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

WELMEC Guide 7.4

Příklady aplikací
příručky WELMEC Guide 7.2

(Směrnice o měřicích zařízeních 2014/32/EU)

Verze 2022

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

Obsah

Předmluva

Předkládaná příručka vychází z příručky WELMEC Guide 7.2 Software [1].

Tato příručka odráží současný postoj pracovní skupiny WELMEC WG 7 Software. Příručka WELMEC Guide 7.2 odráží strukturu MID, je třeba vzít v úvahu také specifické požadavky na přístroje. V tomto ohledu mohou jiné pracovní skupiny WELMEC stanovit další formální nebo technické požadavky na jednotlivé třídy přístrojů.

Příručka má čistě poradní charakter a sám o sobě neukládá žádná omezení ani další technické požadavky nad rámec těch, které jsou obsaženy v MID. Alternativní přístupy mohou být přijatelné, ale pokyny uvedené v tomto dokumentu představují názor WELMEC na správnou praxi, kterou je třeba dodržovat.

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: Tato příručka platí pro směrnice 2004/22/ES a 2014/32/EU [2, 3].

Úvod

Tento dokument poskytuje technické pokyny pro uplatňování směrnice o měřicích přístrojích (MID).

Zaměřuje se zejména na softwarově vybavené měřicí přístroje a je proto použitelný pro širokou škálu měřicích přístrojů.

Předkládaná příručka je určena k použití v kombinaci s příručkou WELMEC Guide 7.2. Poskytuje příkladná přijatelná řešení pro konkrétní architektury přístrojů (viz příručka WELMEC Guide 7.3 [4]) a uvádí, jak tato přijatelná řešení splňují požadavky stanovené v příručce WELMEC Guide 7.2. Tím také objasňuje požadavky stanovené v příručce WELMEC Guide 7.2 na technické úrovni.

Tato příručka se zabývá pouze přijatelnými řešeními na technické úrovni, nikoli na architektonické úrovni (viz příručka WELMEC 7.3).

Míra podrobností je zaměřena na potřeby výrobců měřidel a oznámených subjektů, které provádějí posuzování shody měřidel podle modulu B.

Dodržováním této příručky lze předpokládat soulad s požadavky MID týkajícími se softwaru. Lze dále předpokládat, že všechny oznámené subjekty přijímají tuto příručku jako kompatibilní interpretaci MID s ohledem na software. Pro objasnění, jak požadavky stanovené v této příručce souvisejí s příslušnými požadavky v MID, podívejte se na křížový odkaz v příručce WELMEC Guide 7.2 [1].

Nejnovější informace týkající se příruček a činností pracovní skupiny WELMEC 7 jsou k dispozici na internetových stránkách www.welmec.org.

1 Terminologie

Termíny použité v této příručce naleznete v terminologické části příručky WELMEC Guide 7.2 [1]. Definice všech ostatních termínů jsou uvedeny níže.

Základní jednotka *(Mother Unit)*: Přístroj nebo část přístroje, která splňuje příslušné požadavky na software. Jedna nebo více funkcí popsaných v příručce WELMEC Guide 7.2 jsou však přesunuty do samostatné komponenty. Samostatná komponenta a základní jednotka společně splňují všechny požadavky příručky WELMEC Guide 7.2.

2 Jak používat tuto příručku

Příručka popisuje konkrétní konfigurace měřicích přístrojů, jakož i hardwarové komponenty a softwarové moduly, ze kterých se přístroje skládají. Každá konkrétní konfigurace, zmíněná také jako "přijatelné řešení", je popsána samostatně. Příručka rovněž obsahuje popisy souvisejících požadavků platných pro konkrétní konfiguraci.

2.1 Celková struktura příručky

Příručka má následující strukturu. Nejprve stručně rozebírá modulární koncepci příručky WELMEC Guide 7.2 v kapitole 3 a zabývá se funkčností vybraných modulů této koncepce. Kapitola 4 se zabývá specifickými technickými realizacemi. Pro každou z nich je odvozen seznam příslušných požadavků. Následně je ukázáno, jak pro popsanou realizací jsou splněny příslušné požadavky. V kapitole 5 jsou uvedeny odkazy a literatura.

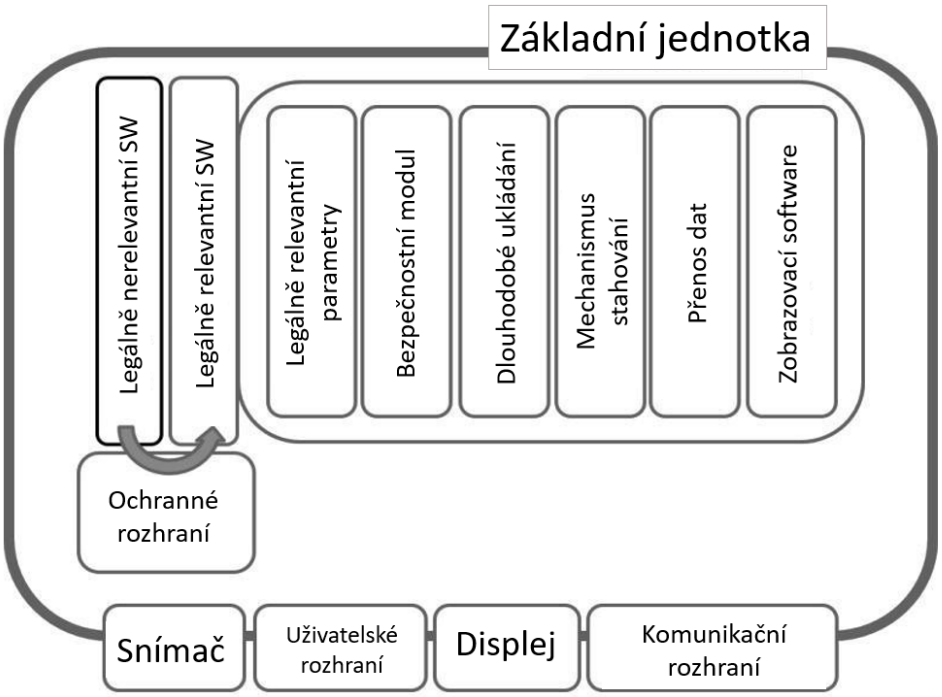
2.2 Jak vybrat příslušné části průvodce

Při přezkoumání nebo vývoji specifické konfigurace měřicího přístroje se oznámeným subjektům i výrobcům doporučuje nahlédnout do kapitoly 4, kde jsou uvedeny použitelné příklady. V příručce nelze uvést všechny možné konfigurace přístroje. Čtenáři by si proto měli vybrat konkrétní implementační detaily z různých příkladů podle svých potřeb.
Vzhledem k tomu, že všechny zde uvedené příklady jsou zaměřeny na přístroje typu U rizikové třídy C (není-li uvedeno jinak), ve srovnání s definicemi v [1], by většina aspektů přijatelných řešení měla být zaměnitelná nebo kombinovatelná.

3 Obecná architektura měřicího přístroje

3.1 Odvozená obecná architektura měřicího přístroje

Pomocí obecných modulů a specifických pojmů definovaných v příručce WELMEC Guide 7.2 [1] lze vytvořit propracovanou modulární strukturu, která je podobná obecné architektuře měřicího přístroje (viz obrázek 3-1).



Obrázek 3-1: Obecná architektura podobná propracované modulární architektuře dle příručky WELMEC Guide 7.2 "Software".

Upozornění: Bezpečnostní modul integruje všechna legálně relevantní bezpečnostní opatření, např. pro integritu, autenticitu, výpočet kontrolního součtu, správu klíčů a certifikátů, softwarové identifikátory, evidence záznamů/souborů atd.

Podrobný popis obecné architektury je uveden v příručce WELMEC Guide 7.3 „Referenční architektury na základě příručky WELMEC Guide 7.2“ [4].

Tato obecná architektura je zde použita k určení příkladných konfigurací měřicích přístrojů, pro které jsou uvedena přijatelná řešení. Dodržováním obecné architektury je zajištěno, že prezentované příkladné aplikace si navzájem neodporují a poskytují jednotnou úroveň podrobnosti.

4 Příklady aplikací

Požadavek U1 je vždy splněn kompletní dokumentací. Požadavek U1 neukládá měřicímu přístroji žádná další technická omezení, a proto není v níže uvedených příkladech uveden.

4.1 Externí úložná jednotka připojená k "Základní jednotce"

4.1.1 Předpoklady týkající se "Základní jednotky"

- "Základní jednotka" bez externí úložné jednotky musí splňovat požadavky U1 až U9 příručky WELMEC 7.2 Guide, 2018.
- Přepojení mezi "základní jednotkou" a externí úložnou jednotkou je fyzicky zaplombováno.
- "Základní jednotka" a úložná jednotka musí společně splňovat požadavky L1 až L8. "Základní jednotka" musí splňovat požadavky L1, L3, L5, L6 a L7.

4.1.2 Příslušné požadavky na externí úložnou jednotku

- "Základní jednotka" a úložná jednotka musí společně splňovat požadavky L1 až L8. Úložná jednotka musí splňovat požadavky L2, L3, L4, L5 a L8.
- Pokud je na úložné jednotce k dispozici legálně relevantní software pro zobrazení nebo tisk uložených dat měření, musí rovněž splňovat požadavek L6.
- Pokud má externí úložná jednotka vlastní legálně relevantní software, musí splňovat požadavky U2, U4, U5, U6, U7, U8 a U9 v kombinaci se "základní jednotkou". (U2: Požadavek se vztahuje na identifikaci softwaru externí úložné jednotky i na identifikaci softwaru "základní jednotky").
- Pokud má externí úložná jednotka uživatelské rozhraní (např. vypínač), musí splňovat požadavek U3 v kombinaci se "základní jednotkou".
- V případě, že má externí úložna jednotka vlastní legálně relevantní software, je třeba zkontrolovat rozšíření D a S, pokud jsou použité.

4.1.3 Popis přijatelného řešení

Následující přijatelné řešení je konkrétně zaměřeno na přístroje typu U rizikové třídy C. Pro jinou základní konfiguraci nebo jinou rizikovou třídu je třeba přijatelné řešení odpovídajícím způsobem upravit.

Měřicí přístroj pro měření více rozměrů se skládá ze dvou laserových snímačů, které snímají dvourozměrný profil předmětů přepravovaných na dopravním pásu. Rychlost pásu měří třetí snímač. Snímače jsou fyzicky uzavřeny a připojeny k centrální procesorové jednotce kabelem, který pro datovou komunikaci používá sériový protokol. Všechna kabelové připojení jsou rovněž fyzicky chráněna proti neoprávněné manipulaci. Procesorová jednotka je vybavena hodinami reálného času (RTC) a vestavěným displejem, na kterém se zobrazuje vypočítané množství měřených

objektů. Každému novému objektu je procesorovou jednotkou přiřazen jedinečný identifikátor a časové razítko. Jakmile se na displeji zobrazí naměřená hodnota (délka, šířka, výška nejmenší krychle odpovídající měřenému objektu) spolu s jedinečným identifikátorem a časovým razítkem, vypočítá se CRC32 s tajným počátečním vektorem a připojí se k souboru naměřených dat.
Pro dlouhodobé ukládání je k procesorové jednotce připojena externí úložná jednotka, která obsahuje legálně relevantní software, a to prostřednictvím sériového komunikačního připojení. Když jsou obě součásti uvedeny do provozu, připojení je zaplombováno,. Úložná jednotka přijímá od procesorové jednotky sady naměřených dat a potvrzuje každou přijatou sadu dat. Úložná jednotka poskytuje procesorové jednotce zpětnou vazbu pro každou uloženou datovou sadu, která informuje, zda uložení proběhlo úspěšně, nebo zda došlo k chybě (selhání, zaplnění paměti, poškození paměti atd.). Procesorová jednotka je rovněž schopna poskytnout uživateli uložené výsledky měření. Sady dat je možné vyhledávat zadáním časového razítka nebo pomoci jedinečného identifikátoru prostřednictvím klávesnice. Prostřednictvím sériového protokolu může načíst úložná jednotka na vyžádání výsledek měření, který je specifikovaný jednoznačným identifikátorem a odeslat ho do procesorové jednotky.

Procesorová jednotka poté zkontroluje integritu datové sady a zobrazí výsledek uživateli. Pokud jsou data poškozena, zobrazí se varovné hlášení. Procesorová jednotka je schopna na příkaz zobrazit verzi softwaru úložné jednotky (vyžádáno prostřednictvím sériového protokolu).

4.1.4 Mapování mezi požadavky a vlastnostmi přijatelného řešení

Č.	Požadavek	Přijatelné řešení (Třída rizika C)
U2	Označení softwaru	Při spuštění se zobrazí verze softwaru procesorové jednotky. Verzi softwaru úložné jednotky lze získat prostřednictvím sériového protokolu a je uvedena ve speciálním menu.
U3	Vliv uživatelských rozhraní	Uživatelské rozhraní procesorové jednotky je navrženo tak, aby nemohlo dojít k nepřípustnému ovlivnění softwaru, parametrů nebo měřených dat. Úložná jednotka nemá uživatelské rozhraní.
U4	Vliv komunikačních rozhraní	Neexistují žádná otevřená komunikační rozhraní.
U5	Ochrana proti náhodným či neúmyslným změnám	Jednou denně se vypočítá kontrolní součet softwaru CRC32 s tajným počátečním vektorem a typově specifické parametry procesorové jednotky se vypočítají a porovnají s referenční hodnotou. Podobný proces lze spustit pro externí úložnou jednotku prostřednictvím sériového protokolu. Pokud některá z kontrol selže, zobrazí se uživateli varovní hlášení a další měření není možné. Specifické parametry přístroje jsou kalibrační data pro snímače vzdálenosti a rychlosti. Ty jsou uloženy ve speciální flash paměti uvnitř procesorové jednotky. Integrita flash paměti se kontroluje jednou denně a po spuštění a restartu pomocí kontrolního součtu CRC32. Pokud kontrola selže, zobrazí se uživateli varovné hlášení a další měření není možné.
U6	Ochrana proti nepřípustným záměrným změnám	Viz U5. Navíc jsou zaplombované kryty všech komponent a všechna komunikační připojení. Vestavěný displej na příkaz zobrazí vypočtenou hodnotu CRC32 legálně relevantního softwaru a typově specifické parametry.
U7	Ochrana parametrů	Neexistují žádné příkazy pro úpravu specifických parametrů přístroje prostřednictvím rozhraní.
U8	Autentizace prezentovaných naměřených dat	Naměřené údaje jsou prezentovány pomocí legálně relevantního softwaru. Přístroj neobsahuje žádný legálně nerelevantní software.
U9	Vliv jiného softwaru	Přístroj neobsahuje žádný legálně nerelevantní software.
L1	Úplnost uložených naměřených dat	Uložené datové sady vždy odpovídají formátu uvedenému v bodě 4.1.3. Neúplné datové sady jsou úložnou jednotkou vyřazeny a procesorové jednotce je zasláno chybové hlášení.
L2	Ochrana proti náhodným či neúmyslným změnám	Každý datový soubor je přenášen spolu s kontrolním součtem CRC32. Kontrolní součet se kontroluje před načtením. Výsledek kontroly se zobrazí vedle načteného výsledku měření.
L3	Integrita dat	Každý datový soubor je přenášen spolu s kontrolním součtem CRC32. Kontrolní součet se kontroluje před načtením. Výsledek kontroly se zobrazí vedle načteného výsledku měření.
L4	Dohledatelnost uložených naměřených dat	Vzhledem k tomu, že úložná jednotka a procesorová jednotka jsou propojeny zaplombovaným kabelem, nejsou nutné žádné další prostředky pro ověření původu naměřených dat.
L5	Utajení klíčů	Tajný počáteční vektor používaný pro výpočet kontrolního součtu naměřených dat slouží jako kryptografický klíč. Je uložen ve spustitelném kódu procesorové jednotky. Neexistují žádné příkazy pro čtení nebo úpravu startovacího vektoru, které lze použít prostřednictvím rozhraní.
L6	Načtení, verifikace a zobrazení uložených dat	Software v úložné jednotce před načtením ověří každou datovou sadu. Software na procesorové jednotce zobrazuje načtené výsledky měření a informuje uživatele o poškozených nebo upravených datových sadách.
L7	Automatické uložení	Po dokončení měření se výsledek odešle do úložné jednotky bez zásahu uživatele. Další měření lze zahájit pouze v případě, že operace ukládání proběhla úspěšně.
L8	Kapacita paměti a kontinuita	Úložná jednotka má dostatečnou kapacitu pro uložení výsledků měření pro dvě po sobě jdoucí ověřovací období. Výsledky měření starší, než dvě ověřovací období se automaticky vymažou. Pokud se přesto paměť zaplní, zobrazí se uživateli varovné hlášení a další měření již není možné.

Tabulka 4-1: Technické požadavky a popis přijatelných řešení pro externí úložnou jednotku.

4.2 Externí zobrazovací jednotka připojená k "Základní jednotce"

4.2.1 Předpoklady týkající se "Základní jednotky"

- "Základní jednotka" bez externí zobrazovací jednotky musí splňovat požadavky U1, U2, U3 až U7 a U9 příručky WELMEC 7.2 Guide, 2018**.**
- Pro identifikaci "základní jednotky", která je vyžadována v U2, existuje rozhraní k zobrazovací jednotce.
- Pokud lze zobrazovací jednotku oddělit od "základní jednotky" bez porušení plomby, pak rozhraní "základní jednotky", které se obvykle používá pro připojení zobrazovací jednotky, musí splňovat požadavek U4.
- Přenos dat mezi "Základní jednotkou" a zobrazovací jednotkou musí splňovat požadavky T1 až T8. Základní jednotka" musí splňovat požadavky T1, T2, T3, T4, T5, T7 a T8.

4.2.2 Příslušné požadavky na zobrazovací jednotku

- "Základní jednotka" a zobrazovací jednotka musí společně splňovat požadavky U2 a U8.
- Pokud má externí zobrazovací jednotka vlastní legálně relevantní software, musí v kombinaci se "základní jednotkou" splňovat požadavky U2, U4, U5, U6, U7 a U9. (U2: Požadavek se vztahuje na identifikaci softwaru externí zobrazovací jednotky i na identifikaci softwaru "základní jednotky".
- Pokud má externí zobrazovací jednotka uživatelské rozhraní (např. vypínač), musí v kombinaci se "základní jednotkou" splňovat U3.
- Případně se zkontrolují rozšíření D a S.
- Přenos dat mezi "základní jednotkou" a zobrazovací jednotkou musí splňovat požadavky T1 až T8. Zobrazovací jednotka musí splňovat požadavky T2, T3, T4, T5, T6, T7 a T8.

4.2.3 Popis přijatelného řešení

Následující přijatelné řešení je konkrétně zaměřeno na přístroje typu U rizikové třídy C. Pro jinou základní konfiguraci nebo jinou rizikovou třídu je třeba přijatelné řešení odpovídajícím způsobem upravit.

Přístroj pro měření kapalin jiných než voda je vybaven třemi ultrazvukovými snímači, které měří objem kapaliny protékající potrubím. Snímače jsou fyzicky zaplombovány a prostřednictvím kabelu připojeny k centrální procesorové jednotce, která pro datovou komunikaci používá sériový protokol. Všechna kabelová připojení jsou rovněž fyzicky chráněna proti neoprávněné manipulaci. Celkový naměřený objem se ukládá do vyhrazeného, průběžně se zvyšujícího registru. Po instalaci přístroj měří průtok kapaliny bez nutnosti manuálního zadávání. Nastavení kalibračních parametrů lze provést pouze při otevřeném krytu přístroje. Procesorová jednotka je vybavena LED diodou, která signalizuje, že do protokolu chyb bylo přidané nové chybové hlášení.

Pro zobrazení aktuálního výsledku měření lze k sériovému portu procesorové jednotky připojit displej. Po připojení je třeba projít všechny záznamy v protokolu chyb, a to vydáním příkazů (prohlížení pomocí příkazů vpřed, vzad) procesorové jednotce, která

odpovídajícím způsobem odpoví, a teprve poté se zobrazí výsledek měření. Sériové rozhraní procesorové jednotky a zobrazovací jednotky jsou chráněny softwarovým filtrovacím modulem, který zamítá všechny příchozí nepřípustné příkazy. Procesorová jednotka po připojení předává aktuální objem a časové razítko displeji, který automaticky zobrazuje výsledek.

4.2.4 Mapování mezi požadavky a vlastnostmi přijatelného řešení

Č.	Požadavek	Přijatelné řešení (Třída rizika C)
U2	Označení softwaru	Při spuštění se zobrazí verze softwaru zobrazovací jednotky. Verze softwaru procesorové jednotky se vypočítá a odešle do displeje při propojení obou jednotek. Verze softwaru procesorové jednotky se zobrazí vedle výsledku měření.
U3	Vliv uživatelských rozhraní	Procesorová jednotka nemá uživatelské rozhraní. Uživatelské rozhraní zobrazovací jednotky se skládá ze dvou tlačítek, která mohou spouštět pouze dva povolené příkazy "předchozí položka" a "další položka".
U4	Vliv komunikačních rozhraní	Sériová komunikační rozhraní procesorové jednotky a zobrazovací jednotky jsou chráněna softwarovými filtračními moduly, které zamítají všechny nepřípustné příkazy.
U5	Ochrana proti náhodným či neúmyslným změnám	Jednou denně se vypočítá kontrolní součet softwaru CRC32 s tajným počátečním vektorem a typově specifické parametry procesorové jednotky se vypočítají a porovnají s referenční hodnotou. Podobný proces lze spustit pro externí zobrazovací jednotku, když je připojená k procesorové jednotce. Pokud některá z kontrol selže, přidá se záznam do protokolu chyb a rozsvítí se LED dioda na vnější straně procesorové jednotky. LED dioda se vypne až poté, co uživatel projde všechny záznamy v protokolu chyb. Specifické parametry přístroje jsou kalibrační údaje pro ultrazvukové snímače. Ty jsou uloženy ve speciální flash paměti v procesorové jednotce. Integrita flash paměti se kontroluje jednou denně pomocí kontrolního součtu CRC32. Pokud kontrola selže, přidá se záznam do protokolu o chybách.
U6	Ochrana proti nepřípustným záměrným změnám	Viz U5. Sériová komunikační rozhraní navíc splňuje U4.
U7	Ochrana parametrů	Neexistují žádné příkazy pro úpravu specifických parametrů přístroje prostřednictvím rozhraní.
U8	Autentizace prezentovaných naměřených dat	Naměřené údaje jsou prezentovány pomocí legálního softwaru. Přístroj neobsahuje žádný legálně nerelevantní software.
U9	Vliv jiného softwaru	Přístroj neobsahuje žádný legálně nerelevantní software.
T1	Úplnost přenesených dat	Datové sady odesílané z procesorové jednotky do zobrazovací jednotky vždy odpovídají formátu uvedenému v poslední větě kapitoly 4.2.3.
T2	Ochrana proti náhodným či neúmyslným změnám	Každý datový soubor je přenášen spolu s kontrolním součtem CRC32. Kontrolní součet je kontrolován zobrazovací jednotkou. Výsledek kontroly se zobrazí spolu s načteným výsledkem měření.
T3	Integrita dat	Každý datový soubor je přenášen spolu s kontrolním součtem CRC32. Kontrolní součet je kontrolován zobrazovací jednotkou. Výsledek kontroly se zobrazí spolu s načteným výsledkem měření.
T4	Dohledatelnost přenesených naměřených dat	Protože CRC používaný k ochraně přenášených dat proti modifikaci a je založen na tajném počátečním vektoru, zajišťuje také autenticitu přenášených dat.
T5	Utajení klíčů	Tajný počáteční vektor používaný pro výpočet kontrolního součtu naměřených dat slouží jako kryptografický klíč. Je uložen ve spustitelném kódu procesorové jednotky a zobrazovací jednotky. Prostřednictvím uživatelského nebo komunikačního rozhraní nejsou k dispozici žádné příkazy k načtení nebo úpravě počátečního vektoru.
T6	Příjem, verifikace a zacházení s přenesenými naměřenými daty	Pokud kontrola CRC přijatých dat v zobrazovací jednotce selže, zobrazí se vedle (případně zkresleného) výsledku měření chyba.
T7	Zpoždění při přenosu	Pokud je zobrazovací jednotka připojena k procesorové jednotce, ale data měření se opozdí, nezobrazí se žádný výsledek měření. Na displeji se zobrazí obecné chybové hlášení, výsledek měření v procesorové jednotce není takovým zpožděním ovlivněn.

T8	Dostupnost přenosových služeb	Pokud je zobrazovací jednotka připojena k procesorové jednotce, ale nejsou přijata žádná data měření, nezobrazí se žádný výsledek měření. Na displeji se zobrazí obecné chybové hlášení, výsledek měření v procesorové jednotce není přerušením komunikačního spojení ovlivněn.

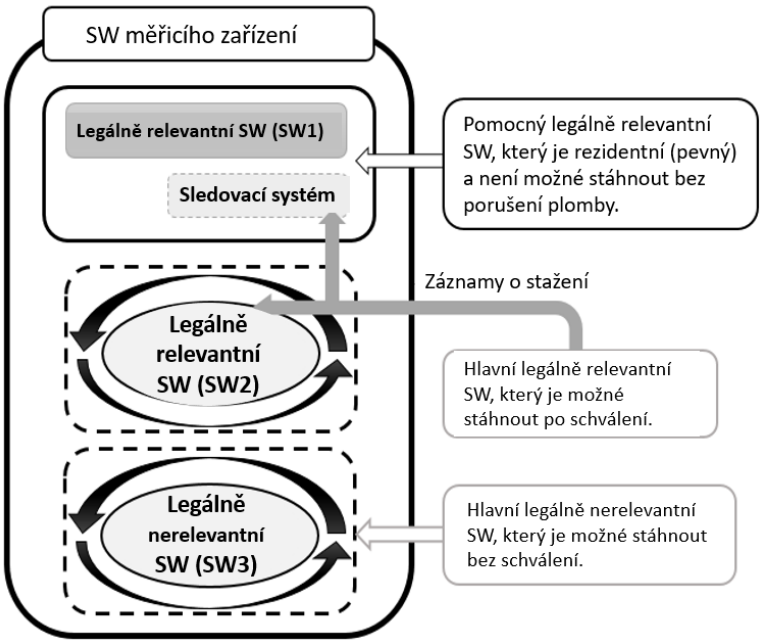
Tabulka 4-2: Technické požadavky a popis přijatelných řešení pro externí zobrazovací jednotku.

4.3 Rozšíření D: Stahování legálně relevantního softwaru

Toto rozšíření se použije, pokud jsou přístroje vybaveny nástrojem pro stažení softwaru bez porušení plomby podle příručky WELMEC Guide 7.2, 2018. Rozšíření je možné použít pro měřící zařízení typu P po splnění požadavků D1-D4.

4.3.1 Popis přijatelného řešení

Následující přijatelné řešení je zaměřeno na typ P rizikové třídy C. Pro jinou základní konfiguraci nebo jinou rizikovou třídu je třeba přijatelné řešení odpovídajícím způsobem upravit.



Obrázek 4-3: SW měřicího zařízení

Měřicí přístroj obsahuje 3 různé MCU (MCU1, MCU2 a MCU3). MCU1 obsahuje legálně relevantní SW (dále jen "SW1"), který je zodpovědný za celý proces stahování a je pevně zabudován (není možné jej měnit nebo aktualizovat bez porušení plomby). MCU2 obsahuje legálně relevantní SW (dále jen "SW2"), který zajišťuje veškeré legálně relevantní funkce, a MCU3 obsahuje legálně nerelevantní SW (dále jen "SW3"). SW1 a SW2 mají své vlastní kontrolní součty a verze SW, které je možné přečíst bez dalších nástrojů. MCU1 obsahuje skrytý digitální podpis, funkce pro provádění stahování SW a dva záznamníky událostí (Sledovací systém: EL_1, EL_2). Záznamy v záznamnících událostí není možné upravovat či vymazat. Záznamy lze

vymazat až po porušení pečeti. EL_1 obsahuje záznamy o úspěšně staženém SW. V případě, že počet záznamů je 50, MCU1 se elektronicky uzamkne a od té doby není možné stahovat SW. EL_2 obsahuje záznamy o neúspěšně staženém SW. Kapacita záznamů je 500. Pokud je jeden ze záznamníků plný, MCU1 bude rovněž elektronicky zablokován a další stahování SW není možné. Další stahování je možné až po vymazání záznamů ze záznamníků událostí. Záznamy v záznamnících událostí jsou chráněny proti vymazání/změně přepínačem, který je pod plombou. SW1 je zodpovědný za celý proces stahování. Před zahájením procesu stahování SW1 zkontroluje, zda je digitální podpis nové stažené verze SW2 správný. Digitální podpis slouží ke kontrole pravosti, integrity a odpovídajícího původu. Pokud je ověření digitálního podpisu negativní, je proveden tomu odpovídající záznam do EL_2. Důvodů, proč proces stahování nedokončí úspěšně, může být několik, např. problémy s připojením, chyby v přenosu atd.; každý typ problému má svou vlastní identifikaci. Pokud je ověření digitálního podpisu vyhovující, zahájí se proces stahování SW. Prvním krokem je přenos aktuálního legálně relevantního softwaru do dočasné paměti. Pokud při přenosu dojde k chybě, je proveden záznam do EL_2. Digitální podpis se používá také pro kontrolu integrity nového staženého softwaru SW2 (jako kontrola, zda byly všechny balíčky přeneseny kompletně a bez závad). Pokud je kontrola integrity negativní, je proveden záznam do EL_2. Druhým krokem je instalace. Proces instalace začíná, jakmile úspěšně skončí testy integrity atd. Během procesu instalace je proces měření zastaven maximálně na 2 minuty. Po úspěšné instalaci SW1 vytvoří záznam do EL_1, pokud ne, pak vytvoří záznam do EL_2.

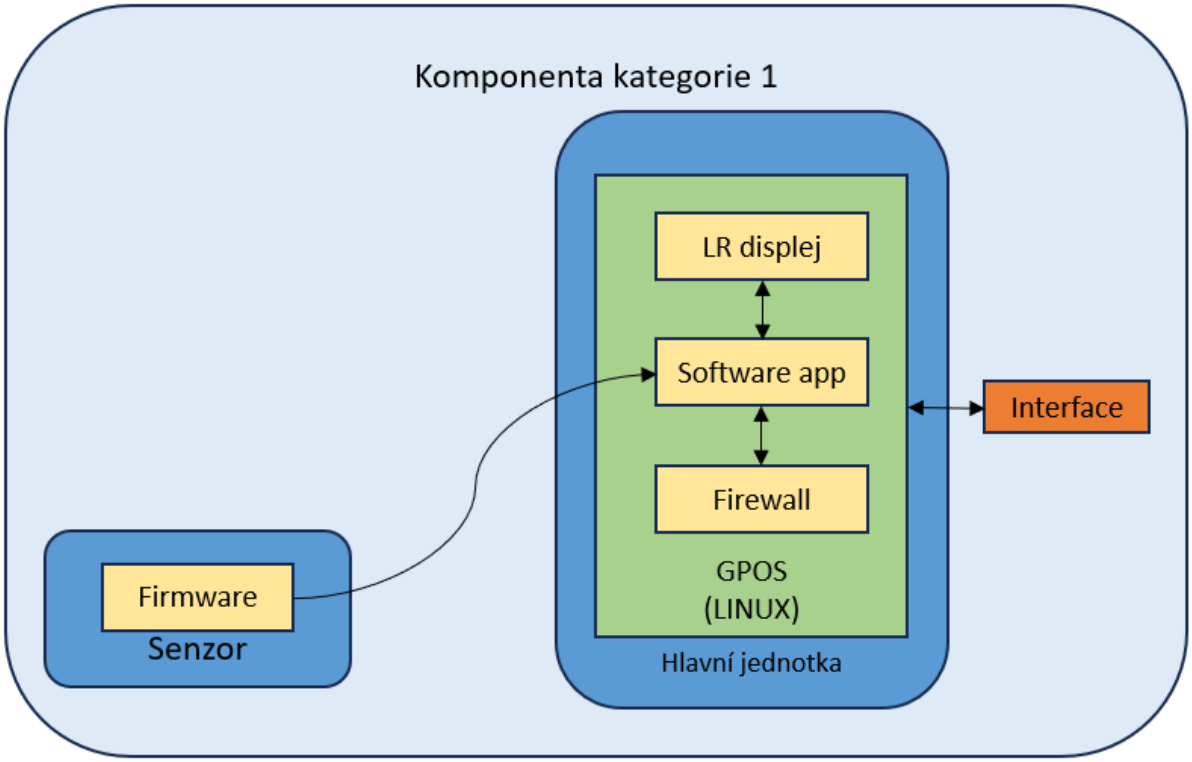
4.3.2 Mapování mezi požadavky a vlastnostmi přijatelného řešení

Č.	Požadavek	Přijatelné řešení (Třída rizika C)
D1	Mechanismus stahování	SW na MCU1 (SW1) je zodpovědný za celý mechanismus stahování. Proces stahování se skládá z kontroly digitálního podpisu, stažení aktuálního softwaru do dočasné paměti, kontroly integrity nového softwaru, správného procesu instalace, vytvoření záznamů do záznamníků událostí atd.
D2	Prokázání věrohodnosti přeneseného softwaru	Před zahájením procesu stahování SW1 zkontroluje, zda je digitální podpis nové stažené verze správný.
D3	Integrita stahovaného softwaru	Digitální podpis se používá pro kontrolu integrity nově staženého softwaru SW2 (jako kontrola, zda byly všechny balíčky přeneseny kompletně a bez chyb). Po kontrole integrity SW vytvoří záznam do záznamníku událostí EL_1 (v případě správného výsledku) nebo do EL_2 (v případě nesprávného výsledku v kterémkoli bodě procesu stahování).
D4	Dohledatelnost stahovaného legálně relevantního softwaru	MCU1 obsahuje dva záznamníky událostí (EL_1, EL_2). EL_1 obsahuje záznamy o úspěšně staženém SW. V případě, že počet záznamů je 50, MCU1 se elektronicky zablokuje a stahování SW od té doby není možné. EL_2 obsahuje záznamy o neúspěšně staženém SW. Kapacita záznamů je 500. Pokud je jeden ze záznamníků plný, MCU1 bude rovněž elektronicky zablokován a další stahování SW není možné. Další stahování je možné až po vymazání záznamů ze záznamníků událostí. Záznamy v záznamnících událostí jsou chráněny proti vymazání/změně pomocí přepínače pod plombou

Tabulka 4-3: Technické požadavky a popis přijatelných řešení pro stahování legálně relevantního softwaru.

4.4 Rozšíření O: Komponenta kategorie 1

Příklad se zabývá měřicím přístrojem s vestavěným počítačem a zaměřuje se především na použití rozšíření O na komponentu kategorie 1.



Obrázek 4-4: Přehled systému komponenty kategorie 1

4.4.1 Předpoklady týkající se přístroje

- Senzor splňuje všechny požadavky typu P i rozšíření T pro uzavřené sítě týkající se přenosu měřicích dat do vestavěného PC.
- Všechny požadavky typu U jsou splněny vestavěným PC.
- Kontrolní součet softwaru senzoru se denně ověřuje a posílá do vestavěného PC společně s číslem verze pro indikaci na příkaz.
- Legálně relevantní indikace je realizována prostřednictvím hardwarového displeje připojeného k vestavěnému PC. Naměřená data z měření získané prostřednictvím komunikačního rozhraní přístroje nejsou legálně relevantní.

4.4.2 Příslušné požadavky na přístroj

- Požadavky typu P a rozšíření T pro senzor
- Požadavky typu U a rozšíření O pro vestavěné PC

4.4.3 Popis přijatelného řešení

Komponenta kategorie 1 se skládá ze senzoru s digitálním výstupem připojeného k malému vestavěnému PC uvnitř uzavřeného obalu. Na vestavěném PC běží bootovací načítač uboot (uboot boot loader) a operační systém Linux, na kterém běží aplikace

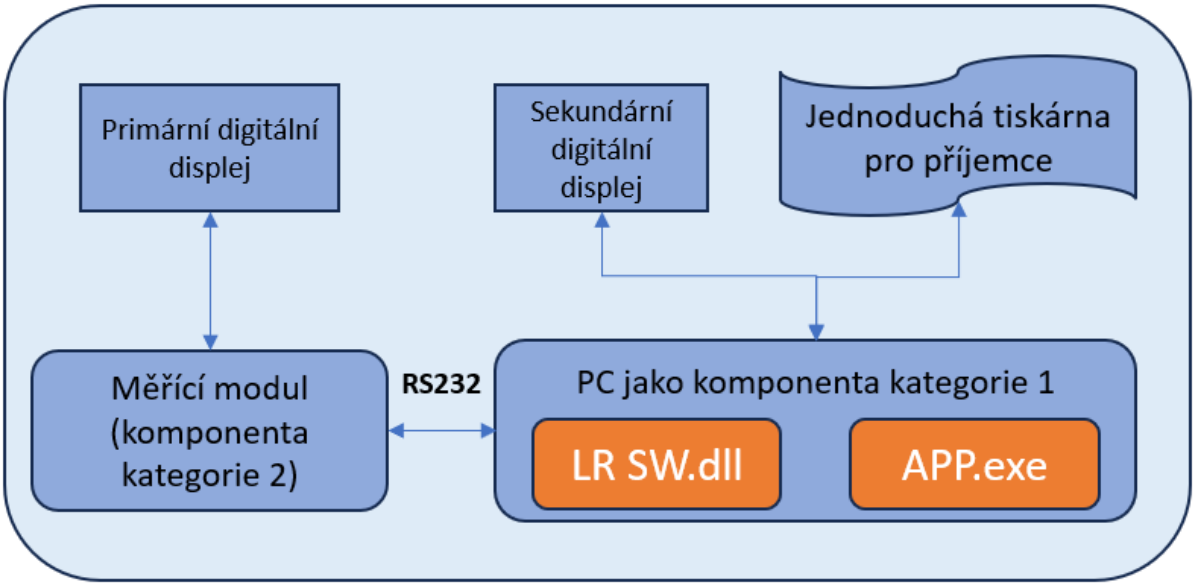
pro vizualizaci výsledku měření a zaznamenávání chyb. BIOS je zabezpečen náhodným heslem a chráněn uzavřeným obalem komponenty. Při spuštění uboot ověřuje integritu operačního systému pomocí SHA256 vypočítaného nad legálně relevantními částmi operačního systému (konfigurace bootování, /etc, /kernel, /lib). Operační systém se spustí pouze v případě, že hash odpovídá své referenční hodnotě. Hash a číslo verze distribuce Linuxu spolu s verzí jádra jsou zobrazeny během bootování. Legálně relevantní startovací skript, který je součástí konfigurace bootování, poté ověří integritu legálně relevantní aplikace a v případě nesrovnalosti vypne operační systém. Aplikace běží v režimu Kiosk. Pro získání měřicích dat, která nejsou legálně relevantní, v zařízení jsou NFC a Ethernetové rozhraní. Obě jsou logicky mapovány na interní softwarové rozhraní chráněné na straně operačního systému firewallem a na úrovni aplikace filtrem příkazů. Priorita procesu aplikace zajišťuje, že má vždy dostatek procesorového času (CPU time).

4.4.4 Mapování mezi požadavky a vlastnostmi přijatelného řešení

Č.	Požadavek	Přijatelné řešení (riziková třída C)
O1	Hardware	• Uzavřený kryt s otevřenými rozhraními NFC a Ethernet.
O2	Bootovací proces	• Zabezpečení systému BIOS heslem spolu se zapečetěným krytem zajišťuje, že systém uboot nelze snadno obejít. • Uboot kontroluje integritu operačního systému. Startovací skript kontroluje integritu aplikace a v případě selhání kontroly vypne operační systém.
O3	Systémové prostředky	Neměnné softwarové prostředí spolu s prioritou procesu právně relevantní aplikace zajišťují, že pro legálně relevantní aplikaci je vždy k dispozici dostatek prostředků.
O4	Ochrana během používání	Startovací proces zajišťuje, že je vždy nastaven režim Kiosk a že uživatel nemůže získat přístup k funkcím operačního systému.
O5	Ochranná rozhraní	Konfigurace firewallu zajišťuje, že pro externí komunikaci jsou otevřeny pouze omezené počty portů.
O6	Identifikace operačního systému a jeho konfigurace	Verze distribuce Linuxu a SHA256 pro legálně relevantními částmi operačního systému jsou zobrazeny na displeji během bootování.
O7	Ochrana operačního systému	SHA256 pro konfigurací bootování, /kernel, /knihovny apod.

4.5 Rozšíření O: Komponenta kategorie 2

Tento příklad se zabývá měřicím přístrojem s počítačem a zaměřuje se především na použití Rozšíření O na komponentu kategorie 2.



Obrázek 4-5: Přehled systému měřicího přístroje, který se skládá z primárního digitálního displeje, měřicího modulu, počítače, sekundárního displeje a jednoduché tiskárny pro příjemce

4.5.1 Předpoklady týkající se měřicího přístroje

- Měřicí modul splňuje všechny požadavky typu P. Na měřicím modulu není spuštěn žádný legálně nerelevantní software. Měřicí modul je připojen pouze jedním sériovým portem, který slouží ke komunikaci s PC. Jsou splněny požadavky na rozšíření T pro uzavřené sítě týkající se přenosu měřicích dat do PC.
- Primární zobrazení je realizováno pomocí digitálního hardwarového displeje připojeného k měřicímu modulu (komponenta kategorie 1).
- Technická pracovní skupina zařadila PC do kategorie 2. Všechny požadavky typu U a rozšíření S, D, L a T pro uzavřené sítě jsou splněny PC.
- Legálně relevantní data nelze získat prostřednictvím komunikačního rozhraní PC.

4.5.2 Příslušné požadavky na přístroj

- Požadavky typu P a požadavky rozšíření T pro měřicí modul.
- Požadavky typu U, požadavky T, požadavky S, požadavky L, požadavky D a rozšíření O kategorie 2 pro PC za podmínky, že technická pracovní skupina přiřadila tuto komponentu do kategorie 2.

4.5.3 Popis přijatelného řešení pro PC

Aplikace běží v režimu Kiosk. Priorita procesu aplikace zajišťuje, že má vždy dostatek procesorového času (CPU time).
Kontrolní součet softwaru LR SW.dll je zobrazen na sekundárním displeji a lze jej zkontrolovat při spuštění a je prezentován na příkaz spolu s číslem verze.

LR SW.dll obsahuje všechny legálně relevantní funkce. Legálně nerelevantní APP.exe je používán pro jiné účely. Rozhraní pro připojení periferních zařízení (např. klávesnice, tiskárna, myš) a pro komunikaci se systémem daňového úřadu (tax authority system), jako je USB, Ethernet, jsou chráněny. Zásady pro používaní USB zajišťují, že k PC mohou být připojena pouze předem vybraná zařízení. Konfigurace firewallu Windows zajišťuje, že pro externí komunikaci jsou otevřeny pouze omezené počty portů.
Operační systém je identifikován verzí Windows 7 Embedded a SHA256 pro specifické legálně relevantní konfigurační soubory a klíče registru. Identifikace je zobrazena LR SW.dll na příkaz. Neexistují žádná rozhraní pro přímý přístup k paměti. Hash je kontrolován aplikací, která v případě nesrovnalosti vypne systém.

4.5.4 Mapování mezi požadavky a vlastnostmi přijatelného řešení

Č.	Požadavek	Přijatelné řešení (riziková třída C)
O1	Hardware	• Uzavřený kryt PC s otevřenými rozhraními USB, Ethernet. • Hardware rozhraní, která mohou ovlivnit operační systém, jsou vypnuta operačním systémem. • Neexistují žádná rozhraní pro přímý přístup k paměti.
O3	Systémové prostředky	• Režim Kiosk spolu s prioritou procesu legálně relevantní aplikace zajišťuje, že jsou vždy k dispozici dostatečné prostředky pro legálně relevantní aplikaci
O4	Ochrana během používání	• Startovací proces zajišťuje, že je vždy nastaven režim Kiosk a že uživatel nemůže získat přístup k funkcím operačního systému.
O5	Ochranná rozhraní	• Konfigurace firewallu Windows zajišťuje, že pro externí komunikaci jsou otevřeny pouze omezené počty portů. • Zásady používání USB zajišťují, že k PC mohou být připojena pouze předem vybraná zařízení.
O6	Identifikace operačního systému a jeho konfigurace	• Verze operačního systému Windows 7 Embedded. • SHA256 nad specifickými legálně relevantními konfiguračními soubory a klíči registru
O7	Ochrana operačního systému	• SHA256 pro specifické legálně relevantní konfigurační soubory a klíče registru, které kontrolují aplikace.

5 Odkazy a literatura

[1] WELMEC Guide 7.2 “Software”,https://www.welmec.org/documents/guides/72/

[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] Draft WELMEC guide 7.3 “Reference Architectures Based on WELMEC Guide 7.2”

6 Přehled revizí

Č.	**Datum**	**Významné změny**
0	Srpen 2018	Počáteční verze
1	Duben 2019	Revidovaná verze po zasedání pracovní skupiny WG 7. Všechny odkazy na části a certifikáty pro součástí byly odstraněny.
2	Duben 2020	Byly upraveny kapitoly 4.1.1, 4.1.2, 4.2.1 a 4.2.2, pokud jde o požadavky, které je třeba splnit. Přijatelné řešení v kapitole 4.2.3 bylo upraveno pro měřidlo, které měří jiné kapaliny než vodu. 4.3 Bylo doplněno rozšíření D: Stažení legálně relevantního softwaru.

Tabulka 10-1: Historie revizí.