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

WELMEC Guide 7.6

Posouzení rizik softwaru

pro měřicí přístroje

Verze 2021

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

Příručka je určena pro posuzování rizik softwaru a IT měřicích přístrojů podle směrnice o měřicích přístrojích (MID) [1] a směrnice o vahách s neautomatickou činností (NAWID) [2].

Příručka má čistě doporučující charakter a sama o sobě neukládá žádná omezení ani další technické požadavky nad rámec těch, které jsou obsaženy v MID [1] nebo NAWID [2].

Alternativní přístupy mohou být přijatelné, ale pokyny uvedené v tomto dokumentu představují názor WELMEC na správnou praxi, kterou je třeba dodržovat.

Další pracovní skupiny WELMEC mohou pro posouzení rizik stanovit další formální nebo technické požadavky.

Ačkoli je tato příručka zaměřena na nástroje obsažené v předpisech MID [1] a NAWID [2], metoda je obecné povahy a lze ji použít i mimo ně.

Úvod

V rámci posuzování shody měřicích přístrojů podle MID [1] nebo NAWID [2] musí výrobce provést a zdokumentovat posouzení rizik, aby prokázal shodu měřicího přístroje se základními požadavky, viz MID [1] Příloha II, Modul B 3c a NAWID [2] Příloha II, Modul B 1.3c.

Oznámený subjekt je odpovědný za analýzu předloženého posouzení rizik s cílem určit, zda byly dostatečně pokryty všechny základní požadavky.

Tento dokument popisuje metodu posuzování rizik souvisejících se softwarem měřicího přístroje, na který se vztahují směrnice MID [1] a NAWID [2]. Příručka se nezabývá jinými riziky, jako je EMC, zdravotní problémy, riziko úrazu elektrickým proudem atd. Všude, kde se odkazuje na MID [1] nebo WELMEC 7.2 [3], vztahuje se to také na NAWID [2] a WELMEC 7.5 [4], které mají stejné nebo podobné požadavky. V obou případech tato příručka poskytuje metodu pro posouzení rizik specifických pro daný přístroj, zejména pro nové technologie, které nejsou řešeny v dokumentech zavedenými přijatelnými řešeními.

Metoda je určena výrobcům měřicích přístrojů, aby jim pomohla poskytnout odpovídající zprávu o posouzení rizik a oznámeným subjektům, konkrétně oznámeným subjektům podle modulu B, G a H1 směrnice MID [1] a směrnice NAWID [2], aby jim pomohla při úloze analyzovat předloženou zprávu, tj. zda zpráva pokrývá všechny hrozby vůči aktivům která mají být chráněna, a zda jsou navrhovaná opatření ke zmírnění hrozeb přijatelná.

Důrazně se doporučuje, aby hodnocení rizik prováděla skupina lidí s různými odpovědnostmi (například marketing, podpora, návrh, testování atd.).
Podle normy ISO/IEC 27005 [5] je „riziko kombinací důsledků, které by vyplývaly z výskytu nežádoucí události, a pravděpodobnosti výskytu této události.“.
K odhadu rizik spojených se softwarem pro měřicí přístroje jsou proto zapotřebí tři položky:

1. seznam nežádoucích událostí – v případě legální metrologie označovaných také jako hrozby. Hrozby pro aktiva odvozené z příslušných požadavků v MID [1],
2. míra důsledků – označovaná také jako dopad – vyplývající z realizované hrozby a
3. odhad pravděpodobnosti výskytu.

Oddíl 1 uvádí terminologii používanou v této příručce.
Oddíl 2 popisuje obecný pracovní postup metody posuzování rizik softwaru.
Oddíl 3 odvozuje použitelná aktiva z MID [1] a zavádí definice hrozeb.
Oddíl 4 popisuje analýzu rizik z oddílu 3 pomocí elementárních vektorů útoku.
Oddíl 5 uvádí odhadované skóre rizika v kontextu typu měřicího přístroje a oblasti jeho použití
Oddíl 6 uvádí navrhovaný formát zprávy o posouzení rizik.

1 Terminologie

Některé termíny jsou převzaty z norem ISO/IEC 27005:2011 [5], ISO Guide 73:2009 [6] a ISO/IEC Guide 73:2002 [7].

Vektor útoku (Attack vector): technické kroky útočníka k realizaci hrozby.

Strom pravděpodobnosti útoku (Attack Probability Tree – AtPT): grafické znázornění hrozby a souvisejících vektorů útoku, které ukazuje, jak může být útok rozdělen na dílčí cíle/útoky.
POZNÁMKA 1: Úroveň podrobnosti AtPT volí posuzovatel.
POZNÁMKA 2: Dílčí uzly stromu, které se dále nedělí, se označují jako elementární útoky.

Posuzovatel (Assessor): V této příručce se posuzovatelem rozumí osoba/y vybraná/é od výrobce měřicího přístroje, která/é provádí posouzení rizik.

Aktivum (Asset): Cokoli, co má pro organizaci hodnotu, a co proto vyžaduje ochranu [ISO/IEC 27005:2011].
POZNÁMKA: Aktivům je přiřazena jedna nebo více z následujících bezpečnostních vlastností: dostupnost, integrita, autenticita.
POZNÁMKA: Majetkem mohou být vlastnosti měřicích přístrojů, které je třeba chránit.

NAWID: Směrnice o neautomatických vahách, 2014/31/EU EVROPSKÉHO PARLAMENTU A RADY ze dne 26. února 2014 (přepracované znění).

MID: Směrnice o měřicích přístrojích, 2014/32/EU EVROPSKÉHO PARLAMENTU A RADY ze dne 26. února 2014 (přepracované znění).

Analýza rizika (Risk Analysis): Proces, jehož cílem je pochopit povahu rizika a určit jeho úroveň.
POZNÁMKA 1: Analýza rizik je základem pro hodnocení rizik a rozhodování o jejich ošetření.
POZNÁMKA 2: Analýza rizik zahrnuje odhad rizik [ISO/IEC 27005].

Posouzení rizika (Risk Assessment): Celkový proces identifikace, analýzy a vyhodnocení rizik [ISO Guide 73:2009].

Odhad rizika (Risk Estimation): Proces přiřazování hodnot pravděpodobnosti a důsledkům rizika [ISO/IEC Guide 73:2002].

Hodnocení rizika (Risk Evaluation): [ISO Guide 73:2009]: Proces porovnávání výsledků analýzy rizik s kritérii rizika s cílem určit, zda je riziko a/nebo jeho velikost přijatelná nebo tolerovatelná.

Identifikace rizika (Risk Identification): Proces vyhledávání, rozpoznávání a popisování rizik [ISO Guide 73:2009].

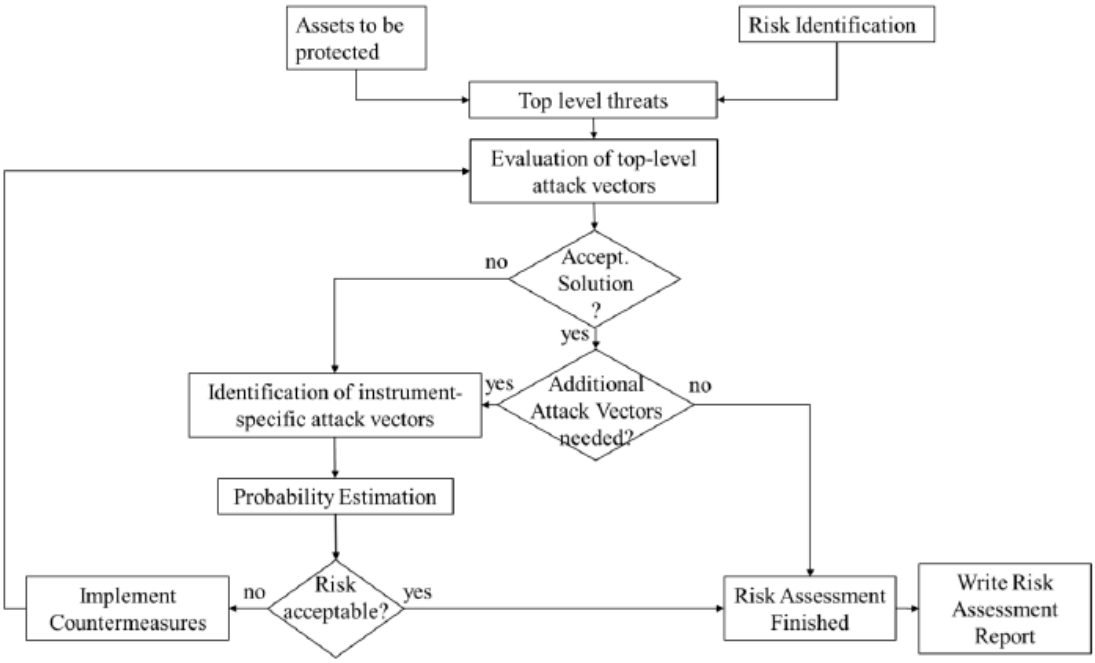
Hrozba (Threat): Nežádoucí událost, která může vést ke znehodnocení jedné nebo více bezpečnostních vlastností aktiva.

2 Pracovní postup posuzování rizik softwaru

Popsaná metoda se řídí rámcem a definicemi uvedenými v normě ISO/IEC 27005 [5], která rozděluje proces posuzování rizik do tří různých fází:

1. Identifikace rizik (viz oddíl 3): Výsledkem tohoto procesu je seznam nežádoucích událostí (hrozeb pro aktiva) odvozených z legálních požadavků MID [1].
2. Analýza rizik (viz oddíl 4): V této fázi se k identifikovaným hrozbám přiřazují kvantitativní nebo kvalitativní úroveň rizika na základě vyhodnocení tzv. vektorů útoku. V závislosti na přiřazené rizikové třídě pro daný typ přístroje (viz příručka WELMEC Guide 7.2 [3]) by měly být zkoumány pouze jednoduché obecné útoky (většina přístrojů rizikové třídy C a nižší) nebo složitější útoky (především rizikové třídy D a vyšší). U komplexních útoků lze k vyhodnocení použít stromy pravděpodobnosti útoků (AtPT).
3. Hodnocení rizik (viz oddíl 5): Riziko se zde vypočítá v kontextu posuzovaného měřidla a jeho předpokládané oblasti použití, aby se určilo, zda je zbytkové riziko (po zmírnění rizika) přijatelné. Riziko se zde vypočítá v kontextu posuzovaného měřicího přístroje a jeho předpokládané oblasti použití, aby se určilo, zda je zbytkové riziko (po zmírnění rizika) přijatelné.

Obrázek 2-1 znázorňuje předpokládaný pracovní postup procedury.



Obrázek 2-1: Pracovní postup procedury pro posouzení rizika.

Posouzení rizik lze provést ve dvou fázích.

1. V první fázi probíhá posouzení rizik s definovanými hrozbami nejvyšší úrovně uvedených v kapitole 3.3.1.
2. Na základě povahy měřicího přístroje nebo jeho rizikové třídy může být nezbytné pro měřicí přístroj definovat specifické vektory útoku, viz kapitola 3.3.4, a provést další posouzení na základě specifických přístrojových vektorů útoku. Je třeba poznamenat, že může být zapotřebí prozkoumat další vektory útoku bez ohledu na rizikovou třídu nástroje.

3 Identifikace rizika

V rozsahu působnosti toho dokumentu jsou všechna rizika spojena s možným neshodou se zásadními požadavky směrnice MID [1].

Poznámka: Požadavky MID [1] musí být splněny, i když riziko, že k události může dojít, je velmi nízké. (např. MID [1] požaduje odpovídající ochranu proti změnám softwaru. Z toho vyplývá, že žádná ochrana nesplňuje základní požadavky.)

Poznámka: Pouhý důkaz o zásahu není adekvátní ochranou proti změnám v softwaru. Software by měl být chráněn proti neúmyslným a úmyslným změnám (bod 8.4 přílohy I MID) a měl by existovat důkaz o zásahu. (MID příloha I bod 8.3) Viz pokyny v příručce WELMEC Guide 7.2 [3] P5, P6 a U5 a U6 (také P5, P6 a U5 a U6 v příručce WELMEC 7.5 [4]).

3.1 Hlavní aktiva

*Požadavky přílohy I v MID [1] jsou podobné požadavkům v příloze I NAWID. [2], viz zejména požadavky 8-10, 14

Č.	**Aktivum**	**Bezpečnostní vlastnosti**	**Požadavek (příloha I, MID [1])***
1	legálně relevantní software	• dostupnost • integrita • autenticita	• 7.1 • 7.2 • 7.6 • 8.3 • 8.4
	identifikace legálně relevantního softwaru	• dostupnost • integrita • autenticita	• 7.6 • 8.3
	důkaz o zásahu do legálně relevantního softwaru	• dostupnost • integrita • autenticita	• 8.2 • 8.3
	adekvátní ochrana legálně relevantního softwaru	• dostupnost	• 8.1
2	Legálně relevantní parametry	• dostupnost • integrita • autenticita	• 7.1 • 8.4
	adekvátní ochrana legálně relevantních parametrů	• dostupnost • integrita • autenticita	• 8.2 • 8.3
	důkaz o zásahu [1]do legálně relevantního softwaru	• dostupnost • integrita • autenticita	• 8.1
3	výsledek měření, včetně relevantních údajů o výsledku měření	• dostupnost • integrita	• 7.1 • 8.4
	Adekvátní ochrana	• dostupnost • integrita	• 8.1

[1] I když důkaz o zásahu není vyžadováv případě ochrany parametrů nebo uložených výsledků o měření, jedná se o typickou formu ochrany, kterou je třeba vzít v úvahu při posouzení integrity parametrů a uložených výsledků měření.

		• autenticita	
4	záznam výsledku měření	• dostupnost • integrita	• 11.1 • 11.2
	Adekvátní ochrana	• dostupnost • integrita • autenticita	• 8.2 • 8.3
	důkaz o zásahu	• dostupnost • integrita • autenticita	• 8.1
5	Označení výsledku měření: Značení Zobrazení výsledku měření: Značení	• dostupnost • integrita • autenticita	• 7.1 • 9 • 10.2 • 7.1 • 10.1 • 10.2 • 10.4
	Adekvátní ochrana	• availability • integrity • authenticity	• 8.1

3.2 Definice hrozby

Hrozby se skládají alespoň z jednoho chráněného aktiva a jednoho odpovídajícího tvrzení, jehož bezpečnostní vlastnost (dostupnost, integrita a/nebo autenticita) může být znehodnocena hrozbou. Teoreticky by pro každé aktivum měla být formulovaná alespoň jedna hrozba.

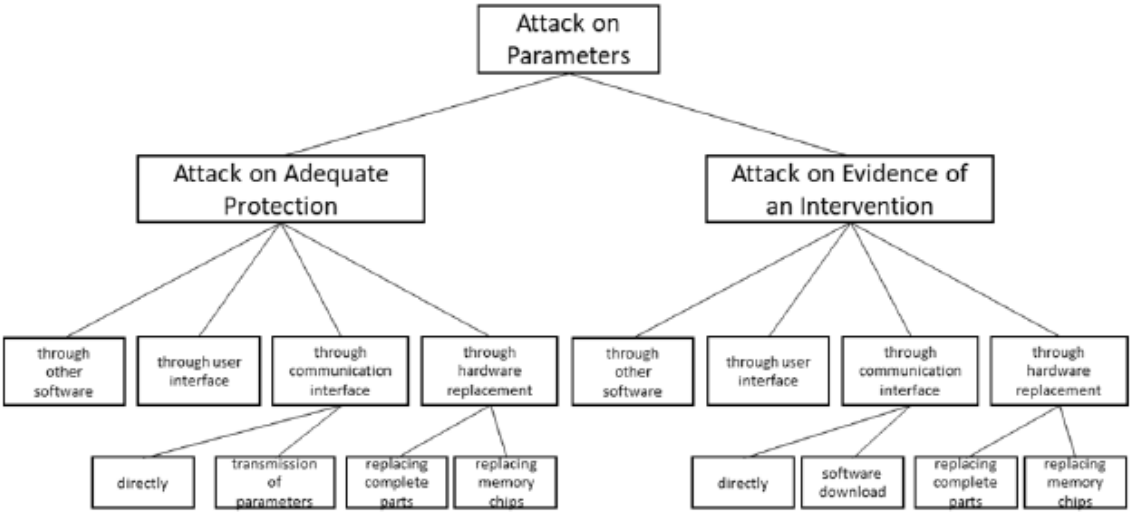
3.3 Obecné hrozby s vektory útoku na vysoké úrovni odvozené z MID

Hlavní aktiva odvozená z MID [1], viz 3.1, jako je software, parametry, výsledek měření, indikace a uložený výsledek, lze převést na obecnou sadu hrozeb s vektory útoku na vysoké úrovni nezávislými na hlavních aktivech, jako je ovlivnění prostřednictvím jiného softwaru nebo prostřednictvím uživatelského rozhraní či komunikačního rozhraní nebo ovlivnění prostřednictvím nahrazení hardwaru nebo softwaru, přičemž se soustředíme pouze na způsob útoku a nerozlišujeme mezi útoky na software, parametry atd.

Každý z těchto vektorů útoku na vysoké úrovni lze rozdělit na alternativní podřízené vektory útoku:

- Pro ovlivnění prostřednictvím komunikačního rozhraní je třeba vzít v úvahu přímé ovlivnění nebo ovlivnění během přenosu.
- U nepřípustného ovlivnění v souvislosti s výměnou hardwaru je třeba vzít v úvahu nepřípustné ovlivnění výměnou (kompletních) dílů, komponentů nebo připojením zařízení k měřicímu přístroji.

Účelem tohoto rozdělení je pomoci definovat kořenový uzel stromu útoku, který představuje cíl a/nebo záměr útočníka, zatímco podřízené uzly jsou upřesněním takového útoku. Listy stromu pak představují elementární útoky, které již nelze víc upřesnit. Jednoduchý příklad je uveden na **obrázku 3-1.**



Obrázek 3-1: Jednoduché znázornění útoků na "parametry" jako chráněné aktivum. Podrobné vysvětlení lze nalézt v [8].

V části 3.4 je popsána implementace prostřednictvím AtPT.

3.3.1 Vektory útoku na vysoké úrovni nezávislé na hlavních aktivech

Č.	Vektor útoku na vysoké úrovni	Požadavek (příloha I, MID [1])
1	nepřípustný vliv na hlavní aktiva* **prostřednictvím jiného softwaru**	• 7.1 • 7.2 • 7.6 • 8.3 • 8.4
2	nepřípustný vliv na hlavní aktiva **prostřednictvím uživatelského rozhraní**	• 7.1 • 7.2 • 8.3 • 8.4
3	nepřípustný vliv na hlavní aktiva **prostřednictvím komunikačního rozhraní**	• 7.1 • 7.2 • 8.1 • 8.3 • 8.4
4	nepřípustný vliv na hlavní aktiva **prostřednictvím nahrazení hardwaru měřicího přístroje**	• 7.1 • 8.2
5	nepřípustný vliv na hlavní aktiva **prostřednictvím nahrazení softwaru**	• 8.3 • 8.4

3.3.2 Dílčí útočné vektory odvozené z kapitoly 3.3.1

S ohledem na to, že komunikační rozhraní neovlivňuje:

Č.	Dílčí vektor útoku	Požadavek (příloha I, MID [1])
1	nepřípustný vliv přímo prostřednictvím komunikačního rozhraní připojením zařízení k měřicímu přístroji	• 7.1 • 7.2 • 7.6 • 8.3 • 8.4
2	nepřípustný vliv při přenosu včetně stahování softwaru	• 7.1 • 7.2 • 8.3 • 8.4

S ohledem na neovlivnění výměnou hardware:

Č.	Dílčí vektor útoku	Požadavek (příloha I, MID [1])
1	nepřípustné vliv prostřednictvím výměny kompletních dílů	• 7.1 • 8.2
2	nepřípustné vliv prostřednictvím výměny komponentů	• 7.1 • 8.2

3.3.3 Shrnutí obecných hrozeb s vektory útoku na vysoké úrovni pro měřicí přístroje

Na základě MID [1] nebo NAWID [2] a příručky WELMEC Guide 7.2 [3] lze definovat následující hrozby nejvyšší úrovně. Patří mezi ně č. 6 z 3.3.1 jako ovlivnění prostřednictvím jiného softwaru a č. 4 jako ovlivnění prostřednictvím komunikačních rozhraní.

Útočník napadne software, parametry, výsledek měření, uložený výsledek nebo indikaci prostřednictvím

- *Jiného software*
- *Uživatelského rozhraní*
- *Komunikační rozhraní*
  - *Přímé ovlivnění připojením zařízení k měřicímu přístroji*
  - *Prostřednictvím přenosu (včetně stahování softwaru)*
- *Připojení zařízení k přístroji*
- *Výměny hardwaru.*
  - *Výměna kompletních dílů*
  - *Výměna komponentů*
- *Výměnou softwaru (pro přístroje typu U*)*

** Poznámka pro posuzovatele: Měřicí přístroje "typu U" nebo "měřicí přístroje používající univerzální počítač" podle WELMEC 7.2 [3]. Další podrobnosti viz WELMEC 7.2.[3]: "Typ U" je blíže vysvětlen v kapitole 5.1 a v kapitole 4.1 jsou popsány přístroje "typu P" neboli " jednoúčelových měřicích přístrojích".*

3.3.4 Specifické útočné vektory pro přístroje

Na základě hlavních hrozeb lze definovat specifické útočné vektory pro přístroje.

Pokud však nelze hlavní hrozbu realizovat, nemusí být nutné definovat specifické útočné vektory pro přístroj.

Na druhou stranu, pokud je přístroj založen na univerzálním počítači nebo jsou některé hardwarové moduly "umístěny v cloudu", může být nutné definovat specifické útočné vektory (i pro přístroje rizikové třídy B nebo C).

Kromě toho extrakce tajných startovních vektorů/klíčů v případě přístroje třídy D nebo E během přenosu je specifickým útočným vektorem, odvozeným od neexistujícího nepřípustného vlivu během přenosu. Měla by být posouzena motivace, vysvětlující, proč specifická rizika/útočné vektory pro přístroj existují či nikoliv.

Poznámky pro posuzovatele:

- *U jednoúčelového měřicího přístroje (viz 3.3.1) rizikové třídy B, který není propojen s jinými přístroji a obsahuje všechny moduly v jednom pouzdře, je vliv na software prostřednictvím uživatelského rozhraní zmírněn, pokud je k dispozici softwarový modul, který přijímá a interpretuje příkazy z uživatelského rozhraní.*
- *Tento softwarový modul předává ostatním legálně relevantním softwarovým modulům pouze povolené příkazy. Všechny neznámé nebo nepovolené sekvence ovládání klíčových spouštěčů nebo tlačítek jsou odmítnuty a nemají žádný vliv na legálně relevantní software, specifické parametry, výsledek měření, uložený výsledek nebo indikaci.*
- *Za předpokladu, že je tento softwarový modul správně implementován, není třeba pro tento měřicí přístroj specifikovat specifické vektory útoku, pokud jde o útoky přes uživatelské rozhraní (viz také kapitola 3.2).*
- *V takovém případě by mělo být ve zprávě o posouzení rizik uvedeno odůvodnění kratšího výběru hrozeb (viz oddíl 6).*

3.4 Hrozby založené na stromu pravděpodobnosti útoku

AtPTs jsou grafickým znázorněním hrozeb a s nimi spojených útočných vektorů, které lze použít k efektivnímu zkoumání složitých hrozeb a útočných vektorů (zejména rizikové třídy D a E). Kořenový uzel útočného stromu představuje cíl a/nebo záměr útočníka, zatímco dílčí uzly jsou dále rozpracovanými variantami takového útoku. Tyto dílčí uzly stromu pak představují elementární útoky, které již nelze dále rozpracovávat. Příklady AtPTs lze najít v [8]. V kontextu tohoto dokumentu se AtPTs používají pro tři různé účely:

• pro grafické znázornění hlavních hrozeb měřicích přístrojů (viz Sekce 3.3.1),

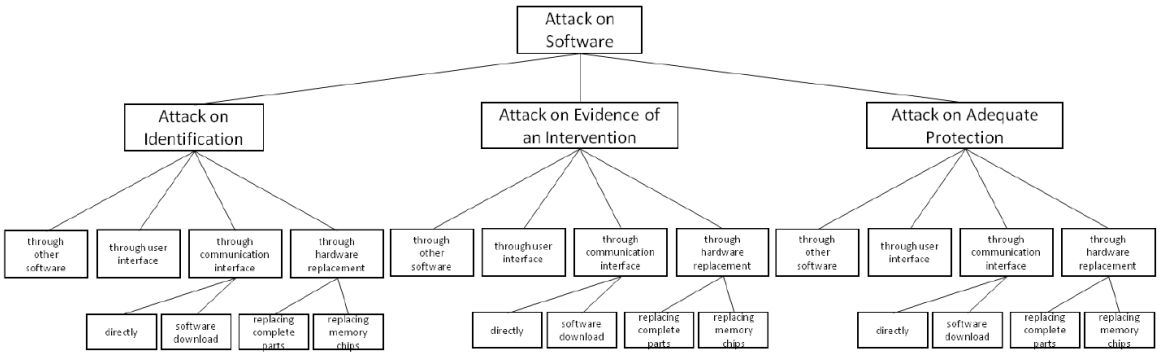
• pro modelování dalších hrozeb při identifikaci vhodných útočných vektorů pro složitější přístroje(viz Sekce 3.3.4),

• pro odhad pravděpodobnosti výskytu složitých útočných vektorů prostřednictvím šíření atributů (viz Sekce 4.2.2)."

3.4.1 Stromy pravděpodobnosti útoku založené na obecných hrozbách s útočnými vektory vyšší úrovně

Všechny následující příklady se vztahují k identifikovaným hlavním aktivům (software, parametry, výsledek měření, uložený výsledek a indikace) z bodu 3.1 a k obecným hrozbám ze Sekce 3.3.1.

3.4.1.1 Útoky na legálně relevantní software

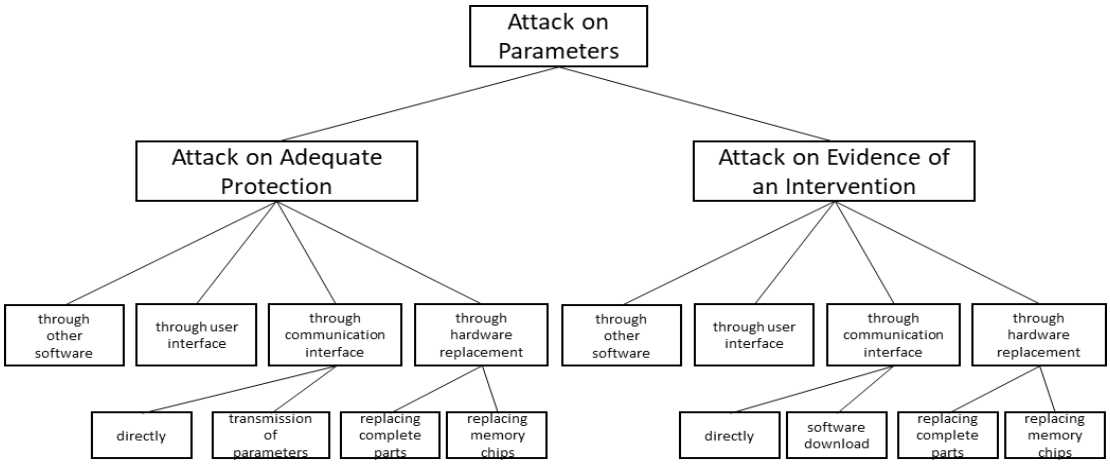


Obrázek 3-2: Obecný AtPT pro hrozby týkající se manipulace s softwarem a jeho odvozenými aktivy.

Útok může mít dopad na identifikaci, důkaz o zásahu nebo obecnou ochranu softwaru během zpracování (nepřípustný dopad).

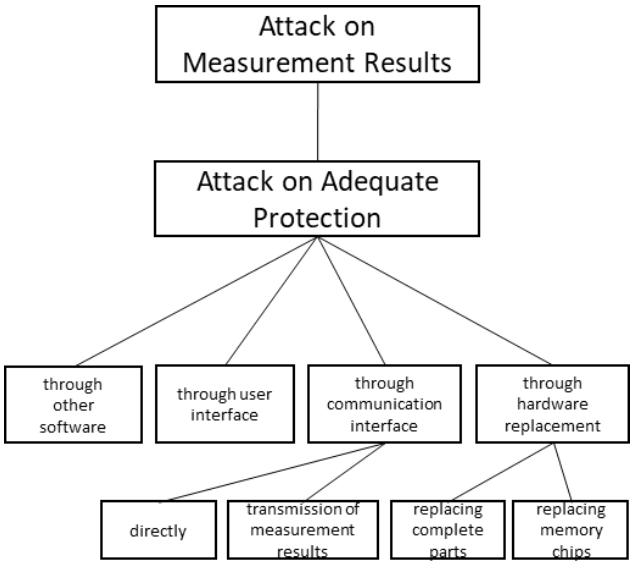
Tři dílčí stromy ukazují (na základě architektury měřicího přístroje z příručky WELMEC 7.2 [3]) jak by mohl být útok proveden bez vstupu do jakýchkoli technických detailů.

3.4.1.2 Útoky na legálně relevantní parametry



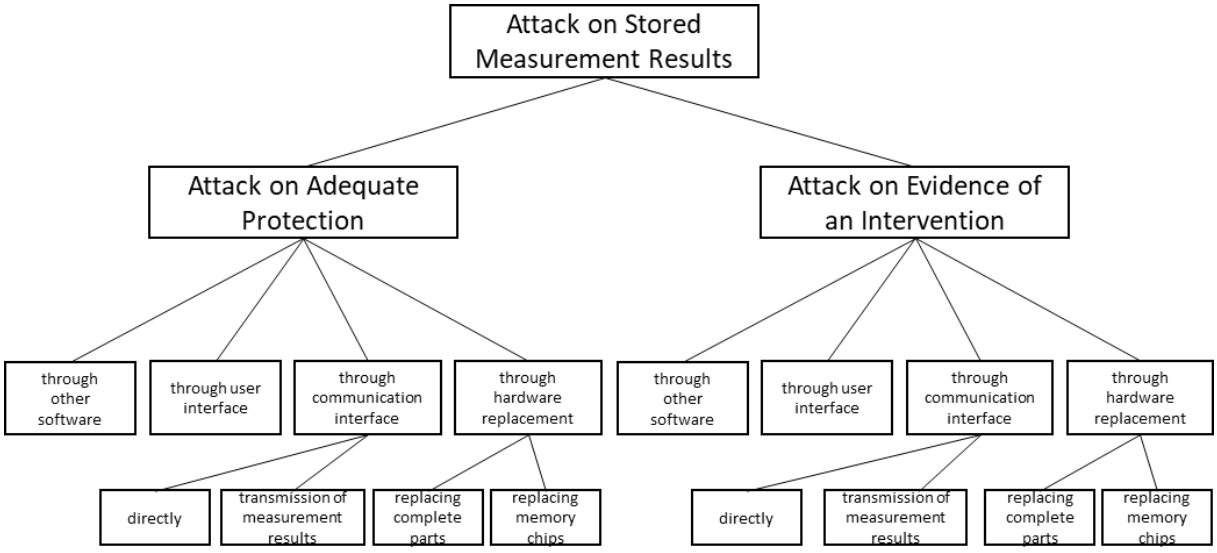
Obrázek 3-3: Obecný AtPT pro hrozby týkající se manipulace s parametry.

3.4.1.3 Útoky na legálně relevantní měřicí výsledky během zpracování



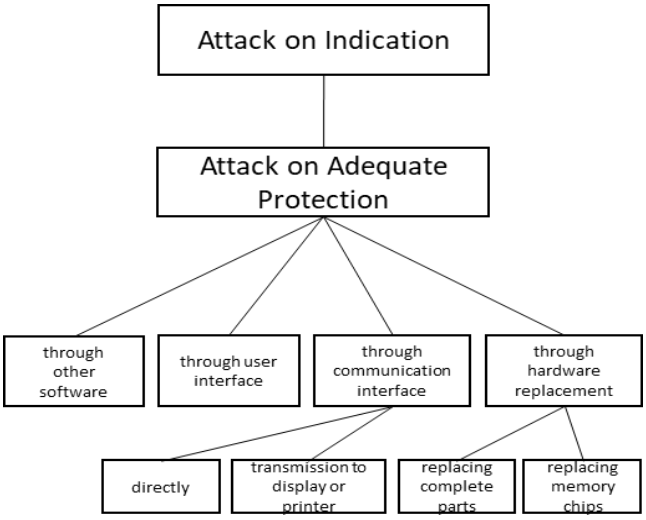
Obrázek 3-4: Obecný AtPT pro hrozby týkající se manipulace s měřicími výsledky.

3.4.1.4 Útoky na uložené výsledky měření



Obrázek 3-5: Obecný AtPT pro hrozby spojené s manipulací uložených výsledků měření.

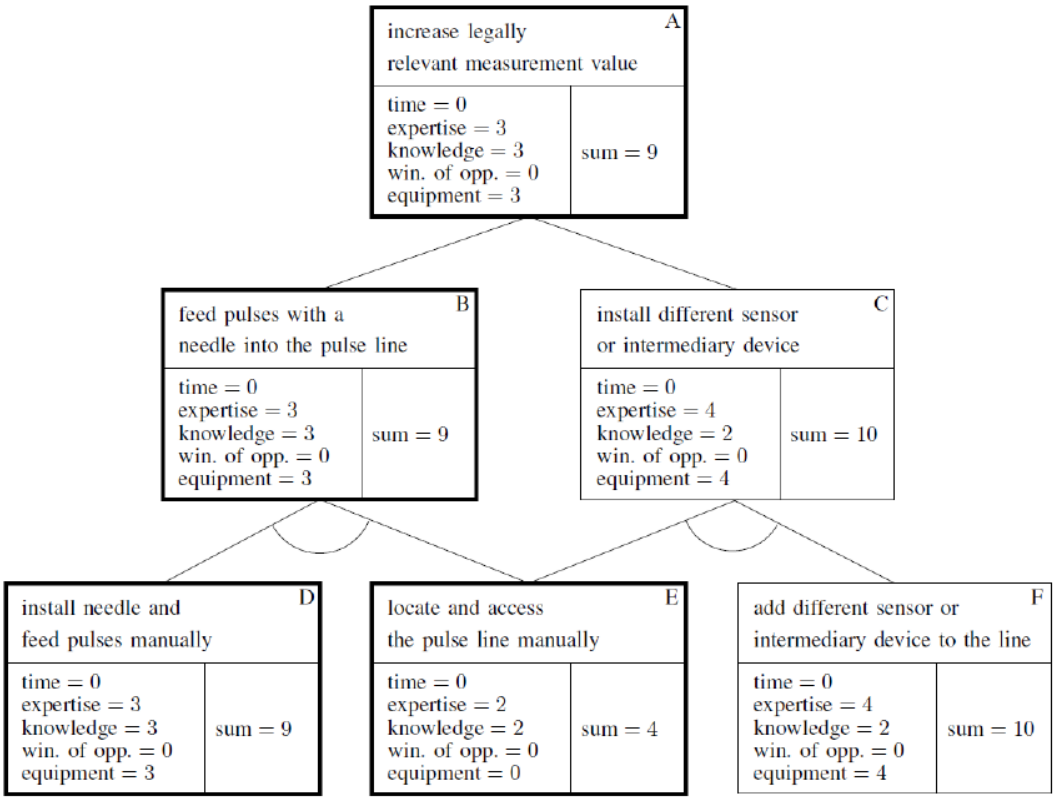
3.4.1.5. Útoky na legálně relevantní indikaci výsledku měření.



Obrázek 3-6: Obecný AtPT pro hrozby týkající se manipulace s legálně relevantní indikací.

3.4.2 Strom pravděpodobnosti útoků na základě specifických vektorů útoků pro přístroj

Specifické hrozby pro přístroj lze znázornit pomocí stromů pravděpodobnosti útoků (viz **Obrázek 3-7**). Tyto hrozby umožňují zkoušejícímu rozdělit určité hrozby na samostatné dílčí cíle v závislosti na vlastnostech přístroje. Aby bylo možné srovnat výsledky hodnocení pro takové hrozby, je důležité plně zdokumentovat příslušné stromy pravděpodobnosti útoků, viz Příloha C.
Následující příklad taxametru je čerpán z [8]. Příklad je podrobně popsán v příloze D.



Obrázek 3-7: Příkladový strom pravděpodobnosti útoků s přiřazenými hodnotami pro všechny uzly pro manipulaci s měřicí hodnotou taxametru narušením analogového signálového traktu. V tomto scénáři existují dva známé vektory útoků: manuální přidávání dalších pulsů do pulsní linky pomocí jehly (uzel (B)) a instalace jiného generátoru pulsů nebo jiného intermediárního zařízení do signálové cesty (uzel (C)). Jelikož jsou tyto dva vektory útoků alternativami vůči sobě, jsou spojeny s mateřským uzlem (A) pomocí OR-spojení vyjádřeného dvěma jednoduchými hranami. Oblouk mezi dvěma nebo více hranami by představoval určité AND-spojení.

4 Analýza rizik: Analýza vektorů útoku

Analýza rizik musí zohlednit konstrukci přístroje.

Pokud se například přístroj skládá ze samostatných modulů a/nebo má v měřicím řetězci zahrnuty periferní přístroje, je třeba riziko vyhodnotit na dvou úrovních:

1. Pro každý samostatný modul[2] nebo periferii;

2. Kompletní přístroj.

Skutečnost, že software jednoho modulu je dostatečně chráněn, neznamená, že je dostatečně chráněn celý přístroj, tj. software ostatních modulů může být chráněn nedostatečně.

Integrita celého přístroje může být ohrožena napadením jednoho modulu nebo rozhraní mezi moduly přístroje.

4.1 Analýza rizik vektorů útoků na nejvyšší úrovni

Posouzení rizik u hrozeb nejvyšší úrovně se skládá ze dvou kroků:

1. Posuzovatel vyřadí všechny elementární vektory útoku z obecných AtPT (viz kapitola 3.4.1), které nejsou použitelné, tj. protože není přítomna adresovaná vlastnost (např. jiný software nebo komunikační rozhraní). Tyto vektory útoku není třeba dále zkoumat.
2. Posuzovatel rovněž zkontroluje, zda jsou zbývající vektory útoku nejvyšší úrovně jsou řádně ošetřeny pomocí protiopatření podle jednoho z přijatelných řešení z příručky WELMEC Guide 7.2 [3]. Tyto vektory útoku se považují za adekvátně zmírněné implementací těchto přijatelných řešení.

Pokud je měřicímu přístroji přiřazena třída rizika C nebo nižší, pokud jsou použita přijatelná řešení uvedená v příručce WELMEC 7.2 a není třeba brát v úvahu žádné další specifické hrozby pro daný přístroj (viz 3.3.4), je analýza rizik dokončena, pokud jsou analyzovány vektory útoku nejvyšší úrovně.

V opačném případě se pravděpodobnost výskytu zbývajících vektorů útoku určí podle metody popsané v kapitole 4.2.

[2] Může být užitečné, aby výrobci modulů a/nebo periférií nechali své zařízení zhodnotit z hlediska rizika v rámci dobrovolného modulárního přístupu, viz příručka WELMEC 8.8 a různé technické příručky pro dobrovolný modulární přístup pro specifické měřicí přístroje na webových stránkách WELMEC.

4.2 Analýza rizik specifických útočných vektorů pro přístroje

4.2.1 Identifikace dalších útočných vektorů.

Tato metoda může být nástrojem k nalezení dalších hrozeb, útočných vektorů a aktiv, vedle těch obecných identifikovaných z MID [1]/NAWID [2] a WELMEC 7.2 [3]. Bez ohledu na rizikovou třídu přístroje musí posuzovatel zvážit, zda existují další útočné vektory, například související s nesnadnou technologií, jako je cloudové připojení nebo distribuovaný přístroj:

1. Pro přístroje, které nepoužívají přijatelné řešení uvedené v příručce WELMEC Guide 7.2 [3], je třeba zvážit specifické útočné vektory pro daný přístroj.
2. U komplexních přístrojů může být nutné zohlednit specifické útočné vektory na přístroj, viz 3.3.4.
3. Pro měřicí přístroje z rizikových tříd D a vyšších je třeba zohlednit složitější útoky kromě těch, které jsou popsány v sekci 3.3.1. Například útoky, které by mohly využívat více než jedno rozhraní (např. kombinace uživatelského rozhraní a komunikačního rozhraní) nebo by mohly záviset na kryptografických útocích na data během přenosu (např. extrakce tajných startovacích vektorů/klíčů).

Pokud se útočné vektory stanou příliš složitými na kompletní zpracování, mohou být AtPTs použity k ilustraci, jaké (jednoduché) elementární útočné vektory lze kombinovat, aby hrozba byla realizována. Využití AtPTs v legální metrologii je vysvětleno podrobně v [8].

4.2.2 Odhad pravděpodobnosti

K odhadu pravděpodobnosti výskytu útočného vektoru se používá metoda nazývaná analýza zranitelnosti podle ISO/IEC 18045 [10]. Analýza spočívá v přiřazení bodového hodnocení útočnému vektoru v pěti různých kategoriích, konkrétně potřebný čas, odbornost a znalost systému, stejně jako příležitost k útoku a speciální vybavení potřebné k provedení útoku.

ID útoku	Popis vektoru útoku	Čas	Odbornost	Znalost systému	Příležitost	Vybavení	Celkem	Dopad	Odůvodnění
Avx1									
Avx2									
Avx3									

Tabulka 4-1: Hodnocení elementárních útočných vektorů.

Každý útočný vektor (AVxy) musí být řádně popsán pro snadné vyhodnocení výsledků posouzení. Na základě tohoto popisu musí být poskytnuto odůvodnění vybraných bodových skóre, aby byla zajištěna objektivnost výsledků. Příklady vyhodnocených útočných vektorů s příslušným odůvodněním bodového skóre jsou uvedeny v příloze D. Každý samostatný kompletní útočný vektor (např. kořenový uzel Stromu pravděpodobnosti útoku) musí mít přiřazeno dopadové skóre, které může být buď 1

pro útoky provedené jednou ovlivňující všechna budoucí (nebo minulá) měření, nebo 1/3, pro útoky, které je třeba opakovat pro každou samostatnou měřicí událost.

Přiřazení vypočítaného souhrnného skóre k pravděpodobnostnímu hodnocení je uvedeno v Tabulce 7-6 v Příloze B. Poté je riziko spojené s každým útočným vektorem vypočítáno násobením hodnoty dopadu a pravděpodobnostního skóre.

Pokud byl k prozkoumání složitého útočného vektoru použit AtPT, pravidla pro výpočet pravděpodobnosti výskytu kořenového uzlu ze skóre vedlejších uzlů jsou uvedena v [8]. Riziko spojené s kořenovým uzlem je pak opět vypočítáno násobením jeho dopadového a pravděpodobnostního skóre.

5 Hodnocení rizik

V posledním kroku hodnocení rizik jsou odhadnutá riziková skóre zasazena do kontextu typu měřicího přístroje. Pro přístroje rizikové třídy C a nižší je skóre nižší než čtyři obvykle přijatelné. Pokud je vypočítané rizikové skóre vyšší, posuzovatel by měl požádat výrobce, aby implementoval dodatečná ochranná opatření a hodnocení opakoval. U rizikových tříd D a vyšších by měl posuzovatel rozhodnout, zda je třeba horní limit pro rizikové skóre nastavit na nižší hodnotu v závislosti na zamýšleném oboru použití.

Pro jednoduché přístroje (obvykle riziková třída C a nižší) není skóre potřebné, pokud všechny útočné vektory mají ochranná opatření dle přijatelného řešení nebo nejsou relevantní a neexistují žádné specifické útočné vektory pro daný přístroj, viz 4.2.1 a schéma na Obrázku 2-1.

5.1 Hodnocení rizika v kontextu účelu měřicího zařízení a příslušné motivace útočníka.

Příručka WELMEC Guide 7.2 [3] uvádí příklady pro některé druhy měřicích zařízení v Rozšíření I. Pro přístroje, které tam nejsou uvedeny a/nebo přístroje s konkrétním účelem, může být použit následující postup, aby byl zohledněn účel daného typu měřicího přístroje:
Vypočtené "Bodové hodnocení rizika" dle kapitoly 4 může být považováno za horní limit a může být sníženo na základě následujících úvah:

Posuďte účel zařízení podle následujících tří hledisek v "Úvahách o hodnocení rizika útočníka":

5.1.1 Výhoda útočníka (AB) – jaká bude výhoda z manipulace? *Attacker's Benefit (AB)*

Přestože útoky "jenom pro radost" samozřejmě nelze zcela vyloučit, stále je větší pravděpodobnost určitého útoku, pokud má útočník z tohoto útoku nějaký prospěch. Toto může být zohledněno následující klasifikace:

	Benefit	Bodové hodnocení
I	Žádné	3
II	Malý finanční prospěch nebo poškození konkurenta	2
III	Střední finanční přínos	1
IV	Vysoký finanční přínos	0

Poznámka: Rozdíl mezi malým a velkým finančním ziskem je jistě poněkud subjektivní. Platí pravidlo: Pokud z toho útočník může získat dostatek peněz na živobytí, mělo by se to považovat za "velký finanční prospěch".

5.1.2 Riziko útočníka být podezřelý (ARS) – jak je zřejmé, kdo má prospěch z manipulace?
Attacker's Risk of being suspected (ARS)

Pokud je pravděpodobné, že bude útočník podezřelý, protože je jedinou osobou, která by měla prospěch z konkrétního útoku, tento útok bude méně pravděpodobný než ten, kde se útočník může skrýt v anonymitě.

	Profitující	Bodové hodnocení
I	Z manipulace by měla prospěch pouze jedna osoba.	3
II	Malá skupina osob (např. zaměstnanci určité společnosti)	2
III	Velká, ale omezená skupina osob	1
IV	Doslova kdokoli	0

Poznámka: Tento aspekt je podobný "Riziku sankce" v příručce WELMEC Guide 5.3, Příloha I, čl. 10.

5.1.3 Riziko útočníka při odhalení (ARC) - jaké by byly důsledky, pokud by byl útočník odhalen?
Attacker's Risk, when getting caught (ARS)

Čím vyšší je potenciální trest za konkrétní manipulaci, tím méně pravděpodobné je, že někdo bude ochoten toto riziko podstoupit.

	Potenciální trest	Bodové hodnocení
I	Dlouhé zatčení	3
II	Krátké zatčení	2
III	Vysoká finanční sankce	1
IV	Nízká finanční sankce	0

Poznámka: Toto hledisko je podobné hledisku "Závažnost sankce" v příručce WELMEC Guide 5.3, příloha I, čl. 11.

5.1.4 Zohlednění motivace útočníka

Bodové hodnocení z 5.1.1 až 5.1.3 může být sečteno, což poskytuje měřítko motivace útočníka s hodnotami od 0 (vysoká motivace) do 9 (nízká motivace). Podle argumentace uvedené v [9] může být tato hodnota brána jako dolní limit pro body pro "odbornost" a "vybavení" pro každý útočný vektor - tj. pokud součet z 5.1.1 do 5.1.3 dává 6, body pro "odbornost" a "vybavení" by neměly být voleny nižší než 6.

6 Zpráva o posouzení rizik

Pro jednoduché přístroje využívající přijatelná řešení lze k zaznamenání výsledků hodnocení rizika použít kontrolní seznam z Přílohy A.

Pro všechny ostatní přístroje je v Příloze C poskytnuta šablona zprávy.

7 Odkazy a literatura

[1] 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

[2] 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

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

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

[5] “ISO/IEC 27005:2011(e) Information technology -Security techniques - Information security risk management”, International Organization for Standardization, Geneva, CH, Standard, June 2011

[6] “ISO Guide 73:2009 Risk management — Vocabulary, Geneva, CH, Standard, November 2009”

[7] “ISO/IEC Guide 73:2002 Risk management — Vocabulary — Guidelines for use in standards, Geneva, CH, Standard, January 2002”

[8] Esche et al. “Representation of Attacker Motivation in Software Risk Assessment Using Attack Probability Trees.” Federated Conference on Computer Science and Information Systems (FedCSIS) 2017 https://annals-csis.org/Volume_11/drp/pdf/112.pdf

[9] Esche, Thiel: “Incorporating a Measure for Attacker Motivation into Software Risk Assessment for Measuring Instruments in Legal Metrology.” 18. GMA/ITG-Fachtagung Sensoren und Messsysteme 2016 https://doi.org/10.5162/sensoren2016/P7.4

[10] “ISO/IEC 18045:2008 Information technology –Security techniques – Methodology for IT security evaluation”, International Organization for Standardization, Geneva, CH, Standard, August 2008

Příloha A Kontrolní seznam

Viz samostatný soubor v Excelu "Annex A_Riskanalysis (version 4).xlsx".

Příloha B Tabulky a příklady

V tabulkách 7-1 až 7-5 jsou uvedeny bodové hodnoty, které se přidělují různým atributům útoku. Vysvětlení, které bodové hodnocení zvolit pro konkrétní případ, lze nalézt ve sloupci poznámky

Uplynulý čas	Body	Poznámky
méně než 1 den	0	Předpokládaný útočník s potřebnými odbornými znalostmi, vědomostmi a vybavením, který má přístup k přístroji, může provést uvažovaný vektor útoku za méně než jeden den.
méně než 1 týden	1	Předpokládaný útočník s potřebnými odbornými znalostmi, znalostmi a vybavením, který má přístup k přístroji, může uvažovaný vektor útoku provést za méně než jeden týden, protože útočník potřebuje připravit jednoduchý skript k provedení útoku nebo provést jednoduché silové vyhledání hesla.
méně než 2 týdny	2	Předpokládaný útočník s potřebnými odbornými znalostmi, vědomostmi a vybavením, který má přístup k přístroji, může uvažovaný vektor útoku provést za méně než dva týdny, protože útočník musí připravit jednoduchý program k provedení útoku nebo provést jednoduché silové vyhledávání hesla.
méně než 1 měsíc	4	Předpokládaný útočník nemá potřebné odborné znalosti, vědomosti nebo vybavení, případně nemá přístup k přístroji a může provést uvažovaný vektor útoku za méně než jeden měsíc, protože útočník potřebuje k provedení útoku připravit středně složitý skript nebo provést středně složité silové vyhledávání hesla.
méně než 2 měsíce	7	Předpokládaný útočník nemá potřebné odborné znalosti, vědomosti nebo vybavení, případně nemá přístup k přístroji a může realizovat uvažovaný vektor útoku za méně než dva měsíce, protože útočník musí připravit středně složitý program k provedení útoku nebo provést středně složité silové vyhledávání hesla.
méně než 3 měsíce	10	Předpokládaný útočník nemá potřebné odborné znalosti, vědomosti nebo vybavení, případně nemá přístup k přístroji a může realizovat předpokládaný vektor útoku za méně než tři měsíce, protože útočník musí připravit středně složitý útok, program k provedení útoku nebo provést středně složité silové vyhledávání hesla.

méně než 4 měsíce	13	Předpokládaný útočník nemá potřebné odborné znalosti, vědomosti nebo vybavení, případně nemá přístup k přístroji a může realizovat zamýšlený vektor útoku za méně než čtyři měsíce, protože útočník musí připravit složitý program, k provedení útoku nebo provést složité silové vyhledávání hesla.
méně než 5 měsíců	15	Předpokládaný útočník nemá potřebné odborné znalosti, vědomosti nebo vybavení, případně nemá přístup k přístroji a může realizovat předpokládaný vektor útoku za méně než čtyři měsíce, protože útočník potřebuje k provedení útoku připravit složitý program a infrastrukturu nebo provést složité silové vyhledávání hesla nebo použít jednoduchý kryptografický klíč.
méně než 6 měsíců	17	Předpokládaný útočník nemá potřebné odborné znalosti, vědomosti nebo vybavení, případně nemá přístup k přístroji a může realizovat předpokládaný vektor útoku za méně než čtyři měsíce, protože útočník potřebuje k provedení útoku připravit složitý program a infrastrukturu nebo provést složité silové vyhledávání hesla nebo použít středně složitý kryptografický klíč.
více než 6 měsíců	19	Předpokládaný útočník bude k provedení útoku potřebovat více než půl roku. To zahrnuje jak kroky provedené na samotném přístroji, tak přípravné práce provedené jinde, protože útočník musí připravit komplexní program a infrastrukturu k provedení útoku infrastrukturu nebo provést složité silové vyhledávání hesla nebo použít složitý kryptografický klíč.

Tabulka 7-1: Bodové hodnocení potřebného času

Odbornost	Body	Poznámky
Laik	0	Co se týče dovedností v oblasti IT, laikem je každý člověk, který je schopen procházet webové stránky pomocí počítače.
Odborník	3	Zkušený uživatel je každý, kdo je schopen najít, nainstalovat a používat specializovaný software (například network sniffer) pro konkrétní úkol.
Expert	6	Každý, kdo je schopen napsat, sestavit a používat specifický software k provedení určitého úkolu, se považuje za experta.
Expert v několika oborech	8	Úroveň odbornosti "expert v několika oborech" by měla být zvolena pouze v případě, že je k provedení útoku zapotřebí odbornost ve více než jedné oblasti (vývoj softwaru, kryptografie, vývoj hardwaru).

Tabulka 7-2: Bodové hodnocení odborných znalostí

Znalost systému	Body	Poznámky
Veřejné	0	Znalosti potřebné k provedení útoku jsou veřejně dostupné. Do této kategorie spadají všechny informace, které lze nalézt vyhledáváním na internetu.
Omezené	3	Příkladem omezených znalostí jsou pouze uživatelské příručky dodávané společně s přístrojem. Takové informace jsou dostupné pouze omezené skupině osob, nikoli veřejnosti.
Důvěrné	7	Informace známé pouze výrobci a autorizovaným osobám. Příkladem důvěrné informace je například nastavení připojení sdílené pouze mezi výrobcem a uživatelem.
Kritické	11	Informace, které jsou známy pouze omezenému počtu zaměstnanců výrobce a případně orgánu posuzování shody, jsou klasifikovány jako "kritické". Do této kategorie by spadalo i heslo stanovené ověřovatelem.

Tabulka 7-3: Bodové hodnocení znalostí systému

Příležitost	Body	Poznámky
Nepotřebný/neomezený přístup	0	Nepotřebný/neomezený přístup znamená, že útočník nepotřebuje mít k provedení útoku přístup k instrukcím nebo že neexistuje žádný riziko odhalení vstupu.
Lehká	1	Přístup se považuje za snadný, pokud je přístup k návodu dosažitelný bez obtíží a pokud musí trvat déle než jeden den.
Mírná	4	Pokud útočník nepotřebuje mít přístup k přístroji po dobu delší než jeden měsíc a pokud je přístup pravděpodobně odhalen, jedná se o mírný přístup.
Obtížná	10	Obtížný přístup znamená, že útočník bude muset k přístroji přistupovat přímo déle než měsíc a jeho odhalení je velmi pravděpodobné.
Žádná	**	Pokud přístup k měřicímu systému není možný z časových důvodů, není třeba vyhodnocovat související scénář útoku.

Tabulka 7-4: Bodové hodnocení pro okno příležitostí

Nástroj/vybavení	Body	Poznámky
Standardní	0	Standardním vybavením se rozumí jakékoli snadno dostupné vybavení, jako je například jakýkoli běžný nástroj v počítači nebo software, který lze volně stáhnout z internetu.
Specializované	4	Pokud je třeba nástroj zakoupit nebo jej lze napsat bez většího úsilí, spadá do kategorie specializovaného vybavení.
Na zakázku	7	Nástroj na zakázku je vysoce sofistikovaný software, který musí být vyvinut speciálně pro účely útoku na přístroj.
Více nástrojů na zakázku	9	Tato úroveň by měla být použita pouze v případě, že je potřeba několik nástrojů na míru pro různé účely (kryptoanalýza, vývoj softwaru atd.).

Tabulka 7-5: Bodové hodnocení vybavení

Součet bodového hodnocení	Skóre pravděpodobnosti	Poznámky
0 - 9	5	Přístroj nenabízí žádnou odolnost proti útokům a útok je velmi pravděpodobný.
10 - 13	4	Přístroj má pouze základní bezpečnostní prvky; je pravděpodobné, že dojde k útoku
14 - 19	3	Bezpečnostní prvky přístroje nabízejí zvýšenou základní ochranu. Útok není příliš pravděpodobný.
20 - 24	2	Přístroj je středně odolný proti útokům a jeho napadení je nepravděpodobné.
>24	1	Bezpečnostní prvky přístroje zajišťují vysokou ochranu proti útokům; útok je velmi nepravděpodobný.

Tabulka 7-6: Zobrazení bodového hodnocení na skóre pravděpodobnosti

Výběr příkladů plně vyhodnocených vektorů útoku je uveden v **tabulce 7-7**.

ID útoku	Vektor útoku	Čas	Odbornost	Znalost systému	Příležitost	Vybavení	Odůvodnění
Př. 1	Útočník správně uhodne čtyřmístné heslo administrátora tak, že vyzkouší libovolné kombinace.	1	0	0	0	0	Předpokládaný útočník: uživatel přístroje. Zadání hesla trvá maximálně 10 sekund, všech 10 000 kombinací lze otestovat za 100 000 sekund = 1,15 dne. Útok může provést každý laik schopný ovládat počítač. Vzhledem k tomu, že útočníkem je uživatel, je příležitost neomezená. Není potřeba žádné speciální vybavení.
Př. 2	Útočník vytvoří falešný výsledek měření ze sad dat měření, které jsou chráněny CRC32 vypočteným pomocí tajného počátečního vektoru.	0	3	3	0	0	Předpokládaný útočník: zákazník Protože CRC je lineární logická operace na binárních vektorech, spojení XOR dvou datových sad automaticky vytvoří třetí datovou sadu se správným CRC. Spojení XOR může vypočítat každý zkušený uživatel pomocí standardního softwaru. Pro získání dvou nebo více datových sad pro zákazníka je příležitost neomezená. Druh kontrolního součtu (CRC32) je popsán v uživatelské příručce.
Př. 3	Útočník vypočítá tajný počáteční vektor CRC32 ze zachycených sad měření, které byly vytvořeny pomocí tajného počátečního vektoru.	1	6	3	4	4	Předpokládaný útočník: zákazník Počáteční vektor CRC32 má délku 32 bitů. Proto existuje 2^32 = 4,3*10^9 možných počátečních vektorů. Každý útočník s programovacími schopnostmi (expert) by mohl během několika hodin napsat program (specializovaný nástroj), který by našel správný startovací vektor metodou hrubé síly. K ověření, zda byl nalezen správný vektor, je potřeba několik tisíc datových sad s kontrolními součty. Jejich získání vyžaduje středně dlouhou dobu. Druh kontrolního součtuv(CRC32) je popsán v uživatelské příručce.

Tabulka 7-7: Příklady vyhodnocených vektorů útoku

Příloha C Struktura zprávy

1) **Stručné shrnutí hodnoceného [typu měřicího přístroje] [název].**

ID	Typ komponenty	Popis
C1	Komunikační rozhraní	
U1	Uživatelské rozhraní	
S1	Ukládání naměřených dat	
X1	Přenos naměřených dat	
P1	Ukládání legálně relevantního softwaru	

Tabulka 1: Seznam datových přenosů, úložišť, uživatelských a komunikačních rozhraní.

2) Kontrolní seznam hrozeb nejvyšší úrovně

Zde se uvede vyplněný kontrolní seznam z přílohy A.

3) Další specifické útočné vektory pro daný přístroj

Zde se uvede vyhodnocená motivace, která vysvětlí, proč je třeba zvážit specifická rizika/vektory útoku pro jednotlivé přístroje, nebo proč je třeba je nezohlednit. V případě, že je třeba zvážit další hrozby specifické pro daný přístroj (viz 3.3.4), vyplní se následující tabulky.

a) Seznam dalších hrozeb, které umožňují vektory útoku specifické pro daný přístroj

ID	Cíl hrozby	Popis
T1		
T2		
T3		

Tabulka 2: Seznam uvažovaných hrozeb.

Poznámka: Cíle (Tx.x) z Přílohy A lze použít jako hrozby pro rizikovou třídu C a nižší.

b) Seznam vyhodnocených útočných vektorů (AVxy), které umožňují hrozbu Tx.

ID útoku	Popis vektoru útoku	Čas	Odbornost	Znalost systému	Příležitost	Vybavení	Celkem	Dopad	Odůvodnění
Avx1									
Avx2									
Avx3									

Tabulka 3: Hodnocení elementárních vektorů útoku.

Pokud je třeba kombinovat elementární vektory útoku pomocí stromu pravděpodobnosti útoku, aby byla naplněna další hrozba, uvedou se zde takové stromy pravděpodobnosti útoku.

c) Seznam pravděpodobnostního skóre, přiřazeného dopadu a konečného rizikového skóre pro každý útočný vektor (AVxy).

ID útoku	Celkem	Skóre pravděpodobnosti	Dopad	Riziko
Avx1				
Avx2				
Avx3				

Tabulka 4: Skóre rizika přiřazené jednotlivým vektorům útoku.

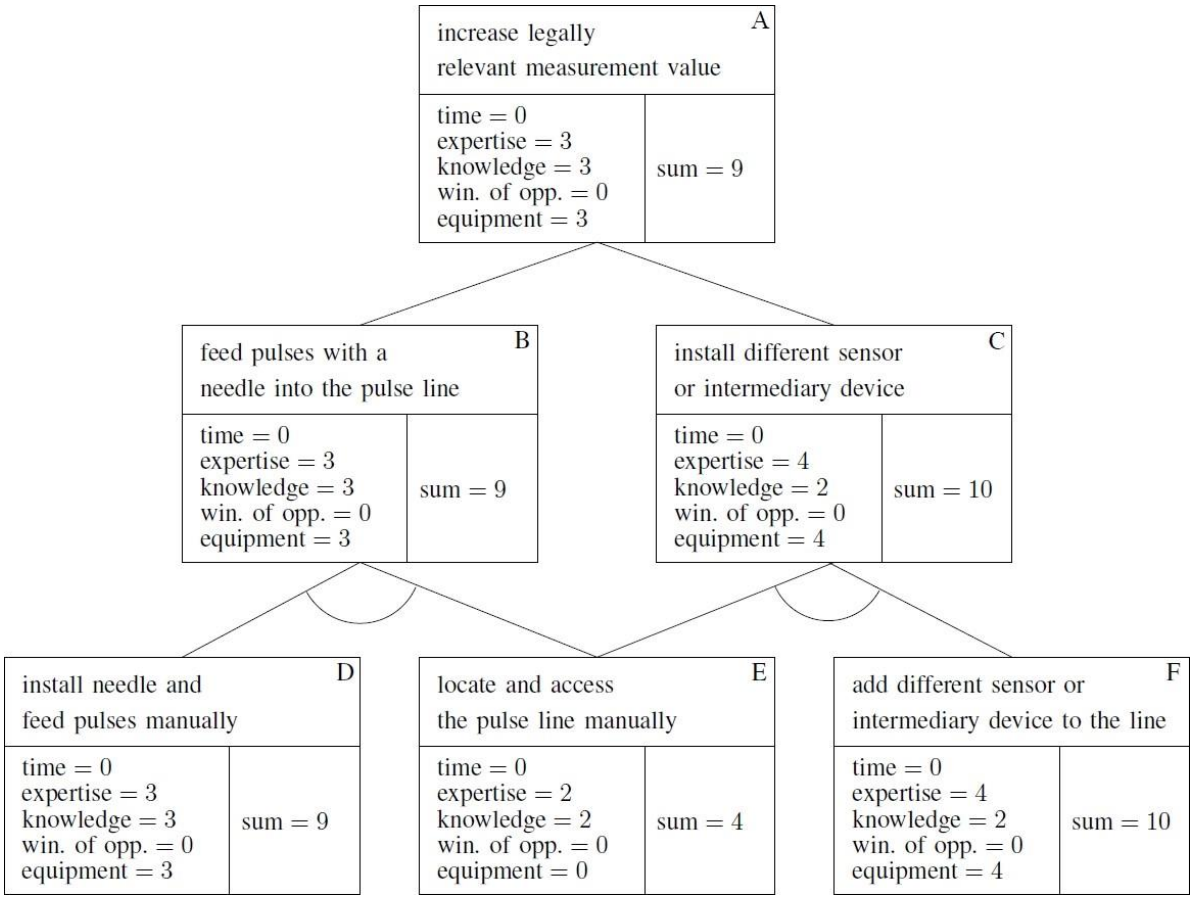
Poznámka: Pravidla pro výpočet celkového skóre, skóre dopadu, skóre pravděpodobnosti a rizika jsou uvedena v kapitole 4.

4) Závěr

Zde se uvede, zda jsou zjištěná rizika pro přístroj přijatelná nebo zda je třeba provést protiopatření.

Příloha D Hodnocení stromů pravděpodobnosti útoku

Nejzákladnější vlastnosti jakéhokoli stromu útoků lze shrnout následovně: Zatímco kořenový uzel takového stromu představuje hlavní cíl útočníka, jeho vedlejší uzly lze považovat za zpřesnění tohoto cíle, která je třeba dosáhnout, aby byl daný cíl splněn. Podle této interpretace základní uzly stromu útoků představují elementární útoky, pro které není možné další zpřesnění. Příklad stromu pravděpodobnosti útoku, který se skládá pouze ze šesti uzlů, je uveden na **obrázku 7-1**.



Obrázek 7-1: Příklad stromu pravděpodobnosti útoku pro taxametr připojený ke generátoru impulzů u kola automobilu pomocí pulzního vedení.

V příkladu jsou znázorněny možné strategie útočníka, jak manipulovat s tarifem vypočítaným taxametrem. Před vysvětlením významu zobrazeného stromu, je nutné vysvětlit specifika jeho grafické reprezentace:

Vedlejší uzly jsou vždy logicky spojeny tak, aby tvořily buď výraz AND (a) nebo OR (nebo). Výraz AND je znázorněn obloukem spojujícím příslušné vedlejší uzly a indikuje, že všechny tyto uzly musí být realizovány k dosažení útoku spojeného s nadřazeným uzlem. Na druhou stranu, pokud vedlejší uzly představují alternativní cesty k dosažení nadřazeného cíle, jsou spojeny výrazem OR, v takovém případě není kreslen žádný oblouk.

Nelze zaručit, že strom útoku bude binární strom. Pokud však identifikujeme více než dva vedlejší uzly, lze je vždy transformovat do binární struktury tak, že kombinujeme

páry těchto uzlů do dílčích cílů, dokud nezůstanou pouze dva vedlejší uzly. Příklad stromu pravděpodobnosti útoku zobrazený na Obrázku 7-1 znázorňuje útoky na analogovou signálovou cestu mezi generátorem impulzů na kole automobilu a taxametrem.

Pro tento scénář existují dva známé vektory útoku:
ruční přidávání dalších impulzů do pulzního vedení pomocí jehly (uzel (B) na Obrázku 7-1) a
instalace jiného generátoru impulzů nebo jiného přidaného zařízení do signálové cesty (uzel (C) na Obrázku 7-1).

Vzhledem k tomu, že tyto dva vektory útoku jsou vzájemnými alternativami, jsou spojeny s nadřazeným uzlem (A) pomocí OR-spojení, což je vyjádřeno dvěma jednoduchými hranami. Oblouk mezi dvěma nebo více hranami by znázorňoval AND-spojení. Taková AND-spojení lze nalézt v další úrovni AtPT. Vkládání impulzů pomocí jehly (uzel (B)) vyžaduje jak přístup k pulznímu vedení (uzel (E)), tak samotné ruční přidávání impulzů (uzel (D)). Pokud má být nainstalován jiný senzor (uzel (C)), je opět vyžadován přístup k pulznímu vedení (uzel (E)). Kromě toho je třeba realizovat samotnou instalaci (uzel (F)). Uzly (E) a (F) jsou opět spojeny AND-spojením. Uzel (E) hraje roli v obou útocích a tedy nabízí možnost fungování jako možný vstupní bod pro protiopatření. Pro výpočet pravděpodobnostního skóre původní hrozby (A) jsou dílčím uzlům (D), (E) a (F) přiřazeny bodové skóre v dříve zmíněných pěti kategoriích. Lze prokázat, že kombinace dvou uzlů do souhrnného uzlu nemá dopad na matematické vlastnosti lokálního podstromu, jako je pravděpodobnost výskytu. Proto je na posuzovateli, aby omezil počet upřesnění útoku, jak uzná za vhodné.

V praxi není potřebné další upřesnění uzlu, pokud příslušný útok představuje jednoduchý technický úkol s známým rozsahem a snadno určitelnými vlastnostmi. Každému uzlu lze přiřadit sadu předem definovaných charakteristik, např. čas, odbornost, znalost systému, příležitost a vybavení jako míra pravděpodobnosti výskytu. Atributy jakéhokoli nadřazeného uzlu lze stanovit kombinací informací spojených s příslušnými vedlejší uzly. Je důležité poznamenat, že neexistuje požadavek, aby jakýkoli uzel existoval v stromu pouze jednou. Místo toho mohou mít uzly více kopií, jejichž atributy jsou propojeny; proto změna v jedné části stromu útoku může ovlivnit i jinak nespojené větve. Výsledné stromy pravděpodobnosti útoku (AtPTs) reprezentují jak logiku útoku, tak pravděpodobnost výskytu (a následně riziko) spojenou s hrozbou. To znamená, že každý útokový vektor již není hodnocen individuálně, ale jsou hodnoceny pouze nejzákladnější útoky na dílčích uzlech. To snižuje možnost nesprávného posouzení útoku a umožňuje znovu použít nejzákladnější útoky pro různé hrozby.

Atributy pro nadřazené uzly, a nakonec pro kořenový uzel, mohou být vypočítány odspodu nahoru dodržením následujících stanovených pravidel. Pro šíření atributů vzhůru ve stromu jsou zavedena řada pravidel specificky upravených pro charakteristiky každého atributu:

- Čas
    - AND: Reprezentace času v bodovém skóre je logaritmická (1 za více než den, 2 za jeden až dva týdny, 19 za půl roku). Sčítání časů pro dvě útoky lze proto aproximovat výběrem maxima z obou.
    - OR: Vybere se časové skóre spojené s menším součtem bodů.

- Odbornost
    - AND: Obvykle se vybírá maximum obou skóre. Pokud je třeba odbornosti v obou oblastech, hardwaru a softwaru (HW a SW), skóre se sčítají s maximální hodnotou 8, viz ISO/IEC 18045 [10].
    - OR: Vybere se skóre odbornosti spojené s menším součtem bodů.

- Znalost systému
    - AND: Vybere se maximum obou skórů znalosti.
    - OR: Vybere se skóre znalosti spojené s menším součtem bodů.

- Příležitost
    - AND: Menší příležitosti (vyšší skóre) pro jeden uzel je relevantním limitem. Proto se vybere maximum.
    - OR: Vybere se skóre příležitosti spojené s menším součtem bodů.

- Vybavení
    - AND: Vybere se maximum obou skórů vybavení, pokud není vyžadováno vybavení z různých oblastí (HW nebo SW), v takovém případě se skóre sčítají s maximální hodnotou 9 dle ISO/IEC 18045 [10].
    - OR: Vybere se skóre vybavení spojené s menším součtem bodů.