WELMEC 7.3

2020

WELMEC

Evropská spolupráce v oblasti legální metrologie

Referenční architektury

Na základě příručky WELMEC Guide 7.2

Pro informaci:
Tato příručka je k dispozici pracovní skupině Měřicí Přístroje pro budoucí použití na Evropských internetových stránkách.

WELMEC

Evropská spolupráce v oblasti legální metrologie

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

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

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

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

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

Referenční architektury

Obsah

Předmluva

Předkládaná příručka vychází z příručky WELMEC Guide 7.2 "Software" [1]. Tato příručka odráží současný postoj pracovní skupiny WELMEC WG 7 Software.

Ostatní pracovní skupiny WELMEC mohou stanovit další formální nebo technické požadavky. Je třeba vzít v úvahu zejména specifické požadavky na přístroje a další požadavky pro řízení měřicích úkolů po uvedení na trh nebo do provozu.

Příručka má čistě poradní charakter a sama 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

Motivací pro inovace je stále více globalizovaný trh, neustále se zvyšující snaha o efektivitu a rychle se rozvíjející požadavky spotřebitelů. Nové příležitosti k růstu proto pocházejí z poskytování nových produktů a služeb, z technologických průlomů, nových procesů a obchodních modelů, netechnologických inovací a inovací v sektoru služeb [6].

Na tomto procesu se podílejí výrobci působící v odvětví legální metrologie. Aby bylo možné doprovázet jejich činnost při zpřístupňování nových produktů na trhu, je třeba identifikovat překážky inovací v procesu posuzování shody a nabídnout řešení.

Diskuse o tomto tématu v rámci WELMECu vytvořily přesvědčení, že nabídnout výrobcům šablonu pro návrh jejich nástroje by bylo velkým přínosem pro zajištění toho, aby byl předpokládaný inovativní produkt v souladu s regulačními požadavky. Současně taková šablona poskytne oznámeným subjektům systém pro shodu inovativních návrhů výrobků v průběhu procesu posuzování shody.

Za tímto účelem poskytuje příručka obecnou šablonu měřicího přístroje založenou na modulární koncepci příručky WELMEC Guide 7.2, která odráží strukturu směrnice MID. Na základě této šablony lze modelovat architektonické příklady inovativních přístupů v měřicích přístrojích. Modely konkrétních referenčních architektur jsou již uvedeny v příručce a předpokládá se přidání dalších referenčních architektur podle potřeb zúčastněných stran.

V těchto modelech je uvedeno, kterým částem příručky WELMEC Guide 7.2 je třeba věnovat zvláštní pozornost.

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, se podívejte 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.

Vzdálené připojení *(Remote Connection)*: Termín označuje zpřístupnění modulů základní jednotce prostřednictvím digitálních komunikačních sítí, např. internetu.

Zobrazovací software *(Display Software)*: Legálně relevantní software pro zobrazení nebo tisk naměřených dat (např. L6, S2) spolu s příslušnými informacemi (např. L1). Zobrazené nebo vytištěné údaje o měření musí indikovat případné narušení autenticity a integrity.

2 Jak používat tuto příručku

Tato část popisuje strukturu příručky a vysvětluje, jak ji používat.

Cílem příručky je poskytnout šablonu pro mapování návrhů měřicích přístrojů na základě nového technologického vývoje podle požadavků příručky WELMEC Guide 7.2. S těmito identifikovanými použitelnými požadavky může být prokázáno splnění základních požadavků MID. Příručka podporuje inovace výrobců a práci oznámených subjektů tím, že usnadňuje vývojovou práci výrobců a postupy zkoušení oznámených subjektů.

Při hodnocení nového technologického vývoje by se měl použít následující postup:

- Porovnání návrhu přístroje s obecnou architekturou měřicího přístroje a kontrola, zda jsou přítomny všechny komponenty modulární architektury, viz. kapitola 3.2.
- Výsledek identifikuje odchylky mezi návrhem přístroje a všeobecnou architekturou, které je třeba upravit podle pokynů WELMEC Guide 7.2.
- Kontrola, zda se zkoušený návrh přístroje vztahuje na některý z příkladů uvedených v této příručce, viz kapitola 4. Příklady poskytují vodítko, které specifické požadavky příručky WELMEC Guide 7.2 je třeba splnit, viz. kapitola 4.x.5.
- Pokud zkoumaný návrh přístroje není uveden v příkladech, obraťte se na WELMEC WG 7 „Software“ s modelovou architekturou podle části 3.2, aby váš přístup byl analyzován a případně zahrnut do této příručky.
- Pokud jsou splněny požadavky podle této příručky, jsou splněny požadavky na zkoušku shody a kontrolu v provozu podle příručky WELMEC 7.2, viz oddíl 4.x.6.
- V rámci procesu posuzování shody je od výrobce požadována analýza rizik. Pro každý příklad jsou k dispozici konkrétní vektory útoku, viz. kapitola 4.x.7. Seznam běžných vektorů útoků, které je vždy třeba vzít v úvahu, je uveden v kapitole 5.
- Použití požadavků na software, které jsou specifické pro daný přístroj, jsou uvedené v příručce WELMEC Guide 7.2, Rozšíření I.

2.1 Celková struktura příručky

Struktura příručky je následující: v kapitole 3.1 stručně popsán modulární koncept příručky WELMEC Guide 7.2. Z tohoto základu je v kapitole 3.2 odvozena obecná architektura softwarového měřicího přístroje. Tímto způsobem lze modelovat technologické koncepty, například pro zařízení IoT, Cloud Computing a atd., a analyzovat otázku týkající se shody se základními požadavky technickým výkladem příručky WELMEC Guide 7.2. Pro vybrané technologické koncepty jsou v kapitole 4 uvedeny tzv. **Referenční architektury**, které představují potvrzení realizace takového technologického přístupu.

Požadavky na odpovídající posouzení rizik [5] pro zabezpečení softwaru jsou uvedeny ve směrnici (2014/32/EU) [2]. Seznam běžných vektorů útoku, tj. schéma, jak by mohly být hrozby realizovány, byl vypracován v pracovní skupině WELMEC

WG 7 a je uveden v kapitole 5, aby byla zaručena srovnatelnost analýzy mezi výrobci a uživateli a oznámenými subjekty. Dále jsou uvedeny konkrétní vektory útoku pro jednotlivé referenční architektury.

2.2 Jak vybrat příslušné části průvodce

Mezi hlavními úkoly takové referenční architektury je zahrnuto splnění základních požadavků, podpořit snadné ověřování a kontrolu měřidla na trhu a prozkoumat současná rizika a hrozby pro měřidla prostřednictvím odpovídající analýzy rizik.

Pro provedení analýzy, zda je zamýšlený návrh měřicího přístroje v souladu se základními požadavky a zda se na něj může vztahovat technický výklad příručky WELMEC Guide 7.2, by měla být použita obecná architektura softwarového měřicího přístroje, uvedená v kapitole 3.2. Tímto způsobem by bylo možné modelovat technologickou koncepci a analyzovat otázku týkající se její shody se základními požadavky a technickým výkladem příručky WELMEC Guide 7.2. S takovým přístupem WELMEC WG 7 by mohly být zohledněny potřeby, např. výrobců nebo oznámených subjektů.

Příručka navíc poskytuje referenční architektury, jako příkladné architektury pro technologické výzvy s využitím obecného modelu měřicího přístroje v kapitole 4.

Referenční architektury tak zajišťují splnění požadavků na software podle přílohy I směrnice MID tím, že splňují příslušné požadavky na architekturu podle příručky WELMEC Guide 7.2. V rámci těchto požadavků a modulu B jsou vazby na zkoušku shody a kontrolu v provozu, tj. na ověření měřidla, stanoveny přílohou I MID 8.2, 8.3, 7.2, 7.6 a modulem B č. 6. Kromě toho jsou k obecnému seznamu vektorů útoku, jak je uvedeno v kapitole 5 pro posouzení rizik [4], navrženy specifické vektory útoku na architekturu, dle požadavků pro posouzení shody [2].

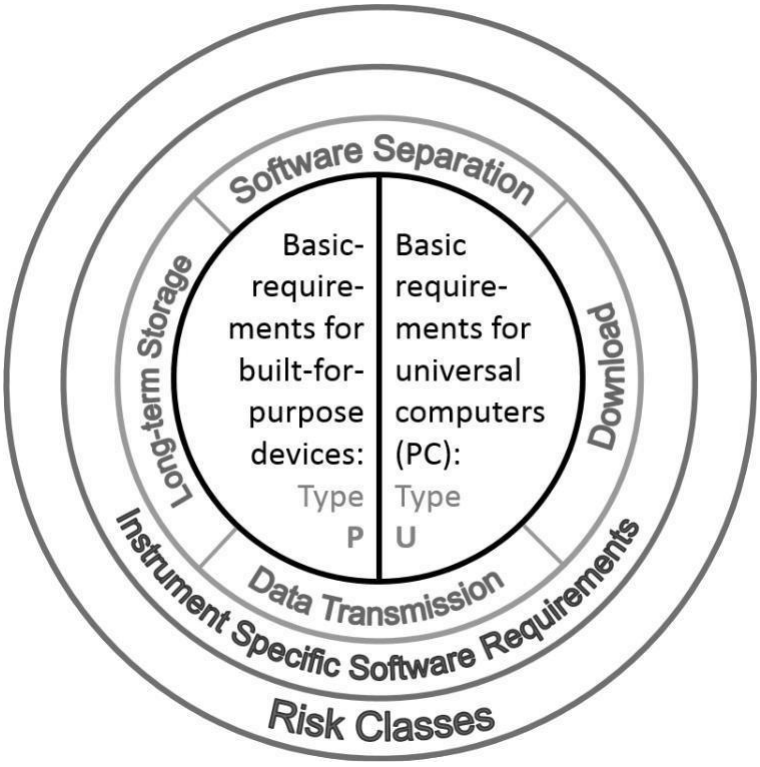
Aby byla obecná referenční architektura použitelná pro konkrétní třídu přístrojů, musí splňovat dodatečné požadavky specifické pro daný přístroj a musí být přizpůsobena rizikové třídě přístroje.

Příručka začíná architekturami, které využívají vzdálené připojení k legálně relevantním částem. Další architektury budou následovat podle potřeb zúčastněných stran.

3 Obecná architektura měřicího přístroje

3.1 Modulární koncepce příručky WELMEC 7.2

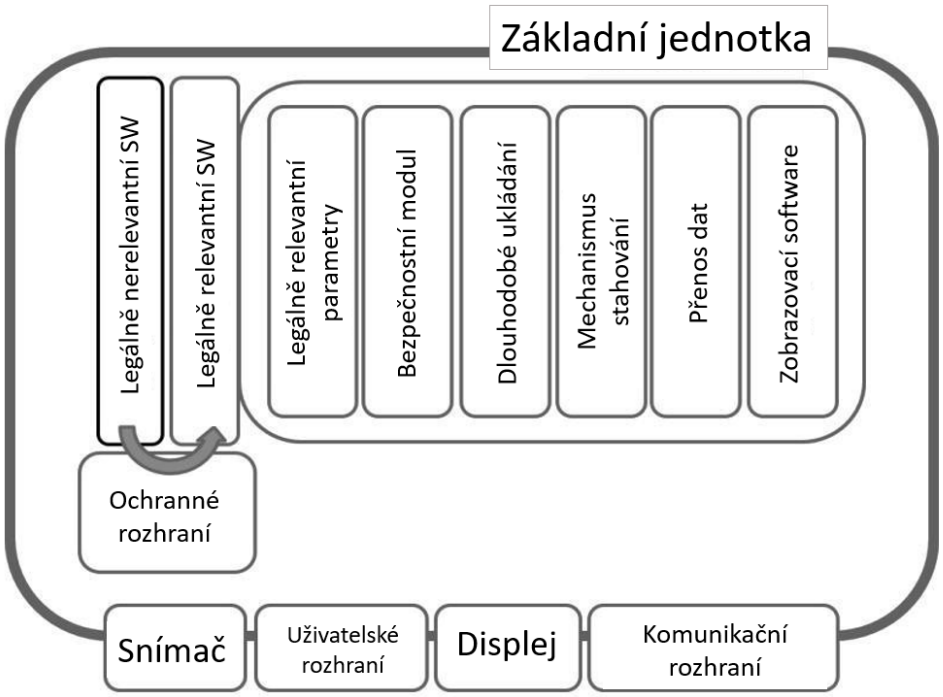
Příručka WELMEC Guide 7.2 [1] poskytuje technický výklad základních požadavků stanovených v příloze I směrnice MID (2014/32/EU) a modulu B. Její struktura vychází z obecné modulární koncepce, která umožňuje popsat širokou škálu technologických IT architektur (viz obrázek 1). Tento modulární přístup zaručuje otevřenost novým technologiím v budoucnosti a podporuje inovace.



Obrázek 1: Modulární architektura příručky WELMEC Guide 7.2 "*Software"* [1].

3.2 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 2).



Obrázek 2: 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.

Tento obecný měřicí přístroj by měl být využit k definování referenčních architektur. Tímto způsobem je možné modelovat technologickou koncepci a analyzovat otázku týkající se souladu se základními požadavky a technickým výkladem příručky WELMEC 7.2. S takovým přístupem WG 7 by mohly být zohledněny potřeby, např. výrobců nebo oznámených subjektů.

Na tomto základě, předkládaná příručka uvádí architektonické příklady technologických výzev pomocí obecného modelu a uvádí, která část příručky WELMEC Guide 7.2 zajišťuje, že takové technologické výzvy jsou pokryty základními požadavky podle MID Přílohy 1 a modulu B.

K navrhovaným architekturám je třeba přidat specifické požadavky na přístroj. Pro odpovídající posouzení rizika jsou pro každou architekturu k dispozici specifické vektory útoku, které by měly být použity navíc k obecným vektorům útoku uvedených v kapitole 5.

4 Vzdálené připojení k legálně relevantním komponentám

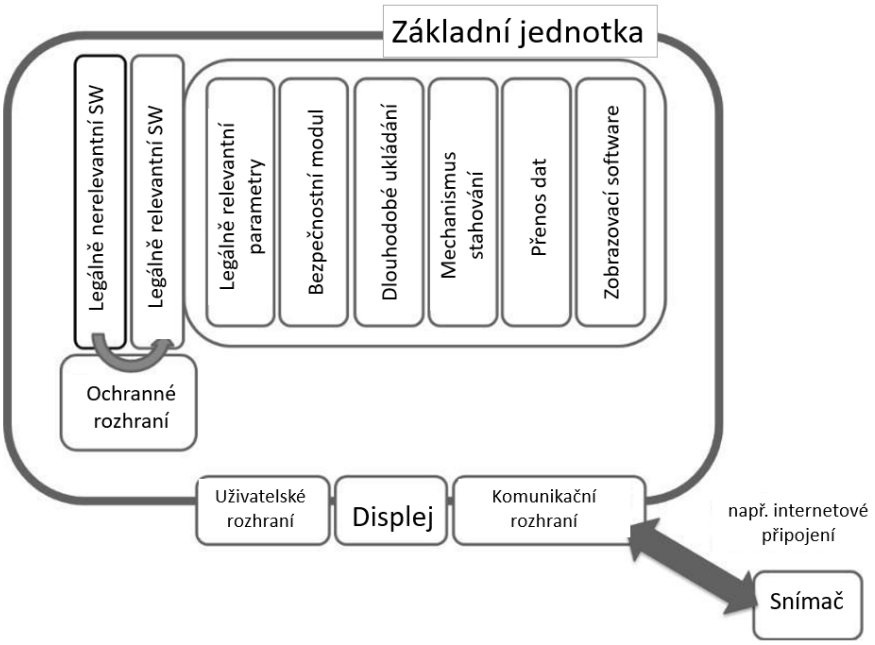
V následujícím textu rozlišujeme mezi externími moduly a zbylými moduly v základní jednotce. Termín "vzdálené připojení" označuje zpřístupnění modulů základní jednotce prostřednictvím komunikačních sítí, např. internetu. Mezní podmínky v této příručce uvádějí, že měřicí přístroj jako celek poskytuje výrobce pro posouzení shody podle modulu B. Pokud části přístroje poskytuje externí poskytovatel služeb, např. externí paměťové zařízení atd., odpovědnost za úlohu stanovenou v MID (2014/32/EU) se nemění, tj. výrobce, který žádá o EU přezkoušení typu, zůstává odpovědným.

4.1 Vzdálené připojení snímače

4.1.1 Specifický popis:

Naměřená data jsou vytvářena externím digitálním snímačem. Snímač je "spárován" se základní jednotkou, jeho poloha je identifikovatelná a každý snímač má jedinečný identifikátor. Párování je proces, při kterém si dvě zařízení vyměňují informace o zařízení, aby mohlo být vytvořeno bezpečné spojení. Cílem procesu párování zařízení je vytvořit sdílení pro utajované informace mezi dvěma zařízeními podle P8/U8.

4.1.2 Specifická architektura:



Obrázek 3: Referenční architektura pro vzdálené připojení snímače.

4.1.3 Mezní podmínky:

Měřicí přístroj je pro posouzení shody podle modulu B dodáván výrobcem jako celek, tj. výrobce dodává i snímač. Změny hardwaru snímače jsou vysledovatelné v záznamníku. Základní požadavky týkající se typu přístroje (P nebo U) splňuje základní jednotka a oddělená část samostatně. Dostupnost všech komponent, tj. úplnost měřicího přístroje, je požadována a je zaručena, pokud je splněna Příloha I, MID.

4.1.4 Specifické požadavky:

- Musí být zaručeno, že vzdáleně připojená komponenta je spárována se základní jednotkou podle P8/U8.
- Pokud je externí jednotka nahrazena podobnou jednotkou, která nebyla spárována se základní jednotkou, měřicí přístroj by neměl fungovat a je nutné provést opětovné ověření s podobnou externí jednotkou, která byla spárována se základní jednotkou podle P8/U8.
- Musí být možné identifikovat externí jednotku a odpovídající základní jednotku.
- Pokud je k dispozici několik schválených dálkových snímačů, pak identifikátory dálkových snímačů jsou legálně relevantními parametry, které zaručují, že změna snímače poskytuje důkaz o zásahu.

4.1.5 Požadavky příručky WELMEC Guide 7.2, které pokrývají tuto konfiguraci architektury:

Splnění požadavků pro rozšíření T: Přenos dat měření prostřednictvím komunikačních sítí.

Požadavek	**Popis**
T1	Úplnost přenesených dat
T2	Ochrana proti náhodným či neúmyslným změnám
T3	Integrita dat
T4	Dohledatelnost přenesených naměřených dat
T5	Utajení klíčů
T6	Zacházení s poškozenými daty
T7	Zpoždění při přenosu
T8	Dostupnost přenosových služeb

Tabulka 4.1.5: Relevantní konfigurace pro architekturu

4.1.6 Požadavky v oblasti zkoušek shody a kontroly v provozu:

Požadavek	**Předpokládá se splnění, …**
MID Příloha I 8.2 "poskytnutí důkazu o zásahu"	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními
MID Příloha I 8.3 "identifikace softwaru musí být snadno dostupná"	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními
MID Příloha I 7.2	pokud jsou P/U splněny v kombinaci s

"žádné nepřiměřené požadavky na uživatele"	požadovanými rozšířeními.

Tabulka 4.1.6: Požadavky na zkoušku shody a kontrolu v provozu

4.1.7 Specifické vektory útoku, které je třeba vzít v úvahu při posuzování rizik:

Kromě obecného seznamu vektorů útoku uvedeného v kapitole 5 je třeba u této konkrétní architektury vzít v úvahu následující útočné vektory:

- **A_Tampering_and_Injection**: Útočník manipuluje s komunikací mezi snímačem a základní jednotkou, čímž poškodí integritu naměřených dat.

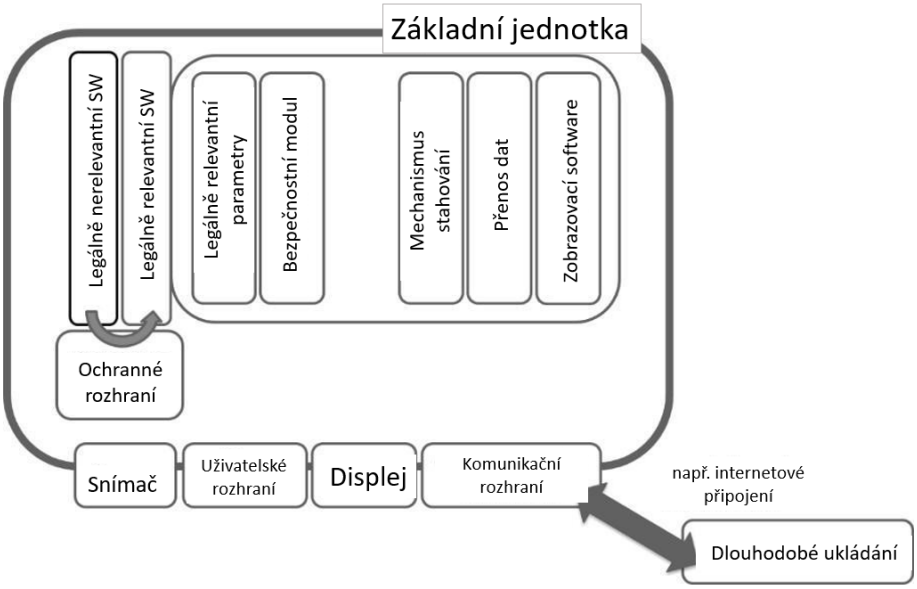
- **A_Spoofing**: Útočník se vydává za jednoho z komunikačních partnerů (odesílatele nebo příjemce), čímž poškozuje autenticitu naměřených dat.

4.2 Vzdálené připojení k uloženým naměřeným datům

4.2.1 Specifický popis:

První uložení naměřených dat se provádí na dálku. V základní jednotce není žádná kopie dat měření.

4.2.2 Specifikace architektury:



Obrázek 4: Referenční architektura pro vzdálené připojení k naměřeným datům

4.2.3 Mezní podmínky:

Měřicí přístroj je pro posouzení shody podle modulu B dodáván výrobcem jako celek, tj. výrobce dodává i externí paměťové zařízení. Pokud jsou části měřidla poskytovány externím poskytovatelem služeb, např. externí paměťové zařízení, odpovědnost stanovená v MID (2014/32/EU) se nemění, tj. výrobce, který žádá o EU přezkoušení typu, zůstává odpovědný. Základní požadavky týkající se typu měřidla (P nebo U) plní základní jednotka a oddělená část samostatně. Požaduje se dostupnost všech součástí, tj. kompletnost měřidla, která je zaručena, pokud je splněna příloha I, MID. Vzdálená paměťová jednotka neobsahuje legálně relevantní software. Veškerá opatření pro zajištění integrity dálkově uložených dat zajišťuje základní jednotka.

4.2.4 Specifické požadavky:

Žádné.

4.2.5 Požadavky příručky WELMEC Guide 7.2, které pokrývají tuto konfiguraci architektury:

Splnění následujících požadavků činí proces nezávislým na konkrétním hardwaru vzdáleného úložného zařízení.

Splnění požadavků podle rozšíření L: Dlouhodobé ukládání naměřených dat.

Požadavek	**Popis**
L1	Úplnost uložených naměřených dat
L2	Ochrana proti náhodným či neúmyslným změnám
L3	Integrita dat
L4	Autentičnost uložených naměřených dat
L5	Utajení klíčů
L6	Načtení, ověření a označení uložených dat
L7	Automatické ukládání
L8	Kapacita paměti a kontinuita

Tabulka 4.2.5: Relevantní konfigurace pro architekturu.

4.2.6 Požadavky v oblasti zkoušek shody a kontroly v provozu:

Požadavek	**Předpokládá se splnění, …**
MID Příloha I 8.2 "poskytnutí důkazu o zásahu"	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními
MID Příloha I 8.3 "identifikace softwaru musí být snadno dostupná**"**	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními
MID Příloha I 7.2 "žádné nepřiměřené požadavky na uživatele**"**	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními.

Tabulka 4.2.6: Požadavky na zkoušku shody a kontrolu v provozu,

4.2.7 Specifické vektory útoku, které je třeba vzít v úvahu při posuzování rizik:

Kromě obecného seznamu vektorů útoku uvedeného v kapitole 5 je třeba u této konkrétní architektury vzít v úvahu následující útočné vektory:

- **A_Tampering_and_Injection**: Útočník manipuluje s komunikací mezi snímačem a základní jednotkou, čímž poškodí integritu naměřených dat.

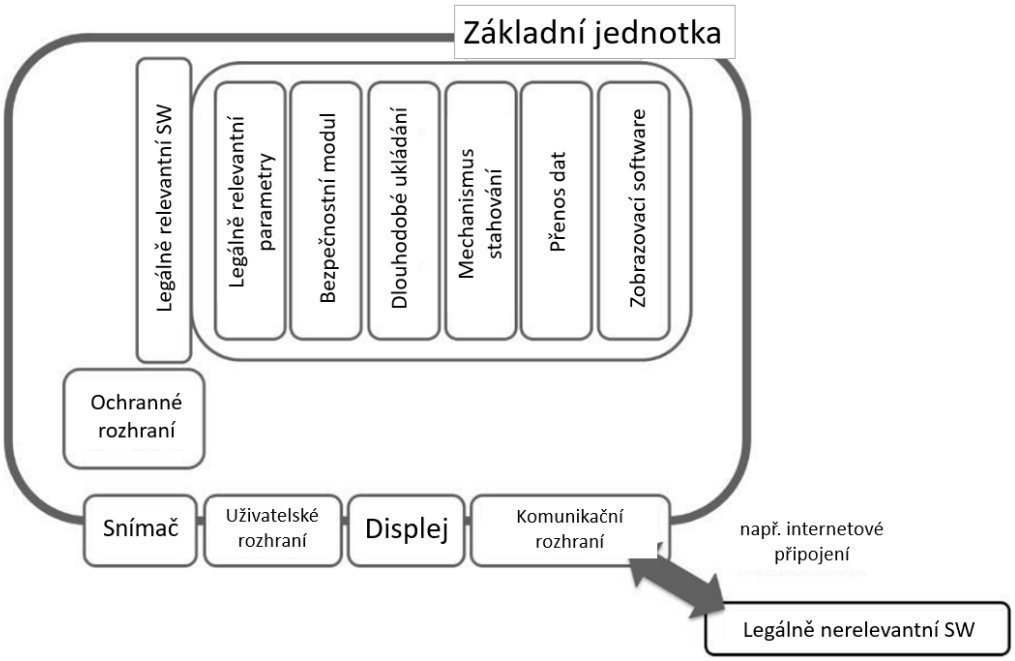
- **A_Spoofing**: Útočník se vydává za jednoho z komunikačních partnerů (odesílatele nebo příjemce), čímž poškozuje autenticitu naměřených dat.

4.3 Vzdálené připojení k legálně nerelevantnímu softwaru

4.3.1 Specifický popis:

Legálně nerelevantní software je poskytován externě prostřednictvím internetové služby, kterou hostuje výrobce. Základní jednotka obsahuje pouze legálně relevantní software.

4.3.2 Specifikace architektury:



Obrázek 5: Referenční architektura pro vzdálené připojení legálně nerelevantního softwaru

4.3.3 Mezní podmínky:

Měřicí přístroj poskytuje výrobce jako celek pro posouzení shody podle modulu B, tj. technickou strukturu obsahující legálně nerelevantní software poskytuje výrobce. Pokud části měřidla poskytuje externí poskytovatel služeb, např. technickou strukturu obsahující legálně nerelevantní software, odpovědnost stanovená v MID (2014/32/EU) se nemění, tj. výrobce, který žádá o EU přezkoušení typu, zůstává odpovědný. Základní požadavky týkající se typu měřidla (P nebo U) plní základní jednotka a oddělená část samostatně. Požaduje se dostupnost všech součástí, tj. kompletnost měřidla, která je zaručena, pokud je splněna příloha I, MID.

4.3.4 Specifické požadavky:

Žádné.

4.3.5 Požadavky příručky WELMEC Guide 7.2, které pokrývají tuto konfiguraci architektury:

Nejsou žádné požadavky na legálně nerelevantní software, pokud je použito rozšíření S.

4.3.6 Požadavky v oblasti zkoušek shody a kontroly v provozu:

Požadavek	**Předpokládá se splnění, …**
MID Příloha I 8.2 "poskytnutí důkazu o zásahu"	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními
MID Příloha I 8.3 "identifikace softwaru musí být snadno dostupná"	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními
MID Příloha I 7.2 "žádné nepřiměřené požadavky na uživatele"	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními.

Tabulka 4.3.6: Požadavky na zkoušku shody a kontrolu v provozu.

4.3.7 Specifické vektory útoku, které je třeba vzít v úvahu při posuzování rizik:

Kromě obecného seznamu vektorů útoku uvedeného v kapitole 5 je třeba u této konkrétní architektury vzít v úvahu následující útočné vektory:

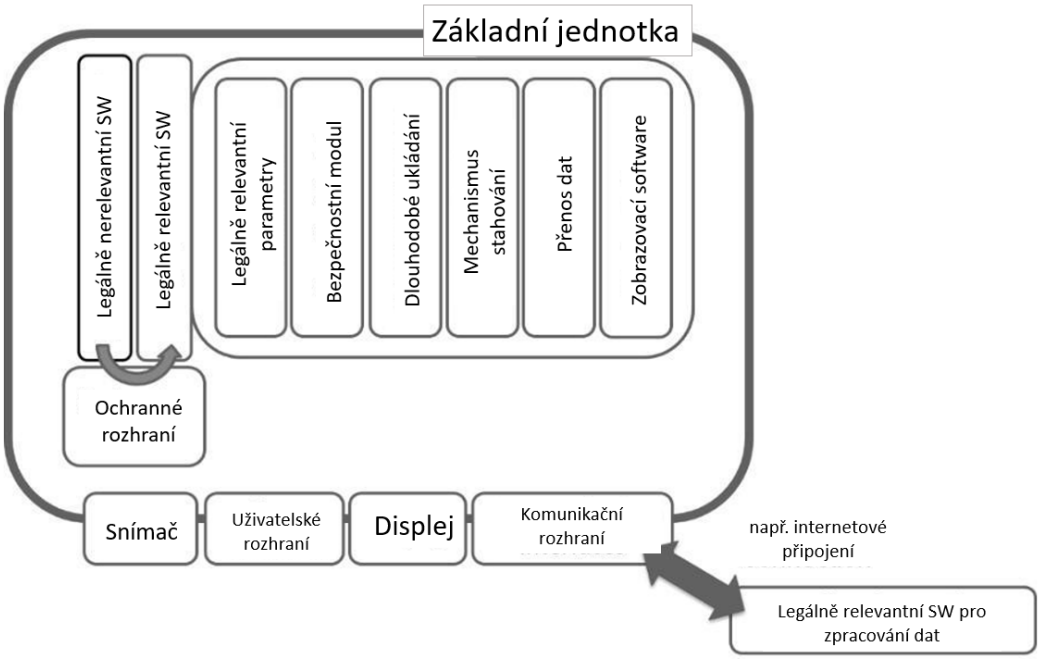
Žádné.

4.4 Vzdálené připojení k legálně relevantnímu softwaru

4.4.1 Specifický popis:

Část legálně relevantního softwaru je poskytována externě prostřednictvím internetové služby hostované výrobcem. Je třeba vzít v úvahu, že tato příručka poskytuje obecné modely. Proto se na část legálně relevantního softwaru, k níž lze získat vzdálený přístup, mohou vztahovat specifické požadavky na přístroj.

4.4.2 Specifikace architektury:



Obrázek 6: Referenční architektura pro vzdálené připojení k legálně relevantnímu softwaru.

4.4.3 Mezní podmínky:

Měřicí přístroj poskytuje výrobce jako celek pro posouzení shody podle modulu B, tj. technickou strukturu obsahující legálně nerelevantní software poskytuje výrobce. Pokud části měřidla poskytuje externí poskytovatel služeb, např. technickou strukturu obsahující legálně nerelevantní software, odpovědnost stanovená v MID (2014/32/EU) se nemění, tj. výrobce, který žádá o EU přezkoušení typu, zůstává odpovědný. Základní požadavky týkající se typu měřidla (P nebo U) plní základní jednotka a oddělená část samostatně. Požaduje se dostupnost všech součástí, tj. kompletnost měřidla, která je zaručena, pokud je splněna příloha I, MID.

4.4.4 Specifické požadavky:

- Musí být možná identifikace externí softwarové jednotky a odpovídající základní jednotky (P2/U2).
- Pokud je k dispozici několik schválených vzdálených softwarových komponent, jsou identifikátory komponent legálně relevantními parametry, které zaručují, že změna komponenty poskytne důkaz o zásahu.

4.4.5 Požadavky příručky WELMEC Guide 7.2, které pokrývají tuto konfiguraci architektury:

Splnění následujících požadavků činí proces nezávislým na konkrétním hardwaru, na kterém je externí část umístěna.
Splnění požadavků pro rozšíření T: Přenos dat měření prostřednictvím komunikačních sítí.

Požadavek	**Popis**
T1	Úplnost přenesených dat
T2	Ochrana proti náhodným či neúmyslným změnám
T3	Integrita dat
T4	Dohledatelnost přenesených naměřených dat
T5	Utajení klíčů
T6	Zacházení s poškozenými daty
T7	Zpoždění při přenosu
T8	Dostupnost přenosových služeb

Tabulka 4.4.5: Relevantní konfigurace pro architekturu.

4.4.6 Požadavky v oblasti zkoušek shody a kontroly v provozu:

Požadavek	**Předpokládá se splnění, …**
MID Příloha I 8.2 "poskytnutí důkazu o zásahu"	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními
MID Příloha I 8.3 "identifikace softwaru musí být snadno dostupná"	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními
MID Příloha I 7.2 "žádné nepřiměřené požadavky na uživatele"	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními.

Tabulka 4.4.6: Požadavky na zkoušku shody a kontrolu v provozu.

4.4.7 Specifické vektory útoku, které je třeba vzít v úvahu při posuzování rizik:

Kromě obecného seznamu vektorů útoku uvedeného v kapitole 5 je třeba u této konkrétní architektury vzít v úvahu následující útočné vektory:

- **A_Tampering_and_Injection**: Útočník manipuluje s komunikací mezi snímačem a základní jednotkou, čímž poškodí integritu naměřených dat.

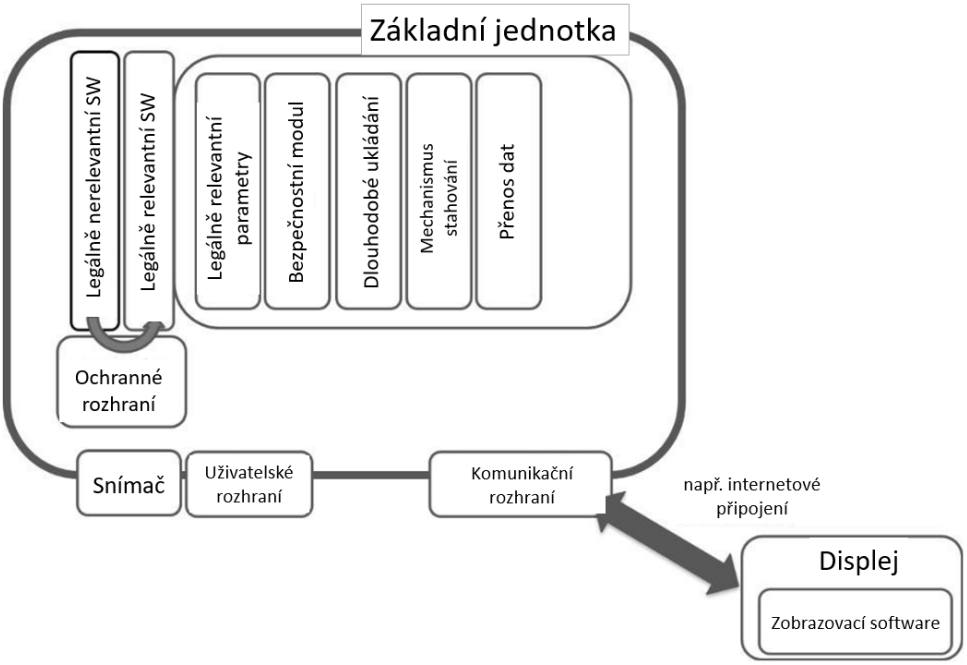
- **A_Spoofing**: Útočník se vydává za jednoho z komunikačních partnerů (odesílatele nebo příjemce), čímž poškozuje autenticitu naměřených dat.

4.5 Vzdálené připojení k legálně relevantnímu displeji

4.5.1 Specifický popis:

Naměřená data se zobrazují externě. Displej je "spárován" se základní jednotkou, jeho umístění je identifikovatelné a každý displej má jedinečný identifikátor. Párování je proces, při kterém si dvě zařízení vyměňují informace o zařízení, aby mohlo být navázáno bezpečné spojení. Cílem procesu párování zařízení je vytvořit sdílení pro utajované informace mezi dvěma zařízeními podle P8/U8.
Je třeba vzít v úvahu, že tato příručka poskytuje obecné modely. Proto se na legálně relevantní zobrazení, které by mohlo být vzdáleně přístupné, mohou vztahovat specifické požadavky na přístroje, např. MID, Příloha I, 10.5.

4.5.2 Specifikace architektury:



Obrázek 7: Referenční architektura pro vzdálené připojení displeje.

4.5.3 Mezní podmínky:

Měřicí přístroj je pro posouzení shody podle modulu B dodáván výrobcem jako celek, tj. výrobce dodává i displej. Pokud jsou části měřidla poskytovány externím poskytovatelem služeb, např. displej, odpovědnost stanovená v MID (2014/32/EU) se nemění, tj. výrobce, který žádá o EU přezkoušení typu, zůstává odpovědný. Změny hardwaru displeje se sledují v záznamníku. Základní požadavky týkající se typu přístroje (P nebo U) plní základní jednotka a oddělená část samostatně. Dostupnost všech součástí, tj. kompletnost měřicího přístroje, je vyžadována a zaručena, pokud jsou splněny požadavky MID, Příloha I, např. měřiče spotřeby musí mít displej, který je spotřebiteli přístupný bez dodatečných nástrojů.

4.5.4 Specifické požadavky:

- Musí být zaručeno, že vzdáleně připojená komponenta je spárována se základní jednotkou podle P8/U8.
- Pokud je externí jednotka nahrazena podobnou jednotkou, která nebyla spárována se základní jednotkou, měřicí přístroj by neměl fungovat a je nutné provést opětovné ověření s podobnou externí jednotkou, která byla spárována se základní jednotkou podle P8/U8.
- Musí být možné identifikovat externí jednotku a odpovídající základní jednotku.
- Pokud je k dispozici několik schválených dálkových displejů, jsou identifikátory dálkových displejů legálně relevantními parametry, které zaručují, že změna displeje poskytuje důkaz o zásahu.

4.5.5 Požadavky příručky WELMEC Guide 7.2, které pokrývají tuto konfiguraci architektury:

Splnění požadavků pro rozšíření T: Přenos dat měření prostřednictvím komunikačních sítí.

Požadavek	**Popis**
T1	Úplnost přenesených dat
T2	Ochrana proti náhodným či neúmyslným změnám
T3	Integrita dat
T4	Dohledatelnost přenesených naměřených dat
T5	Utajení klíčů
T6	Zacházení s poškozenými daty
T7	Zpoždění při přenosu
T8	Dostupnost přenosových služeb

Tabulka 4.5.5: Relevantní konfigurace pro architekturu.

4.5.6 Požadavky v oblasti zkoušek shody a kontroly v provozu:

Požadavek	**Předpokládá se splnění, …**
MID Příloha I 8.2 "poskytnutí důkazu o zásahu"	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními
MID Příloha I 8.3 "identifikace softwaru musí být snadno dostupná**"**	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními
MID Příloha I 7.2 "žádné nepřiměřené požadavky na uživatele**"**	pokud jsou P/U splněny v kombinaci s požadovanými rozšířeními.

Tabulka 4.5.6: Požadavky na zkoušku shody a kontrolu v provozu.

Podrobné přijatelné řešení lze nalézt v příručce WELMEC Guide 7.4, kapitola 4.2.

4.5.7 Specifické vektory útoku, které je třeba vzít v úvahu při posuzování rizik:

Kromě obecného seznamu vektorů útoku uvedeného v kapitole 5 je třeba u této konkrétní architektury vzít v úvahu následující útočné vektory:

- **A_Tampering_and_Injection**: Útočník manipuluje s komunikací mezi snímačem a základní jednotkou, čímž poškodí integritu naměřených dat.

- **A_Spoofing**: Útočník se vydává za jednoho z komunikačních partnerů (odesílatele nebo příjemce), čímž poškozuje autenticitu naměřených dat.

5 Seznam vektorů útoku použitých při posouzení rizika

Rapidní technologický vývoj otevírá nové možnosti, ale také rizika, protože radikálně mění fungování měřicích přístrojů ve společnosti. Proto lze ve směrnici (2014/32/EU) [2] nalézt přísnější požadavky na odpovídající posouzení rizik [5] pro zabezpečení softwaru. Analýza rizik, která zohledňuje současné hrozby a zaručuje srovnatelnost v celé Evropě, by také zvýšila kompetence všech zúčastněných stran. Pro zaručení srovnatelnosti analýzy mezi výrobci a notifikovanými osobami je zde uveden seznam běžných vektorů útoku, tj. schéma, jak by mohly být hrozby realizovány.

5.1 Běžné vektory útoku

Vhodný postup hodnocení rizik, který je schválen v pracovní skupině 7 WELMEC, naleznete v dokumentech poskytnutých knihovnou WELMEC [5]. Následující seznam vektorů útoku je záměrně obecný. Pro každou konfiguraci jsou uvedeny konkrétní vektory útoku.

- **A_PASSWORD:** Útočník získá heslo správce zkoušením možných kombinací.
- **A_CRYPTO_RET:** Útočník získá z přístroje kryptografický materiál.
- **A_BOOT:** Útočník manipuluje se spouštěcím procesem zařízení a následně instaluje škodlivý kód.
- **A_RTC:** Útočník zfalšuje uložená data pomocí manipulací s hodinami reálného času zařízení.
- **A_IF_DEBUG:** Útočník využívá ladicí rozhraní, která nebyla deaktivována.
- **A_INT_SERIAL:** Útočník využije zranitelnost proprietárního sériového protokolu.
- **A_INT_PLUGNPLAY:** Útočník využije zranitelnost rozhraní plug-and-play, například USB.
- **A_WEB_XSS:** Útočník provede na webovém serveru útok typu cross-site scripting (XSS).
- **A_WEB_DOS:** Útočník provede útok typu odepření služby na webový server (DoS).
- **A_SW_REPLACE:** Útočník nahradí legálně relevantní software.
- **A_SW_RUNTIME_CONFIGFILES:** Útočník manipuluje se softwarem během jeho načtení do RAM paměti (runtime) úpravou nechráněných konfiguračních souborů.
- **A_SW_RUNTIME_INTERFACE:** Útočník manipuluje se softwarem během jeho načtení do RAM paměti (runtime) využitím zranitelností externích rozhraní.
- **A_DATA_GEN:** Útočník generuje falešná data měření.
- **A_DATA_DEL:** Útočník odstraní uložená data měření.

5.2 Další zdroje vektorů útoku

Stávající vektory útoků a nově vznikající hrozby lze identifikovat pomocí některého z následujících zdrojů. Výrobci by měli být požádáni, aby při identifikaci nových vektorů útoku nahlíželi do všeobecně známých online databází.

- https://cve.mitre.org/
- https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-rends/enisa-thematic-landscapes

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

Intepretace článků a příloh MID podle požadavků na softwaru dle MID naleznete v příručce WELMEC Guide 7.2 [1].

7 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

[5] Esche M. and Thiel F.: Software Risk Assessment for Measuring Instruments in Legal Metrology, Federated Conference on Computer Science and Information Systems (FedCSIS), pages 1113 – 1123, DOI: 10.15439/2015F127, ISSN 2300-5963, (2015) https://fedcsis.org/proceedings/2015/pliks/127.pdf, Also available from the WELMEC Library: https://www.welmec.org/welmec/library/

[6] Innovation, European Commission, https://ec.europa.eu/growth/industry/innovation_en

8 Přehled revizí

Ne.	Datum	Významné změny
1	Květen 2019	Průvodce byl vydán poprvé.
2	Květen 2020	• Byla přidána kapitola 4.5 Vzdálené připojení k legálně relevantnímu displeji. • V úvodu kapitoly 4 a v mezních podmínkách 4.2.3 - 4.5.3. byla přidána poznámka vysvětlující odpovědnosti v případě, že části přístroje poskytuje externí poskytovatel služeb.

Tabulka 8-1: Historie revizí