I a přílohy VII (MI-005).

11.6.1 Zvláštní předpisy, normy a další normativní dokumenty

Konkrétní požadavky této kapitoly vycházejí z MID, přílohy VII a OIML R117-1 vydání 2019.

11.6.2 Technický popis

11.6.2.1 Konfigurace hardwaru

Měřicí systémy pro kontinuální a dynamické měření množství kapalin jiných než voda jsou buďto zařízení konstruovaná pro daný účel (typ P v tomto dokumentu), nebo se mohou skládat z několika částí, včetně univerzálních zařízení (typ U v tomto dokumentu).
Nejmenší možný měřicí systém musí obsahovat:

- měřidlo,
- předávací bod a
- hydraulický okruh.

Pro správnou funkci je často nutné doplnit:

- zařízení pro eliminaci plynu,
- filtr,
- čerpadlo a
- korekční zařízení.

Měřicí systém může být vybaven dalšími přídavnými a doplňkovými zařízeními.
Přídavná a doplňková zařízení mohou být:

- zařízení pro nastavení nuly;
- opakovací indikační zařízení;
- tiskárna;
- paměťové zařízení;
- zařízení pro indikaci ceny;
- totalizační indikační zařízení;
- korekční zařízení;
- konverzní zařízení;
- přednastavovací zařízení;
- samoobslužné uspořádání a
- samoobslužné zařízení.

Pokud jsou přídavná a doplňková zařízení součástí měřicích systémů pro kontinuální a dynamické měření množství kapalin jiných než voda jako samostatná zařízení, která lze odpojit bez porušení plomby (plomb) a obsahují legálně relevantní software, musí být použito rozšíření T.
Pokud je pro jednu měřicí operaci určeno několik měřidel, považují se tato měřidla za jeden měřicí systém.

Pokud má několik měřidel určených pro samostatné měřicí operace společné prvky (počítadlo, filtr, zařízení pro eliminaci plynu, převodní zařízení atd.), považuje se každé měřidlo za samostatný měřicí systém, který sdílí společné prvky.

11.6.2.2 Konfigurace softwaru

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

11.6.2.3 Princip měření

Množství kapaliny se měří pomocí měřicího snímače objemu nebo snímače hmotnostního průtoku, které mohou pracovat na různých principech. Naměřené množství se ve vysílači převede na signál (např. impulsy) a odešle se do počítacího a indikačního zařízení. Ty společně tvoří měřidlo. K měřidlu lze připojit další přídavná měřicí zařízení pro měření charakteristiky kapaliny. Např. snímač teploty, snímač tlaku. Naměřenou veličinu lze přepočítat na základní podmínky, např. pomocí funkce ATC (automatická teplotní kompenzace) pro přepočet na 15 °C. Měřené množství musí být uvedeno v mililitrech, kubických centimetrech, litrech, metrech krychlových, gramech, kilogramech nebo tunách.

11.6.2.4 Detekce a řešení chyb

Požadavek přílohy VII (MI-005), článek 3.1 se týká elektromagnetického rušení. Tento požadavek je třeba vykládat ve vztahu k softwarově řízeným zařízením, protože detekce rušení a oprava chyb nejsou možné bez vzájemné kompatibility specifických hardwarových součástí a modulů. Z hlediska softwaru nezáleží na typu rušení, např.: elektromagnetické, elektrické nebo mechanické rušení, protože postupy obnovy jsou vždy stejné.

11.6.3 Specifické požadavky na software

Třída rizika B	Třída rizika C	Třída rizika D
I5-1: Obnova po chybě *Nepřerušitelné měřicí systémy musí být navrženy a vyrobeny tak, aby při jejich vystavení rušivým vlivům nedocházelo k závažným poruchám. Zjištění nesprávného postupu při generování, přenosu, zpracování a/nebo indikaci naměřených údajů kontrolními zařízeními musí vést k příslušným opatřením.* *Přerušitelné elektronické měřicí systémy musí být navrženy a vyrobeny tak, aby při vystavení rušivým vlivům buď:* *a) indikace výsledku měření vykazovala momentální odchylku, kterou nelze interpretačně zaznamenat, zapamatovat nebo přenést jako výsledek měření. V případě přerušitelného systému to navíc může znamenat i znemožnění provedení jakéhokoli měření, nebo* *b) změna výsledku měření je větší než hodnota kritické změny; v takovém případě musí měřicí systém umožnit načtení výsledku měření těsně před dosažením hodnoty kritické změny a přerušit průtok.*		
Upřesnění: U nepřerušitelných měřicích systémů musí zjištění nesprávného postupu při generování, přenosu, zpracování a/nebo indikaci měřených údajů kontrolními zařízeními vést k následujícím opatřením: • automatickou opravu nesprávné funkce; nebo • zastavení pouze vadného zařízení, pokud měřicí systém bez tohoto zařízení nadále vyhovuje předpisům. Pokud kontrolní zařízení přerušitelných elektronických měřicích systémů zjistí závažné závady nebo jakoukoli nesrovnalost při vytváření, přenosu, zpracování nebo indikaci měřených údajů, musí reagovat tak, že buď: • automatickou opravu závady, nebo • zastaví pouze vadné zařízení, pokud měřicí systém bez tohoto zařízení nadále vyhovuje předpisům, nebo • měřicí systém musí umožnit načtení výsledku měření těsně předtím, než došlo ke kritické změně hodnoty, a přerušit průtok. Další požadavek je uveden v OIML R117-1:2019, oddíl A.1.5 týkající se parametrů generujících poruchy.		
Požadovaná dokumentace: Stručný popis toho, co se kontroluje, co je nutné pro spuštění procesu detekce poruchy, jaká akce se provede při zjištění poruchy. Seznam parametrů a jejich platných a kontrolovaných rozsahů, které mohou generovat poruchy a které budou detekovány softwarem, včetně očekávané reakce, a pokud je to nutné pro pochopení detekčního algoritmu, jeho popis.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda je realizace obnovy po poruše vhodná. *Ověření funkčnosti:* • potvrďte správnou funkci za přítomnosti definovaných ovlivňujících veličin a vyvolaných chyb.		
Příklad přijatelného řešení: Hardwarový watchdog je resetován cyklicky zpracovávaným mikroprocesorovým podprogramem, aby bylo zablokováno spuštění watchdogu. Pokud nebyla zpracována žádná funkce nebo - v nejhorším případě - mikroprocesor zůstane viset v libovolné nekonečné smyčce, k resetu watchdogu nedojde a v takovém případě se watchdog po určitém časovém úseku spustí a resetuje mikroprocesor.		

Třída rizika B	Třída rizika C	Třída rizika D
I5-2: Legálně nerelevantní software a dynamické chování *Legálně nerelevantní software nesmí nežádoucím způsobem ovlivňovat dynamiku procesu měření.*		
Upřesnění: Tento doplňující požadavek má zajistit, že při použití měřicích přístrojů v reálném čase nedojde k nežádoucímu ovlivnění dynamického chování legálně relevantního softwaru legálně nerelevantním softwarem, tj. že zdroje legálně relevantního softwaru nebudou nežádoucím způsobem omezeny legálně nerelevantním softwarem.		
Požadovaná dokumentace: • Popis hierarchie přerušení. • Časové schéma úkolů softwaru. Limity a poměrné časy pro legálně nerelevantní úkoly.		
Postup validace: *Ověření na základě dokumentace:* • Programátor legálně nerelevantní části softwaru má k dispozici dokumentaci s limity poměrných časů pro legálně nerelevantní úkoly. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Návrh hierarchie přerušení musí zamezit nežádoucím vlivům.		

Třída rizika B	Třída rizika C	Třída rizika D
I5-3: Doplňkové funkce[15] *Doplňkové funkce, např. předplatné nebo intervalové měření, by neměly ovlivnit legálně relevantní měřicí funkce specifikované v MID, Příloha VII (MI-005).*		
Upřesnění: Doplňkové funkce jsou povoleny za předpokladu, že neovlivňují legálně relevantní měřicí funkce specifikované v MID, Příloha VII (MI-005).		
Požadovaná dokumentace: Viz S1 až S3.		
Postup validace: *Viz S1 až S3.*		
Příklad přijatelného řešení: Viz S1 až S3.		

[15] Vždy by měl vzít výrobce v úvahu národní požadavky týkající se doplňkových funkcí.

Třída rizika B	Třída rizika C	Třída rizika D
I5-4: Prostředky zálohování *V případě nepřerušitelných měřicích systémů může existovat zařízení, které zajišťuje pravidelné zálohování měřených dat, jako jsou naměřené hodnoty a aktuální stav procesu. Tato data musí být uložena v energeticky nezávislém úložišti. Měřicí systém musí být vybaven záložním zdrojem, který zajistí provedení všech měřicích funkcí v případě výpadku hlavního napájení, nebo musí být vybaven prostředky pro uchování a zobrazení dat, aby bylo možné ukončit probíhající transakci.*		
Upřesnění: Interval ukládání musí být dostatečně krátký, aby rozdíl mezi aktuálními a uloženými kumulativními naměřenými daty byl malý.		
Požadovaná dokumentace: • Stručný popis toho, jaká data jsou zálohována a kdy k tomu dochází. • Výpočet maximální chyby, která může nastat při zálohování kumulativních dat měření.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda jsou naměřená data uložena v energeticky nezávislém úložišti a zda je lze obnovit. *Ověření funkčnosti:* • Ověřte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: • Data z měření se pravidelně zálohují (frekvence závisí na aplikaci) na energeticky nezávislou paměť v paměťovém zařízení. • Hardwarový watchdog se spustí, pokud není cyklicky resetován. Tento alarm aktivuje přerušení v mikroprocesoru. Přiřazená procedura přerušení okamžitě shromažďuje naměřená data, stavové hodnoty a další relevantní údaje a ukládá je do energeticky nezávislého úložiště, např. do paměti EEPROM nebo jiného vhodného úložiště. Poznámka: Předpokládá se, že přerušení watchdogu má nejvyšší prioritu přerušení a může dominovat nad jakýmkoli normálním zpracováním nebo libovolnou nekonečnou smyčkou, tj. řízení programu vždy přeskočí na rutinu přerušení, pokud watchdog selže.		

Třída rizika B	Třída rizika C	Třída rizika D
I5-5: Stahování softwaru *Během instalace softwaru musí být proces měření zablokován nebo musí být vhodným způsobem zaručeno správné měření.*		
Upřesnění: • Pokud je realizováno stahování softwaru kromě požadavků D1, D2, D3 a D4 aplikujte i tento požadavek. • Tento dodatečný požadavek přináší ujištění, že aplikace běžící v reálném čase nejsou přerušeny.		
Požadovaná dokumentace: Viz D1, D2, D3 a D4.		
Postup validace: Viz D1, D2, D3 a D4..		
Příklad přijatelného řešení: Viz D1, D2, D3 a D4.		

Třída rizika B	Třída rizika C	Třída rizika D
I5-6: Vytištěné označení softwaru *Vypočítanou hodnotu kontrolního součtu či alternativní indikace sloužící k detekci modifikace softwaru musí být možné pro kontrolní účely na příkaz zobrazit, viz P6. Jako výjimka pro elektroměry k měření činné energie typu P s mechanickým čítačem je akceptovatelné, aby hodnota kontrolního součtu či alternativní indikace byla uvedena na štítku měřidla, a to, pokud jsou splněny následující podmínky A, B a C:* *A. Uživatelské rozhraní nenabízí prostředek k aktivaci zobrazení hodnoty kontrolního součtu či alternativní indikace modifikace softwaru na displeji nebo displej přístroje technicky neumožňuje tyto hodnoty zobrazit (mechanický čítač).* *B. Přístroj nemá žádné rozhraní, kterým by identifikaci softwaru mohl sdělit.* *C. Na vyrobeném přístroji již není možné software měnit nebo je změna softwaru možná pouze v kombinaci s výměnou hardwaru nebo jeho části..*		
Upřesnění: • Štítek s označením softwaru musí být nesmazatelný a nepřenosný. • Výrobce hardwaru nebo příslušné hardwarové části zodpovídá za to, že je označení softwaru správně uvedeno na příslušném hardwaru. • Dále platí všechna další upřesnění požadavků P6.		
Požadovaná dokumentace: • Viz P2/U2.		
Postup validace: *Ověření na základě dokumentace:* • Viz P2/U2 *Ověření funkčnosti:* • Viz P2/U2		
Příklad přijatelného řešení: Vytištěné označení softwaru na štítku přístroje.		

Třída rizika B	Třída rizika C	Třída rizika D
I5-7: Nastavení parametrů • *Pro účely ověření měřicího přístroje musí být možné zobrazit nebo vytisknout aktuální nastavení parametrů, které určují legálně relevantní charakteristiky měřicího systému.* • *Parametry musí být chráněny, viz P7 a U7. V případě auditní stopy se časové razítko odečítá z hodin přístroje. Nastavení času a datumu musí být chráněno.*		
Upřesnění: Tyto požadavky jsou uvedeny v OIML R117-1:2019, oddíl A.1.3.3.		
Požadovaná dokumentace: Informace o nastavení parametrů a možnostech ověření.		
Postup validace: Ověřte nastavení parametrů a možnosti ověření měřicího přístroje.		
Příklad přijatelného řešení: Výše uvedená kritéria musí být splněna.		

Třída rizika B	Třída rizika C	Třída rizika D
I5-8: Přídavná a doplňková zařízení (AAD) *Pokud je AAD součástí měřicího zařízení, které je možné odpojit (deinstalovat/vyjmout/ odmontovat), použije se rozšíření T.*		
Upřesnění: V případech, kdy měřicí zařízení obsahuje AAD bez legálně relevantního softwaru, musí být údaje z AAD s legálně nerelevantním softwarem jasně odlišitelné od údajů z AAD s legálně relevantním softwarem. V případech, kdy je možné AAD s legálně relevantním softwarem odpojit bez porušení plomby, která chrání připojení k měřicímu zařízení, musí být použito rozšíření T.		
Požadovaná dokumentace: • Seznam AAD, který obsahuje legálně relevantní software s popisem. • Podle rozšíření T. • Podle rozšíření S (pokud se použije)		
Postup validace: *Ověření na základě dokumentace:* • Podle rozšíření T. • Podle rozšíření S (pokud se použije). • Ověřte, zda dokumentace obsahuje úplný seznam AAD s LRSW. *Ověření funkčnosti:* • Podle rozšíření T. • Podle rozšíření S (pokud se použije).		
Příklad přijatelného řešení:		

11.6.4 Příklady legálně relevantních parametrů, funkcí a dat

Přístup k prostředkům umožňujícím modifikaci softwaru, nastavení a/nebo parametrům, které ovlivňují výsledky měření, musí být zabezpečen.[16]

Parametr	Chráněný	Nastavitelný	Poznámka
Kalibrační faktor	x		
Linearizační faktor	x		
Legálně relevantní konfigurace registrů	X		
Další relevantní parametry, které mohou nebo mohou ovlivnit výsledek měření, například, nikoli však výlučně: • Počet desetinných míst pro indikaci množství • Vypnutí nízkého průtoku • Servisní příkazy (uložení ID periferních jednotek, opětovné nastavení elektronických součtů, kompletní inicializace paměti - elektronické souhrny, statistiky a historie a přechod parametrů do továrního nastavení). • Hodnota měřená hmotnostním měřidlem - nastavení L/kg • Potlačení dilatace výdejní hadice - nastavení skrytého množství na začátku výdeje. • Korekční faktor měřidla • Doba měření po zavěšení trysky • impuls / L, impuls / kg • Aktivace automatické teplotní kompenzace pro jednotlivé trysky (ATC) a kalibrace teplotních čidel. • Typ nebo hustota paliva • Přiřazení teplotních čidel k jednotlivým tryskám	X		

[16] Viz také příručka WELMEC Guide 10.6: Příručka pro zabezpečení výdejních stojanů paliva.

• Konfigurace měřiče hmotnosti • Nastavení nulového bodu měřiče hmotnosti			
Stahování legálně relevantního softwaru	X		
Softwarové nastavení/konfigurace v případě pulzních signálů	X		
Nastavení/konfigurace softwaru v případě digitálních dat	X		

11.6.5 Přiřazení třídy rizika

Následující třída rizika je považována za vhodnou a měla by být použita, pokud jsou prováděny zkoušky softwaru založené na této příručce pro (softwarově řízené) měřicí systémy pro kapaliny jiné než voda:

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

11.7 Váhy

Váhy se dělí do dvou hlavních kategorií:

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

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

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

11.7.1 Zvláštní předpisy, normy a jiné normativní dokumenty

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

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

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

Směrnice MID se nevztahuje na následující kategorii automatických vážicích přístrojů:

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

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

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

11.7.2 Technický popis

11.7.2.1 Konfigurace hardwaru

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

Kontinuální součtová váha je pásová váha určující hmotnost určitého produktu na dopravním pásu, který projíždí přes snímač zatížení. Systém se obvykle skládá z dopravního pásu, válců, snímače váhy na siloměrech, zdroje napájení, elektronických ovladačů a indikačního zařízení. Je také vybaven prostředky na úpravu napnutí pásu.

11.7.2.2 Konfigurace softwaru

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

11.7.2.3 Princip měření

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

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

11.7.2.4 Chyby

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

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

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

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

Třída rizika B	Třída rizika C	Třída rizika D
I6-2: Prostředky zálohování *Pro případ rušení musí existovat prostředky zajišťující pravidelnou zálohu naměřených dat, jako jsou naměřené hodnoty a současný stav procesu.*		
Upřesnění: a. Popis stavu a důležité údaje musí být uloženy v energeticky nezávislé paměti. b. Tento požadavek obvykle implikuje použití řízené paměti zajišťující automatické zálohování v případě rušení. Pravidelné zálohování je přípustné pouze tehdy, když není možné použít řízenou paměť kvůli hardwarovým nebo funkčním omezením. V takovém výjimečném případě musí být intervaly uložení zálohy dostatečně krátké, tj. maximální možný rozdíl mezi aktuálními a uloženými naměřenými daty se musí vejít do definovaného zlomku maximální přípustné chyby (viz oddíl Požadovaná dokumentace). c. Prostředky zálohování by obvykle měly zahrnovat i odpovídající prostředky pro probuzení z režimu spánku, bránící tomu, aby se vážicí systém (včetně příslušného softwaru) v důsledku rušení nedostal do neurčitého stavu.		
Požadovaná dokumentace: Stručný popis mechanismu zálohování a dat, která jsou zálohována, včetně situací, kdy k zálohování dochází. Specifikace nebo výpočet maximální chyby, k níž může dojít u kumulativních naměřených dat, pokud je prováděno cyklické (periodické) zálohování.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte prostředky zálohování. *Ověření funkčnosti:* • Ověřte, zda při simulovaném rušení mechanismus zálohování funguje způsobem popsaným v dokumentaci.		
Příklad přijatelného řešení: Hlídací mechanismus hardwaru se spustí, pokud není cyklicky nulován. Tento alarm vyvolá přerušení v mikroprocesoru. Přiřazený přerušovací program okamžitě nashromáždí naměřená data, hodnoty stavu a jiné relevantní údaje a uloží je do energeticky nezávislé paměti, např. EEPROM, nebo do jiné vhodné paměti. *Poznámka:* Předpokládá se, že přerušení vyvolané hlídacím mechanismem má nejvyšší prioritu, a je tudíž nadřazené jakýmkoliv běžným operacím nebo jakékoliv případné nekonečné smyčce, tj. ovladač programu při spuštění hlídacího mechanismu vždy přeskočí na přerušovací program.		

11.7.4 Příklady legálně relevantních parametrů, funkcí a dat

Tabulka 11-1: V tabulce jsou uvedeny příklady legálně relevantních funkcí a dat a také funkcí a dat specifických pro daný přístroj (DF, DD) či daný typ přístroje (TF, TD) u automatických vážicích přístrojů a neautomatických vážicích přístrojů (R76). Zkratka VV označuje proměnné.

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

Tabulka 11-1: Příklady funkcí a dat - legálně relevantních a specifických pro daný přístroj nebo typ

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

11.7.5 Další vlastnosti

Žádné

11.7.6 Přiřazení třídy rizika

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

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

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

11.8 Taxametry

Taxametry podléhají předpisům směrnice MID. Specifické požadavky na tyto přístroje jsou uvedeny v Příloze MI-007. Tyto požadavky spolu s normativním dokumentem OIML R 21 (2007) a WELMEC CT-007 (korespondenční tabulka) byly vzaty v potaz.

11.8.1 Zvláštní předpisy, normy a jiné normativní dokumenty

OIML doporučení R 21 pro taxametry je normativním dokumentem ve smyslu směrnice MID. WELMEC CT-007 pro taxametry ukazuje shodu mezi základními požadavky směrnice MID a OIML R 21. WELMEC 12.1 poskytuje specifickou interpretaci MID a odpovídajícími články OIML R 21.

11.8.2 Technický popis

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

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

11.8.3 Specifické požadavky na software

MID Příloha IX, 4:

Taxametr musí být schopen prostřednictvím vhodně zabezpečeného (zabezpečených) rozhraní poskytovat tyto údaje:

– údaj o pracovní poloze: „Volný“, „Obsazeno“ nebo „Jízdné“;

– souhrnné údaje podle bodu 15.1;

– všeobecné informace: konstantu generátoru signálu vzdálenosti, datum zabezpečení, identifikaci vozidla, reálný čas, identifikaci sazby,,

– informace o jízdném za cestu: celkovou účtovanou cenu, jízdné, výpočet jízdného, příplatek, datum, počáteční čas jízdy, konečný čas jízdy, ujetou vzdálenost,

– informace o sazbě (sazbách): parametry sazby (sazeb).

Vnitrostátní právní předpisy mohou vyžadovat, aby byla k rozhraní (rozhraním) taxametru připojena určitá zařízení. Jestliže je takové zařízení vyžadováno, pak musí být prostřednictvím zabezpečeného na-stavení možné automaticky vyřadit taxametr z provozu z důvodů nepřipojení nebo nesprávného fungování tohoto požadovaného zařízení.

MID Příloha IX, 9:

V případě poklesu napájení pod minimální hodnotu potřebnou pro provoz přístroje stanovenou výrobcem taxametr musí:

– nadále správně fungovat, nebo správně obnovit svou činnost bez ztráty dat dostupných před výpadkem napájení, pokud se jedná o krátkodobý stav, tj. v důsledku restartování motoru,

– ukončit stávající měření a vrátit se do stavu „Volný“ („For Hire“), pokud se jedná o dlouhodobější výpadek napájení.

MID Příloha IX, 15.2:

Pokud je taxametr odpojen od zdroje, musí poskytnout dlouhodobé uložení souhrnných hodnot. Uložená data v taxametru musí být dostupná 1 rok a musí existovat možnost jejich vyčtení a přenesení na jiné médium.

MID Příloha IX, 19:
Taxametr a pokyny k jeho instalaci stanovené výrobcem musí být takové, aby v případě instalace taxametru podle pokynů výrobce bylo dostatečně znemožněno provádění neoprávněných změn měřicího signálu ujeté vzdá-lenosti.

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

Třída rizika B	Třída rizika C	Třída rizika D
I7-2: Dlouhodobé uchovávání dat *Musí existovat prostředek, který automaticky uchovává souhrnné údaje pokud je přístroj odpojen od zdroje napájení.*		
Upřesnění: 1) Souhrnné údaje by obvykle měly být uloženy v energeticky nezávislém úložišti. 2) Údaje by měly být zálohovány průběžně nebo tak často, aby byl pokryt čas detekce výpadku do doby než poklesne (vnitřní) napětí pod provozní úroveň.		
Požadovaná dokumentace: Stručný popis toho, jaká data jsou zálohována a kdy.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda jsou v případě odpojení od zdroje napájení zálohovány všechny souhrnné údaje. *Ověření funkčnosti:* • Potvrďte správné fungování při působení definovaných vlivů a vyvolaných chyb.		
Příklad přijatelného řešení: Dojde-li k poklesu napětí detektor poklesu napětí podnítí přerušení. Asociovaný prostředek shromáždí souhrnné údaje a uloží je do energeticky nezávislé paměti před tím než vnitřní napětí poklesne pod provozní úroveň. Nebo souhrnné údaje jsou uchovávány průběžně i energeticky nezávislé paměti. Poznámka: Předpokládá se, že přerušení na základě napětí má vysokou prioritu a je nadřazeno jiným běžným procesům nebo nahodilým nekonečným smyčkám, tj. kontrolní rutina programu při poklesu napětí vždy vyvolá přerušení.		

Třída rizika B	Třída rizika C	Třída rizika D
I7-3: Podvodné úpravy *Musí existovat prostředek kontrolující věrohodnost signálu měření vzdálenosti.*		
Upřesnění: 1) Prostředek musí obsahovat odpovídající rutinu, která kontroluje, zda impulzy nebo obdržené informace jsou věrohodné.		
Požadovaná dokumentace: Stručný popis toho, jaké rutiny jsou použity k otestování věrohodnosti.		
Postup validace: *Ověření na základě dokumentace:* • Ověřte, zda prostředek kontroluje věrohodnost a jak. *Ověření funkčnosti:* • Potvrďte správné fungování při působení vyvolaných chyb.		
Příklad přijatelného řešení: Neustále jsou na výstupu generátoru signálu měření vzdálenosti kontrolovány následující definované vlastnosti týkající se úrovně napájení, šířky impulzu a vztahu rychlosti a frekvence (stabilita signálu). Poznámka: Výstup může být digitálního charakteru, např. ze sběrnice CAN daného vozidla.		

11.8.4 Příklady legálně relevantních parametrů, funkcí a dat

Jako doplnění funkcí zmíněných v odstavci 11.8.2 jsou v následující tabulce uvedeny typické parametry taxametru, které by měli být brány v úvahu.

Parametr	Chráněný	Nastavitelný	Poznámka
Konstanta k	x		impulzy / km
Čas / datum	x	x	-
Sazby (obsahující parametry pro automatickou změnu sazby)		x	jednotka měny / km, jednotka měny / h
Specifika země/regionu	***x***	x	měnová jednotka, metoda výpočtu S / D, formulace/jazyk atd.
Parametry rozhraní		x	modulační rychlost atd.

Přinejmenším sazby musí být chráněny samostatně.
Také následující údaje mohou být vzaty v úvahu:

Údaj	Poznámka
Parametry rozhraní:	modulační rychlost atd.
příloha IX, 4:	
Údaj o pracovní poloze:	Volný“, „Obsazeno“ nebo „Jízdné“;
Souhrnné údaje:	podle bodu 15.1 (jednotka měny, km, h)
Všeobecné informace:	konstanta generátoru signálu vzdálenosti (impulzy/km) datum zabezpečení (ddmmyyyy) identifikaci vozidla (licenční číslo dle štítku) reálný čas (hh:mm) identifikaci sazby (kontrolní součet)
Informace o jízdném za cestu:	celkovou účtovanou cenu (jednotka měny) jízdné (jednotka měny) výpočet jízdného (jednotka měny, km, h) příplatek (jednotka měny) datum (ddmmyyyy) počáteční čas jízdy (hh:mm) konečný čas jízdy (hh:mm) ujetou vzdálenost (km)
Informace o sazbě (sazbách):	parametry sazby (sazeb), (jednotka měny / km, jednotka měny / h)

11.8.5 Další vlastnosti

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

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

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

11.8.6 Přiřazení třídy rizika

V současnou chvíli jsou dle výsledků dotazníku WELMEC WG 7 (2004) a v souladu s budoucími rozhodnutími příslušné pracovní skupiny WELMEC WG12 taxametry považovány za odpovídající následující třídy rizika. Měly by být použity při zkouškách softwaru taxametrů (řízených softwarem) dle této příručky:

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

11.9 Ztělesněné míry

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

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

11.10 Měřicí přístroje na měření rozměrů

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

Chybějící odstavce budou v případě nutnosti doplněny v budoucnu.

10.9.6 Přiřazení třídy rizika

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

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

11.11 Analyzátory výfukových plynů

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

Chybějící odstavce budou v případě nutnosti doplněny v budoucnu.

10.10.6 Přiřazení třídy rizika

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

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

12 Vzor protokolu o zkoušce (včetně kontrolních seznamů)

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

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

12.1 Informace náležející do certifikátu

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

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

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

Obrázek 12-1: Označení vybraného typu, třídy rizika a příslušných rozšíření

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

3. **Ověření integrity softwaru**
   - Pro rizikovou třídu C a vyšší: uvedení kontrolního součtu či hodnoty alternativní metody se stejnou úrovní požadavků
   - Pro rizikovou třídu C a vyšší: přesný popis způsobu zobrazení kontrolního součtu či hodnoty alternativní metody se stejnou úrovní požadavků
     Pozn.: Odkaz na dokumentaci (např. uživatelský manuál) je nevhodný.
   - Popis způsobu zobrazení údajů z auditní stopy, pokud jsou aplikovány
   - Popis hardwarového plombování (plombování) a případně dalších typů plombování ve vztahu k softwaru.
   - Uvedení dalších způsobů ochrany integrity, pokud jsou aplikovány.

4. Stručný popis softwarového prostředí

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

12.2 Vzor obecné části protokolu o zkoušce

Protokol o zkoušce č. XYZ122344

Průtokoměr Dynaflow, model DF101

Validace softwaru

(X příloh)

Pověření

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

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

Zadavatel

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

Zkoušený přístroj

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

- měření průtoku kapalin
- zobrazení změřeného objemu
- rozhraní převodníku

Dle příručky WELMEC Guide 7.2 je průtokoměr popsán následovně:

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

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

Typ softwaru

Risk Class [A-E]	P	U	O	L	T	S	D	Ix [1-6]
C	x			x				I1

Vestavěný software měřicího přístroje vyvinula firma

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

Identifikace software:

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

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

Při validaci byly předloženy následující dokumenty výrobce:

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

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

Ověřování integrity softwaru

- U rizikových tříd C a vyšších uveďte kontrolní součet nebo alternativní metodu se stejnou úrovní požadavků.
- Pro třídu rizika C a vyšší přesně popište, jak zobrazit kontrolní součet nebo alternativní metodu se stejnou úrovní požadavků.
- Poznámka: Odkaz na dokument (např. uživatelskou příručku) není vhodný.
- Popište, jak zobrazit auditní stopu, pokud je to relevantní.
- Popište hardwarovou plombu (plomby) a další typy plomb ve vztahu k softwaru, je-li to relevantní.
- Případně další prostředky ochrany integrity.

Krátký popis softwarového prostředí

- Uveďte příslušné informace týkající se:
- Operační prostředí nezbytné pro provoz softwaru (např. operační systém).
- Softwarové moduly pod legální kontrolou (pokud je implementována separace softwaru).
- Hardwarová a softwarová rozhraní (např. infrared, Bluetooth, Wireless LAN...).
- Odkazy na elektronické (hardwarové) části a jejich umístění v měřicím přístroji včetně jejich případného zajištění.

Postup zkoušení

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

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

Byla ověřena shoda s následujícími požadavky:

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

Kontrolní seznam pro výběr konfigurace tvoří přílohu 1 této zprávy.

Přístroji byla přiřazena třída rizika C.

Byly použity následující metody validace:

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

Výsledek

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

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

Kontrolní seznamy k požadavkům P tvoří přílohu 2.1 této zprávy.

Kontrolní seznamy k požadavkům L tvoří přílohu 2.2 této zprávy.

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

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

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

Tento výsledek je platný pouze pro zkoušený přístroj.

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

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

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

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

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

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

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

12.4.1 Kontrolní seznam základních požadavků na přístroje typu P

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

12.4.2 Kontrolní seznam základních požadavků na přístroje typu U

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

U6		Jsou legálně relevantní software a naměřená data chráněny proti nepřípustným záměrným modifikacím či výměně?				
U7		Jsou legálně relevantní parametry zabezpečeny proti nepřípustným modifikacím?				
U8		Je zajištěna autentičnost prezentovaných naměřených dat?				
**V případě odchylky proti požadavkům na software je nutné uvést vysvětlení.*						

12.4.3 Kontrolní seznam pro specifické požadavky rozšíření O

Kontrolní seznam požadavků rozšíření L						
Požadavek	**Postupy zkoušení**		**Vyhověl**	**Nevyhověl**	**Nerelevantní**	**Poznámky***
O1		Je hardwarová část, na které běží legální operační systém, chráněna proti úmyslným změnám?				
O2		U komponent kategorie 1 a kompletních přístrojů: poskytuje bootovací proces stejně nakonfigurované prostředí pro spuštění legálně relevantního softwaru?				
O3		Zajišťuje konfigurace operačního systému dostatek prostředků pro provoz legálně relevantní aplikace?				
O4		Je operační systém nakonfigurován tak, aby legálně relevantní softwarová aplikace nemohla být nepřípustně ovlivněna funkcemi operačního systému nebo jiným softwarem?				
O5		Neovlivňují funkce operačních systémů přístupné přes otevřená rozhraní nepřípustně legálně relevantní software, legálně relevantní parametry nebo údaje z měření?				
O6		Lze identifikovat operační systém a konfiguraci operačního systému? Jsou identifikace operačního systému a identifikace konfigurace operačního systému zobrazovány na příkaz nebo během provozu?				
O7		Je operační systém chráněn proti úmyslným změnám?				
**V případě odchylky proti požadavkům na software je nutné uvést vysvětlení.*						

12.4.4 Kontrolní seznam pro specifické požadavky rozšíření L

Kontrolní seznam požadavků rozšíření L						
Požadavek	**Postupy zkoušení**		**Vyhověl**	**Nevyhověl**	**Nerelevantní**	**Poznámky***
L1		Jsou naměřená data doplněna všemi důležitými informacemi potřebnými pro legálně relevantní účely?				
L2		Jsou uložená data zabezpečena proti náhodným či neúmyslným změnám?				
L3		Jsou uložená naměřená data chráněna proti záměrným změnám?				
L4		Je možné dohledat měření a měřicí přístroj, při němž konkrétní uložená naměřená data vznikla?				
L5		Je s klíči a s nimi souvisejícími informacemi nakládáno jako s naměřenými daty a jsou uchovávány v utajení a chráněny proti zneužití?				

L6		Je přístroj vybaven legálně relevantním modulem nebo komponentou pro čtení, verifikaci a zobrazení uložených naměřených dat?				
L7		Jsou naměřená data uložena automaticky po ukončení měření?				
L8		Je kapacita paměti na dlouhodobé uložení dat pro zamýšlený účel dostatečná?				
**V případě odchylky proti požadavkům na software je nutné uvést vysvětlení.*						

12.4.5 Kontrolní seznam pro specifické požadavky rozšíření T

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

12.4.6 Kontrolní seznam pro specifické požadavky rozšíření S

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

12.4.7 Kontrolní seznam pro specifické požadavky rozšíření D

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

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

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

13.1 Požadavky na software, odkaz na směrnici MID

Požadavek		MID	
Č.	**Označení**	**Článek / Příloha č.** (AI = Příloha 1)	**Označení**
	Základní příručka P		
P1	Dokumentace výrobce	AI-9.3 AI-12 Článek 18	Informace o přístroji, které přístroj provázejí Hodnocení shody Technická dokumentace
P2	Označení softwaru	AI-7.6 AI-8.3	Vhodnost Ochrana před zneužitím
P3	Příkazy zadané přes uživatelské rozhraní	AI-7.1	Vhodnost
P4	Příkazy zadané přes komunikační rozhraní	AI-7.1 AI-8.1	Vhodnost Ochrana před zneužitím
P5	Zabezpečení a ochrana legálně relevantního softwaru a specifických parametrů zařízen	AI-7.1, AI-7.2 AI-8.4	Vhodnost Ochrana před zneužitím
P6	Ochrana softwaru a naměřených dat	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Vhodnost[17] Ochrana před zneužitím
P7	Ochrana parametrů	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Vhodnost Ochrana před zneužitím

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

Požadavek		MID	
Č.	**Označení**	**Článek / Příloha č.** (AI = Příloha 1)	**Označení**
P8	Zobrazovaná naměřená data	AI-7.1, AI-7.2, AI-7.6 AI-8.3, AI-10.2, AI-10.3, AI-10.4	Vhodnost Ochrana před zneužitím Indikace výsledku
	Základní příručka U		
U1	Dokumentace výrobce	AI-9.3 AI-12 Článek 18	Informace o přístroji, které přístroj provázejí Hodnocení shody Technická dokumentace
U2	Označení softwaru	AI-7.6 AI-8.3	Vhodnost Ochrana před zneužitím
U3	Příkazy zadané přes uživatelská rozhraní	AI-7.1	Vhodnost
U4	Příkazy zadané přes komunikační rozhraní	AI-7.1 AI-8.1	Vhodnost Ochrana před zneužitím
U5	Zabezpečení a ochrana legálně relevantního softwaru a specifických parametrů zařízení	AI-7.1, AI-7.2 AI-8.4	Vhodnost Ochrana před zneužitím
U6	Ochrana softwaru a naměřených dat	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Vhodnost Ochrana před zneužitím
U7	Ochrana parametrů	AI-7.1 AI-8.2, AI-8.3, AI-8.4	Vhodnost Ochrana před zneužitím
U8	Zobrazovaná naměřená data	AI-7.1, AI-7.2, AI-7.6 AI-8.3 AI-10.2, AI-10.3, AI-10.4	Vhodnost Ochrana před zneužitím Označení výsledku
	Rozšíření O		
	Rozšíření L		
L1	Úplnost uložených dat	AI-7.1 AI-8.4 AI-10.2	Vhodnost Ochrana proti zneužití Označení výsledku
L2	Ochrana proti náhodným či neúmyslným změnám	AI-7.1, AI-7.2 AI-8.4	Vhodnost Ochrana proti zneužití
L3	Integrita dat	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
L4	Autentičnost uložených dat	AI-7.1 AI-8.4 AI-10.2	Vhodnost Ochrana proti zneužití Označení výsledku
L5	Utajení klíčů	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
L6	Načtení uložených dat	AI-7.2 AI-10.1, AI-10.2, AI-10.3, AI-10.4	Vhodnost Označení výsledku
L7	Automatické uložení	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
L8	Kapacita paměti a kontinuita	AI-7.1	Vhodnost
Lx	Celý obsah rozšíření L	AI-11.1	Další zpracovávání dat k uzavření obchodní transakce
	Rozšíření T		
T1	Úplnost přenášených dat	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
T2	Ochrana proti náhodným změnám	AI-7.1, AI-7.2 AI-8.4	Vhodnost Ochrana proti zneužití
T3	Integrita dat	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití

Požadavek		MID	
Č.	**Označení**	**Článek / Příloha č.** (AI = Příloha 1)	**Označení**
T4	Autentičnost přenášených dat	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
T5	Utajení klíčů	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
T6	Zacházení s poškozenými daty	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
T7	Zpoždění při přenosu	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
T8	Dostupnost přenosových služeb	AI-7.1 AI-8.4	Vhodnost Ochrana proti zneužití
	Rozšíření S		
S1	Realizace oddělení software	AI-7.6, AI-10.1	Vhodnost Označení výsledku
S2	Smíšená indikace	AI-7.1, AI-7.2, AI-7.6 AI-10.2	Vhodnost Označení výsledku
S3	Ochranné rozhraní softwaru	AI-7.6	Vhodnost
	Rozšíření D		
D1	Mechanismus stahování	AI-8.2, AI-8.4	Ochrana proti zneužití
D2	Prokázání věrohodnosti přeneseného softwaru	AI-7.6 AI-8.3, AI-8.4 AI-12	Vhodnost Ochrana proti zneužití Hodnocení shody
D3	Integrita stahovaného softwaru	AI-7.1, AI-8.4	Vhodnost Ochrana proti zneužití
D4	Návaznost stahovaného legálně relevantního softwaru	AI-7.1, AI-7.6 AI-8.2, AI-8.3 AI-12	Vhodnost Ochrana proti zneužití Hodnocení shody
	Rozšíření I (Požadavky na software přístrojů konkrétního typu)		
I1-1, I2-1, I3-1, I4-1, I5-1	Obnova po chybě	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Spolehlivost Specifické požadavky na přístroje na měření spotřeby
I1-4, I2-3, I3-4, I4-4, I5-4	Prostředky zálohování	AI-6 MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Spolehlivost Specifické požadavky na přístroje na měření spotřeby
I1-9, I2-9, I3-9, I4-9	Vnitřní rozlišení, vhodnost označení	MI-002-5.3, MI-003-5.2	Specifické požadavky na přístroje na měření spotřeby
I1-6, I2-6, I3-6, I4-6,	Zamezení vynulování naměřených kumulativních dat	AI-8.5	Ochrana proti zneužití
I1-2, I2-2, I3-2, I4-2, I5-2	Dynamické chování	AI-7.6	Vhodnost Ochrana proti zneužití
I2-10	Životnost zdroje napájení	MI-002-5.2	Specifické požadavky na přístroje na měření spotřeby

Požadavek		MID	
Č.	**Označení**	**Článek / Příloha č.** (AI = Příloha 1)	**Označení**
I2-12	Elektronické přepočítávače objemu	MI-002-9.1	Specifické požadavky na přístroje na měření spotřeby
I2-11	Testovací prvek	MI-002-5.5	Specifické požadavky na přístroje na měření spotřeby
I6-1	Detekce chyb	MI-006-IV, MI-006-V	Diskontinuální a kontinuální součtové váhy
I6-2	Prostředky zálohování, detekce chyb	MI-006-IV, MI-006-V	Diskontinuální a kontinuální součtové váhy

13.2 Interpretace článků a příloh směrnice MID s požadavky této příručky

MID			Softwarová příručka
Článek / Příloha č. (AI = Příloha 1)	**Označení**	**Komentář**	**Požadavek č.**
	Část článku		
1, 2, 3		Bez zvláštní souvislosti se softwarem	
4(b)	Definice, uspořádání podsestav	Přenos naměřených dat... Základní pravidla pro podsestavy	T P, U
5 to 9		Bez zvláštní souvislosti se softwarem	
10	Technická dokumentace	Dokumentace týkající se návrhu, výroby a provozu. Umožnění hodnocení shody. Obecný popis přístroje. Popis elektronických zařízení s výkresy, logickými schématy, obecnými informacemi o softwaru. Umístění plomb a značek. Podmínky kompatibility s rozhraními a podsestavami.	P1, U1
11 to 27		Bez zvláštní souvislosti se softwarem	
	Příloha 1		
AI-1 to AI-5		Bez zvláštní souvislosti se softwarem	
AI-6	Spolehlivost	Detekce chyb, zálohování, obnovení, restart	I1-1, I1-2, I2-1, I2-2, I3-1, I3-2, I4-1, I4-2, I6-1, I6-2
AI-7	Vhodnost	Žádné prostředky usnadňující podvodné použití; minimální možnosti nezáměrného zneužití.	P3 – P8, U3 - U8, L1 – L5, L7, L8, T1 – T8, S2, D3, D4, I1-4, I2-8, I3-5, I4-4
AI-8	Ochrana proti zneužití		
AI-8.1		Žádné vlivy v důsledku připojení jiných zařízení.	P4, U4
AI-8.2		Zabezpečení, důkazy intervence	P6, P7, U6, U7, D1, D4

MID			Softwarová příručka
Článek / Příloha č. (AI = Příloha 1)	**Označení**	**Komentář**	**Požadavek č.**
AI-8.3		Označení softwaru, důkazy intervence	P2, P6, P7, P8 U2, U6, U7, U8, D2, D4
AI-8.4		Ochrana uložených nebo přenášených dat	P5 - P7, U5 - U7, L1 - L5, T1 - T8 D1 - D3
AI-8.5		Nevynulování kumulativních záznamníků	I1-3, I2-4, I3-4, I4-3
AI-9	Informace o přístroji, které přístroj provázejí		
AI-9.1		Kapacita měření (zbývající položky nerelevantní z hlediska softwaru)	L8
AI-9.2		Bez zvláštní souvislosti se softwarem	
AI-9.3		Návod na instalaci, ..., podmínky kompatibility s rozhraním, podsestavami nebo měřicími přístroji.	P1, U1
AI-9.4 to AI-9.8		Bez zvláštní souvislosti se softwarem	
AI-10	Indikace výsledku		
AI-10.1		Označení na displeji nebo na výtisku.	P8, U8, L6, S2
AI-10.2		Význam výsledku, nezaměnitelnost s dalšími označeními.	P8, U8, L1, L4, L6, S2
AI-10.3		Tištěný výstup nebo záznam snadno čitelný a nesmazatelný.	P8, U8, L6, S2
AI-10.4		Pro přímé prodeje: prezentace výsledku oběma stranám.	P8, U8, S2
AI-10.5		Pro měřiče spotřeby: zobrazení pro zákazníka	I1-3, I2-3, I3-3/4, I4-3
AI-11	Další zpracování dat za účelem ukončení obchodní transakce		
AI-11.1		Zaznamenání naměřených výsledků trvalými prostředky.	L1 - L8
AI-11.2		Trvanlivý důkaz naměřených výsledků a informací za účelem identifikace transakce.	L1, L6
AI-12	Hodnocení shody	Okamžité hodnocení shody s požadavky směrnice.	P1, P2, U1, U2, D2, D4
	Přílohy A1 až H1		
A1 až H1		Žádné požadavky na vlastnosti přístrojů	
	Příloha MI-001		
MI-001-1 až MI-001-6		Bez zvláštní souvislosti se softwarem	
MI-001-7.1.1, MI-001-7.1.2	Ochrana před elektromagnetickým rušením	Detekce chyb Prostředky zálohování Prostředky buzení z režimu spánku a obnovy	I1-1, I1-2
MI-001-7.1.3 až MI-001-9		Bez zvláštní souvislosti se softwarem	

MID			Softwarová příručka
Článek / Příloha č. (AI = Příloha 1)	**Označení**	**Komentář**	**Požadavek č.**
	Příloha MI-002		
MI-002-1 až MI-002-2		Bez zvláštní souvislosti se softwarem	
MI-002-3.1	Ochrana před elektromagnetickým rušením	Detekce chyb Prostředky zálohování Prostředky buzení z režimu spánku a obnovy	I2-1, I2-2
MI-002-3.1.3 až MI-002-5.1		Bez zvláštní souvislosti se softwarem	
MI-002-5.2	Vhodnost	Přijatelné řešení sledování životnosti zdroje napájení	I2-5
MI-002-5.3	Vhodnost	Vnitřní rozlišení	I2-3
MI-002-5.4 až MI-002-8		Bez zvláštní souvislosti se softwarem	
MI-002-5.5	Vhodnost	Testovací prvek	I2-7
MI-002-5.6 až MI-002-8		Bez zvláštní souvislosti se softwarem	
MI-002-9.1	Přepočítávače objemu Vhodnost	Přijatelné řešení sledování přepočítávače objemu plynu	I2-6
MI-002-9.2 až MI-002-10		Bez zvláštní souvislosti se softwarem	
	Příloha MI-003		
MI-003-1 až MI-003-4.2		Bez zvláštní souvislosti se softwarem	
MI-003-4.3	Povolené působení přechodných elektromagnetických jevů	Detekce chyb Prostředky zálohování Prostředky buzení z režimu spánku a obnovy	I3-1, I3-2
MI-003-5.1		Bez zvláštní souvislosti se softwarem	
MI-003-5.2	Vhodnost	Vnitřní rozlišení	I3-3
MI-003-5.3 až MI-003-7		Bez zvláštní souvislosti se softwarem	
	Příloha MI-004		
MI-004-1 až MI-004-4.1		Bez zvláštní souvislosti se softwarem	
MI-004-4.2	Povolený vliv elektromagnetického rušení	Detekce chyb Prostředky zálohování Prostředky buzení z režimu spánku a obnovy	I4-1, I4-2
MI-004-4.3 až MI-004-7		Bez zvláštní souvislosti se softwarem	
	Příloha MI-005		
	Příloha MI-006		

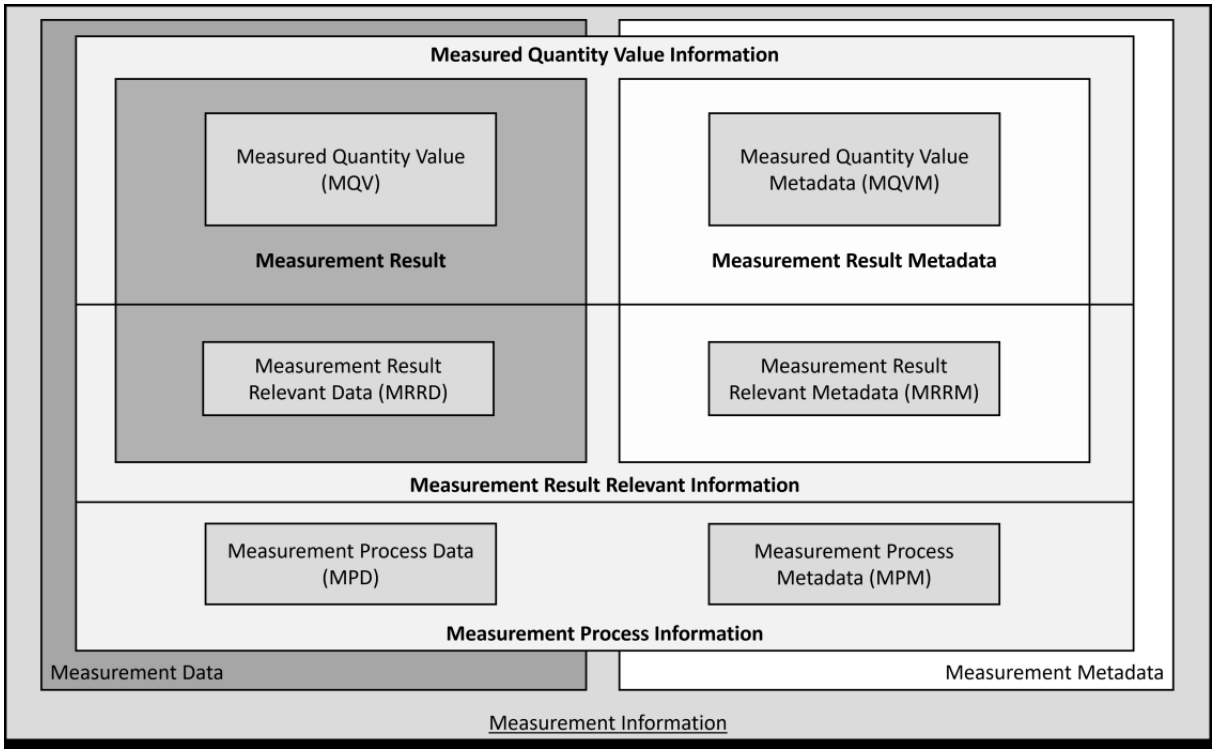
MID			Softwarová příručka
Článek / Příloha č. (AI = Příloha 1)	**Označení**	**Komentář**	**Požadavek č.**
MI-006-IV, MI-006-V	Diskontinuální a kontinuální součtové váhy	Detekce chyb Prostředky zálohování	I6-1, I6-2
	Příloha MI-007		
MI-007-8	Povolený vliv elektromagnetického rušení	Prostředky zálohování	I7-1
	Příloha MI-008		
	Příloha MI-009		
	Příloha MI-010		

14 Poznámky k terminologii měření

Poznámka: Tato informativní příloha má ilustrovat termíny a definice týkající se procesu měření a jejich použití v tomto dokumentu OIML.

V tomto dokumentu je definice výsledku měření "soubor hodnot veličin, které jsou přiřazeny měřené veličině spolu s dalšími relevantními údaji" (tj. relevantní údaje o výsledku měření). To je znázorněno na obrázku A.1 jako hodnota měřeného množství (MQV) a relevantní údaje o výsledku měření (MRRD), které jsou součástí výsledku měření.

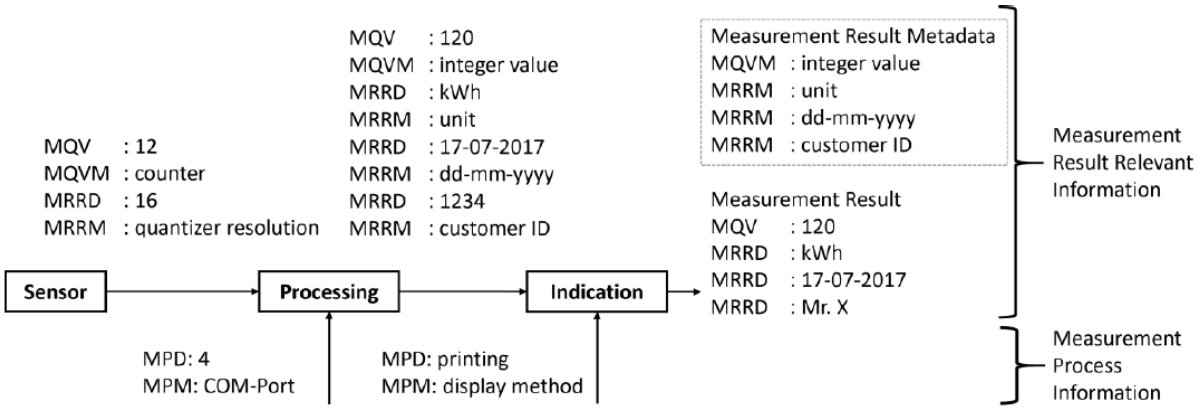
Spolu s údaji o procesu měření (MPD) tvoří údaje o měření.



Obrázek A.1 - Vizuální znázornění informací o měření

Tento dokument OIML obecně rozlišuje mezi daty měření a metadaty měření. Jsou-li obě použita společně, jsou data měření uvedena do kontextu; proto se data měření plus metadata měření rovnají informacím o měření.
Tento dokument OIML také rozlišuje mezi informacemi o výsledku měření a informacemi o procesu měření.

Obrázek A.2 obsahuje blokové schéma, které ilustruje rozdíl mezi daty relevantními pro výsledek měření nebo daty relevantními pro proces měření.



Obr. A.2 – Vývojový diagram procesu měření s příklady pro různá data související s výsledkem měření nebo relevantní pro proces měření.

Na obrázku A.2. jsou rovněž uvedeny údaje, z nichž se skládá výsledek měření:

Hodnota měřeného množství (MQV) a relevantní data výsledku měření (MRRD), zatímco odpovídající metadata výsledku měření potřebná pro správnou interpretaci výsledku jsou znázorněna v orámovaném čárkovaném obdélníku.
Obrázek A.2 ukazuje jednoduchý příklad procesu měření. Pro každý logický krok (od získání dat snímačem po indikaci výsledku) jsou zaznamenány následující části:

- hodnota měřeného množství (MQV) a metadata o hodnotě měřeného množství (MQVM);
- relevantní data výsledku měření (MRRD) a relevantní metadata výsledku měření (MRRM);
- data procesu měření (MPD) a metadata procesu měření (MPM).

Jedna část informací o měření se týká relevantních informací o výsledcích měření.
Při sběru dat snímačem se získá nezpracovaná hodnota čítače 12 (MQV) s "čítačem" jako metadaty o hodnotě měřeného množství (MQVM), která jsou potřebná k interpretaci dat.
Relevantní informace o výsledku měření (MRRI) je 16bitové rozlišení kvantifikátoru ADC,

- kde 16 je relevantní údaj o výsledku měření (MRRD),
- zatímco "rozlišení kvantizeru" jsou metadata relevantní pro výsledek měření (MRRM), která jsou potřebná k interpretaci dat.

Během zpracování je naměřené hodnotě množství (MQV) s "celočíselnou hodnotou" jako metadatům naměřené hodnoty množství (MQVM) přiřazena "kWh" jako relevantní údaj o výsledku měření (MRRD) s "jednotkou" jako relevantní metadata o výsledku měření (MRRM), dále časové razítko "17-07-2017" (MRRD) s formátem "den-měsíc-rok" (MRRM) a Mister X (MRRD) jako ID zákazníka (MRRM).
V obou případech tvoří během snímání čidlem a zpracování naměřená hodnota množství (MQV) a relevantní údaje o výsledku měření (MRRD) součást výsledku měření, zatímco metadata jsou potřebná pro správnou interpretaci výsledku měření.

S procesem měření souvisí další část informací o měření: pro získání naměřené hodnoty množství (MQV) ze snímače se používá COM-Port číslo 4, kde se nachází

- "4" jsou údaje o procesu měření (MPD) a
- "COM-Port" jsou metadata procesu měření (MPM) potřebná k pochopení datového prvku.

Výsledek lze zobrazit na displeji nebo vytisknout.
"Tisk" dat procesu měření (MPD) s odpovídajícím "způsobem zobrazení" metadat procesu měření (MPM) jsou pro proces měření nezbytné, ale nestanou se součástí výsledku měření ani metadat výsledku měření.
Je na technických pracovních skupinách, aby rozhodly, co jsou relevantní data výsledku měření, protože za určitých okolností se data procesu měření (MPD) mohou stát relevantními daty výsledku měření (MRRD).
V uvedeném příkladu, který je znázorněn na obrázku A.2, spojuje COM-Port číslo 4 hodnotu měřeného množství (MQV) se zákazníkem panem X, čímž se data procesu měření (MPD) v průběhu kroku zpracování mění na data relevantní pro výsledek měření (MRRD).

15 Legálně relevantní vlastnosti

Legálně relevantní měřicí přístroj může mít legálně relevantní software a za určitých podmínek legálně nerelevantní software, Totéž platí pro parametry, údaje, nápisy a indikace, které mohou být buď legálně relevantní a za určitých podmínek legálně nerelevantní.
Na základě výše uvedené definice lze určit, zda jsou software, parametry, údaje, nápisy a indikace legálně relevantní s ohledem na MID a NAWID. Dále je uvedeno několik příkladů s ohledem na použití definice.

- Značení a nápisy, které musí splňovat základní požadavky, jsou podle definice legálně relevantní.
- Zabezpečovací a ochranné prvky, které se používají k zabezpečení měřicího přístroje, softwaru, parametrů, měřených údajů, nápisů a označení, musí splňovat základní požadavky, a jsou proto legálně relevantní.
- Data, ať už uložená, přenášená a/nebo indikovaná, používaná k sestavení výsledku měření musí splňovat základní požadavky, a jsou proto legálně relevantní.

  Poznámka: Legálně relevantní údaje se nazývají údaje o měření.

- Pokud je k sestavení, uložení a/nebo přenosu dat měření a/nebo indikaci výsledku měření použita součást, pak tato součást může ovlivnit výsledek měření, a má tedy vliv na splnění požadavků, a je tedy legálně relevantní.

  - Komponenty pro konstrukci naměřených dat zahrnují například snímač, jednotku pro zpracování analogových dat a jednotku pro zpracování digitálních dat;
  - Komponenty pro ukládání nebo přenos naměřených dat zahrnují například pevný disk a kartu síťového rozhraní;
  - komponenty pro indikaci výsledků měření, včetně displeje a tiskárny.

Pokud se modul používá ke konstrukci, ukládání a/nebo přenosu dat měření a/nebo k indikaci výsledku měření, pak může mít tento modul vliv na výsledek měření, a tedy vliv na soulad s požadavky, a je tedy legálně relevantní.

16 Odkazy a literatura

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

[2] DIRECTIVE 2014/32/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (recast), Official Journal of the European Union L 96/149, 29. 3. 2014

[3] Directive 2004/22/EC of the European Parliament and of the Council of 31 March 2004 on measuring instruments. Official Journal of the European Union L 135/1, 30. 4. 2004

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

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

17 Přehled revizí

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

5	květen 2011	Revize kapitoly 5 (část U): Pokrok v oblasti operačních systémů Náhrada termínu „komponenta“ jinými vhodnými termíny v celé příručce, aby nedošlo k chybnému pochopení Doplnění požadavku D1 v oddílu 9.2 zavedením zaplombovatelného mechanismu stahování Propracování části „upřesnění“ u požadavků P2 a U2 v oddílech 4.2 a 5.2 v souvislosti s označováním softwaru Rozšíření příkladů přijatelných řešení v požadavku L2 (oddíl 6.2) a v požadavku U8 (oddíl 5.2)
6	březen 2015	Rozsáhlá revize - Ráz příručky: Příručka je považována za čistě technický dokument interpretující základní požadavky související se softwarem. Výroky, které nejsou v souladu s tímto principem, byly odstraněny. - Adresáti příručky: Tato příručka je určena vývojářům a zkoušejícím softwaru, ale mohou ji využít i jiné strany, především orgány dohledu nad trhem, kdykoliv a kdekoliv to bude vhodné. - Zavedení posledních dvou aktualizací se ukázalo být náročné z hlediska detailní redakční práce. Změny provedené v rámci této revize proto mají za cíl lepší čitelnost příručky, nemění však uvedené technické specifikace. - Označení softwaru (P2/U2): Ve verzi 7.2 příručky již není požadováno, aby samotný software poskytoval i označení softwaru. Stačí, aby označení softwaru dokázal bezpečným způsobem sdělit přístroj. - Rozlišení označení a integrity (P2/U2, P6/U6): Příloha 1 směrnice MID rozlišuje mezi označením softwaru (příloha 1, článek 7.6) a integritou, tj. ochranou softwaru (příloha 1, článek 8.4). Toto rozlišení neoslabuje platnost požadavků. - Podpora kontrol shody s typem: Technické prostředky potřebné k zajištění integrity softwaru jsou považovány rovněž za vhodné při kontrole shody s typem. Požadované prostředky zahrnují např. kontrolní součty nebo ekvivalentní prostředky na různých úrovních u všech přístrojů náležejících do třídy rizika C a vyšší. - Třídy rizika: Třída rizika C byla změněna, a veškerý legálně relevantní software přístrojů náležejících do třídy rizika C je proto nyní považován za fixní (neměnný). Tím pádem odpadají nejasnosti ohledně toho, jaká část softwaru je považována za fixní. V třídě rizika C a vyšší musí být implementováno označení softwaru na úrovni bitů (např. kontrolními součty). - Klasifikace přístrojů využívajících univerzální počítač (přístroje typu U) dle třídy rizika: Přístroje využívající univerzální počítač jsou v zásadě spojeny s vyšším

		rizikem, a proto je zařazení těchto přístrojů do třídy B považováno za neodpovídající. Přístroje typu U lze tedy zařadit jedině do třídy rizika C či vyšší. - Přijatelná bezpečnostní opatření pro třídy vysokého rizika (D a vyšší): Požadavky na algoritmy a minimální délku klíče se řídí doporučeními vydanými národními a mezinárodními institucemi pro bezpečnost dat (např. NIST (USA), DCSSI (Francie), CESG (Velká Británie), CCN (Španělsko), NCSC (Nizozemí), BSI (Německo)). - Legálně relevantní software: již není vnímána nutnost rozlišovat legálně relevantní software od fixního legálně relevantního softwaru. Všechny požadavky na zabezpečení uvedené v Příloze 1 se vztahují na legálně relevantní software.
7	březen 2018	Rozšíření P7 o přijatelné řešení, které zajišťuje, že obsah záznamníku událostí je zobrazen na displeji měřidla. Rozšíření U8 a doplnění odpovídajícího požadavku P8 popisující spárování a proces „handshake“ („potřesení rukou“) mezi jednotkami ve všeobecnějším smyslu. Zlepšení srozumitelnosti rozšíření S odstraněním definice pro oddělení softwaru na nízké a vysoké úrovni.
8	duben 2019	Editorské změny týkající se porovnávání překladů a vedení překladů, vyjasnění použití rozšíření T, opravy v P6, U6, T2, T6 a L2. Reorganizace mezi "Přijatelnými řešeními" a "Upřesňujícími poznámkami" u každého požadavku. Dvě specifické přílohy pro měřidla 10.2 Plynoměry a přístroje pro přeměnu objemu a 10.3 Měřiče činné elektrické energie byly zcela přepracovány. Byla upravena kapitola 11.1 "Informace, které mají být uvedeny v certifikátu o přezkoušení typu".
9	říjen 2020	Revize příloh 10.1 Vodoměry, 10.4 Měřiče tepelné energie, 10.5 Měřicí systémy pro kontinuální a dynamické měření množství kapalin jiných než voda a 10.7 Taxametry.
10	červenec 2021	Provedení změn terminologické podskupiny, které byly předem předloženy na zasedání pracovní skupiny WG 7 v roce 2021. - Přeformulované pokyny k validaci pro rizikové třídy E ("vhodné" -> "správné"), jak byly předloženy na zasedání pracovní skupiny WG 7 v roce 2019.

11	březen 2022	Přidání "Rozšíření O", které podrobně popisuje nové požadavky na měřicí přístroje s operačními systémy. Následně byla celá příručka aktualizována tak, aby obsahovala nové rozšíření. Více požadavků v celém dokumentu bylo upřesněno, aby se zvýšila jejich srozumitelnost a aby byly méně nejednoznačné. Technické specifikace zůstávají stejné. Byla aktualizována šablona zkušebního protokolu.
12	březen 2023	Implementace terminologie OIML D31. V důsledku toho byly všechny požadavky přepracovány tak, aby odpovídaly nové terminologii. V úvodních textech byla provedena další upřesnění týkající se přidání rozšíření O. Rovněž byl doplněn kontrolní seznam pro rozšíření O.

Tabulka 17-1: Přehled revizí