WELMEC 7.1
2. izdanje

WELMEC

Evropska saradnja u oblasti zakonske metrologije

Informativni dokument

Razvoj softverskih zahteva

Maj 2005.

WELMEC

Evropska saradnja u oblasti zakonske metrologije

WELMEC je saradnja između službi za zakonsku metrologiju u državama članicama Evropske unije i EFTA. Ovaj dokument pruža osnovne informacije za WELMEC Vodič 7.2 "Vodič za softver (Direktiva o merilima 2004/22/EZ)". Taj vodič je jedan od niza vodiča koje je objavio WELMEC u cilju davanja smernica proizvođačima i imenovanim telima koja su odgovorna za ocenjivanje usaglašenosti njihovih proizvoda. Vodiči imaju čisto savetodavnu ulogu i oni sâmi ne nameću nikakva ograničenja ili dodatne tehničke zahteve mimo onih sadržanih u relevantnim direktivama EZ. Mogu biti prihvatljivi i alternativni pristupi, ali smernice date u ovom dokumentu predstavljaju gledište WELMEC-a u pogledu toga šta smatra najboljom praksom koju treba slediti.

Objavio:
WELMEC Secretariat
BEV
Arltgasse 35
A-1160 Vienna
Austria

Tel: +43 676 8210 3608
Faks: +43 1 49 20 875

E-pošta : welmec@bev.gv.at
Internet stranica: www.welmec.org

INFORMATIVNI DOKUMENT (NA KOJI SE WELMEC 7.2 OSLANJA)
ISPITIVANJE SOFTVERA NA OSNOVU DIREKTIVE O MERILIMA

SADRŽAJ

Predgovor **5**

1 Uvod **6**

1.1 Osnovne informacije i predmet i područje primene 6

1.2 Koncept 6

2 Terminologija **8**

2.1 Programski kôd 8

2.2 Zakonski relevantan softver 8

2.3 Izmene softvera 10

2.3.1 Nenamerne izmene 10

2.3.2 Namerne izmene (oštećenje, zloupotreba) pomoću jednostavnih zajedničkih softverskih alata 10

2.3.3 Namerne izmene (oštećenje, zloupotreba) pomoću specijalnih soficistiranih softverskih alata 10

2.4 Zaštita softvera 11

2.4.1 Zaštićeni softver 11

2.4.2 Praćenje proteklih događaja 11

2.5 Interfejsi 12

2.5.1 Hardverski interfejs 12

2.5.2 Zaštitni interfejs 12

2.5.3 Softverski interfejs 12

2.5.4 Zaštitni softverski interfejs 12

2.6 Zaštita podataka 12

3 Bitni softverski zahtevi **14**

4 Definicija nivoa **16**

4.1 Nivo zaštite softvera 16

4.2 Nivo ispitivanja softvera (Isptivanje tipa ili pregled projekta) 16

4.3 Stepen usaglašenosti softvera 17

5 Tehničke karakteristike merila i mernih sistema **18**

5.1 Hardverska konfiguracija 18

5.2 Korisnički interfejs (komandni) 18

5.3 Učitavanje softvera 18

5.4 Softverska struktura 19
5.5 Softversko okruženje 19
5.6 Otkrivanje defekata 19
5.7 Dugoročno skladištenje mernih vrednosti 19
5.8 Merni princip 19
5.8.1 Vremenska zavisnost 19
5.8.2 Ponovljivost 19
5.8.3 Složenost 19
6 Tumačenje bitnih softverskih zahteva za odabrana merila i merne sisteme 21
6.1 Primer A: Jednostavno samostalno merilo 21
6.1.1 Opis merila 21
6.1.2 Zakonska klasifikacija 22
6.1.3 Tehnička klasifikacija 23
6.1.4 Tumačenje bitnih softverskih zahteva 23
6.2 Primer B: PC-baziran, modularni, složeni merni sistem 29
6.2.2 Zakonska klasifikacija 30
6.2.3 Tehnička klasifikacija 31
6.2.4 Tumačenje bitnih softverskih zahteva 31
7 Reference i ostala literatura 42
8 Revizije ovog dokumenta 44

PREDGOVOR

Svrha ovog revidiranog dokumenta je da pruži informacije o razvoju softverskih zahteva na osnovu Direktive o merilima. Do objavljivanja MID u aprilu 2004. ovaj vodič je u nekim evropskim zemljama korišćen kao osnova za nacionalna odobrenja tipa. Zbog toga je nadležna radna grupa 7 "Softver" na svom 9. sastanku od 8. oktobra 2004. odlučila da ne povuče ovaj vodič već da ga zadrži kao informativni dokument sa ažuriranim unakrsnim upućivanjima na konačni tekst MID i da ga uskladi sa novim WELMEC Vodičem za softver 7.2.

WELMEC 7.1, 2. izdanje se ne koristi za pregled softvera i ispitivanje softvera u merilima iz MID. Umesto njega, WELMEC Vodič 7.2 je preporučeni WELMEC dokument koji treba koristiti za ocenjivanje usaglašenosti softverski kontrolisanih merila u skladu sa MID.

1 Uvod

1.1 Osnovne informacije i predmet i područje primene

Direktiva o merilima (MID) će sadržavati "Bitne zahteve" (Prilog I) za merila koja se koriste u zakonske svrhe. Neki od tih bitnih zahteva mogu se primeniti direktno na softver koji kontroliše ta merila, a druga i na hardver i na softver merila.

Iskustvo u toku razvoja MID pokazuje da se te vrste bitnih zahetva moraju jednoobrazno tumačiti kada je reč o softveru, da bi se izbegao nejednak tretman korisnika od strane raznih evropskih imenovanih tela.

Posle objavljivanja WELMEC Vodiča za softver 7.2, ovaj vodič ima samo informativni karakter. On je revidiran da bi se prilagodio konačnom tekstu MID i rezultatima Evropske mreže za razvoj MID-Softver. U poslednjem poglavlju 8 nalazi se spisak značajnih izmena u odnosu na prethodno izdanje.

Vodič 7.1 (kao i 7.2) nastoji da čitaoca upozna sa činjenicom da ispitivanje samo metrološke performanse merila, ne vodeći računa o softveru koji kontroliše merilo, u mnogim slučajevima nije više adekvatno za savremena, mikroprocesorski kontrolisana merila ili čak merila bazirana na PC, pošto je u suštini softver i njegov integritet to što određuje metrološka svojstva i pouzdanost merila. Pošto ovaj vodič obuhvata vrlo različite kategorije merila, on može dati samo osnove pregleda softvera. Predviđeno je da on bude sukcesivno izmenjen i dopunjen posebnim prilozima za svaku vrstu merila, slično posebnim prilozima sadržanim u MID.

Svrha ovog vodiča je da pruži potporu jedonobraznom isptivanju softvera u Evropi i da rezultate ispitivanja učini procenjivim za proizvođača. Međutim, vodič nije obavezan, čak ni za merila koja MID obuhvata.

1.2 Koncept

Poglavlje 2 ovog vodiča sadrži kratak pregled najosnovnije terminologije koja se koristi.

U poglavlju 3, "Bitni softverski zahtevi" su izvedeni iz MID, Prilog I. Oni su vrlo bliski bitnim zahtevima MID. Za praktične primene, te zahteve je neophodno protumačiti i dalje razraditi uzimajući u obzir zahteve iz posebnih priloga MID za određena merila, razne oblasti primena merila i tehničke aspekte poput hardverske i softverske konfiguracije merila.

Iskustvo u praksi odobrenja tipa pokazuje da se različite vrste merila ne tretiraju jednako u okviru jedne zemlje i da se ista vrsta merila različito tretira u različitim zemljama, bez jasnog objektivnog razloga. Zbog toga su u poglavlju 4 činjenice ili kriterijumi koji formiraju različito ocenjivanje merila identifikovani kao:

- jačina zaštite softvera od promena
- intenzitet ispitivanja softvera kod odobrenja tipa
- stepen usaglašenosti između softvera koji se primenjuje u verifikovanom merilu i odobrenog softvera.

Nivoi tih činjenica i kriterijuma definisani su i dodeljeni grupama/kategorijama merila kao orijentacioni, neobavezujući princip.

Poglavlje 5 opisuje tehničke karakteristike merila i mernih sistema koji se moraju uzeti u obzir kod ispitivanja softvera. Moguće softverske i hardverske konfiguracije predstavljene su kao "slučajevi" koji su kasnije navedeni u poglavlju 6.

U Poglavlju 6 dati su primeri ispitivanja softvera za 2 tipična merila i merna sistema:

- jednostavno samostalno namensko merilo sa zaštitnim interfejsom
- složen, modularni merni sistem baziran na PC

Primeri sadrže opis merila, njihovu zakonsku i tehničku klasifikaciju i tumačenje bitnih softverskih zahteva, zajedno sa primedbama i dodatnim informacijama koje mogu biti korisne za jednoobrazno ispitivanje softvera. Pored toga, detaljno je opisana zahtevana softverska dokumentacija. Međutim, iz gore navedenih razloga vodič još ne sadrži kompletne zbirke detaljnih, posebnih zahteva za merila i primere.

Konačno, Poglavlje 7 sadrži spisak referenci i druge literature koja zainteresovanom čitaocu može biti od pomoći.

2 Terminologija

Važna napomena: U slučaju da termin definisan u ovom poglavlju odstupa od terminologije iz WELMEC Vodiča 7.2 prvenstvo ima taj termin.

2.1 Programski kôd

Izvorni kod. Čitljivi programski kod napisan u ljudima čitljivom obliku, u principu, pomoću uređivača teksta. [14]

Izvršni kôd. Redosled binarnih brojeva koje očitava i tumači centralna procesorska jedinica (CPU). On je ljudima razumljiv samo ako koriste alate kao što su funkcije za otklanjanje grešaka, disasembleri ili rekompilatori. Uređivač teksta je u ove svrhe beskoristan. [14]

2.2 Zakonski relevantan softver

Softver koji realizuje funkcije ili svojstva zakonski kontrolisanog merila kako je definisano u članu 1. MID. Zakonski relevantan softver obuhvata programske delove i podatke koji čine softver koji podleže zakonskoj kontroli.

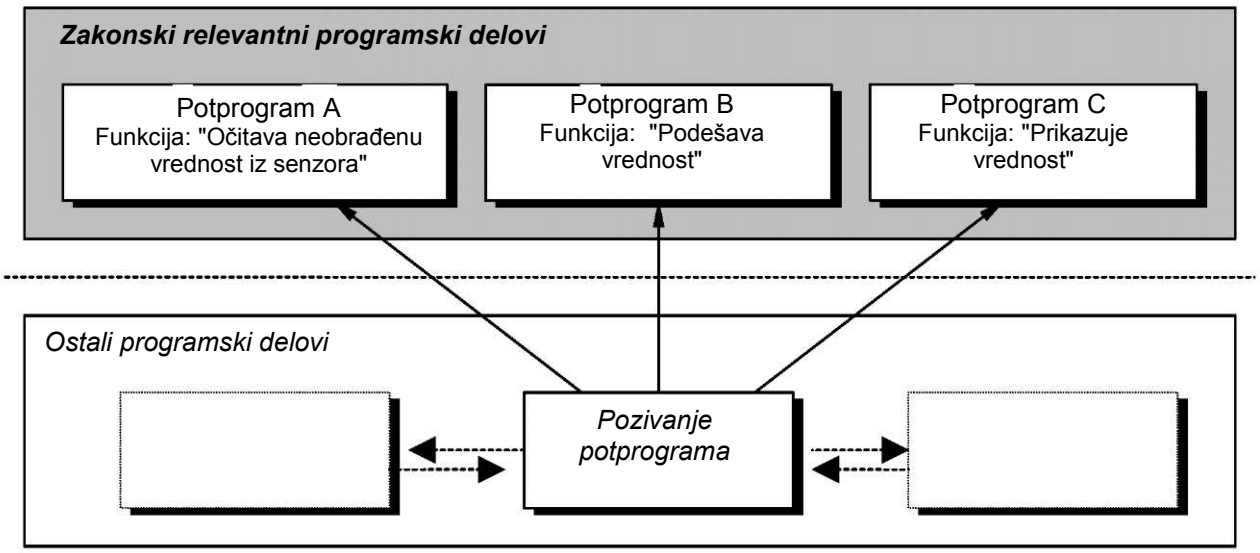
Zakonski relevantni programski delovi

Delovi programskog kôda koji obavljaju funkcije koje podležu zakonskoj kontroli. Slika 2-1 prikazuje relevantne delove programskog sistema koji su realizovan kao potprogrami iznad linije podele. Pored toga, postoje potprogrami ispod linije koji nisu zakonski relevantni. Strelice pokazuju kojeg potprograma poziva neki drugi (vrh strelice) i koji potprogram poziva. Umesto potprograma, komponente programskog kôda mogu se formirati i kompletnim izvršnim programima koji pozivaju jedan drugog preko radnog sistema.

Napomene:

a) *Ova softverska struktura nije propisana ali može imati prednosti (videti 4.3 i tumačenje u 6.1.4. i 6.2.4) Pored toga, tehnički koncept razdvajanja softvera koji je ovde opisan predstavlja poslednju reč tehnike u softverskom inženjeringu, poznatom i kao strukturalno ili modularno programiranje ili objektno orijentisano programiranje i to je inherentni princip kod većine programskih jezika (poput C/C++, Java, Delphi, Visual Basic...).*

b) *Za nivo usaglašenosti "srednji" (videti tačku 4.3) zakonski relevantan programski deo može se sastojati od nepromenljivog dela i ostalih delova. Ti delovi mogu imati različite identifikacije zakonskog softvera .*



Slika 2-1: Jedan primer zakonski relevantnih potprograma koji obavljaju zakonski relevantne funkcije i ostali programski delovi koji su razdvojeni

Zakonski relevantni podaci

Zakonski relevantni podaci mogu se razvrstati u sledeće vrste parametara i podataka:

- ***Parametri specifični za tip*** koji zavise isključivo od posebnog tipa merila. Parametri specifični za tip utvrđuju se prilikom odobrenja tipa merila. U praksi, oni su integrisani u programski kôd.
- ***Parametri specifični za uređaj*** koji zavise isključivo od pojedinačnog uređaja ili merila. Parametri specifični za uređaj obuhvataju ***podešavajuće parametre*** (npr. osetljivost, drugi podešavajući ili korektivni parametri) i druge metrološke parametre kao što su ***parametri za konfiguraciju*** merila (npr. merni opseg, podela skale, merne jedinice).

  Napomena: *Po pravilu,* parametri specifični za *uređaj moraju biti zaštićeni.*
- ***Parametri koji se mogu postaviti*** su podaci koji se unose ručno. Dozvoljeno je da ih korisnik postavi ili izmeni.
- ***Promenljive vrednosti*** obuhvataju ***obrađene merne vrednosti*** koje su pod kontrolom zakonski relevantnih programskih delova (tj. koje su članovi domena podataka takvog programskog dela) i ***konačne merne vrednosti*** kojima se slobodno može pristupiti preko bilo kog softvera. Uz to postoje ***pomoćne varijable*** koje, na primer, sadrže ***komande*** za kontrolu funkcija i toka podataka zakonski relevantnih programskih delova koji realizuju **brojače** za događaje i dr.

Primeri zakonski relevantnih funkcija i podataka navedeni su u Tabeli 2-1.

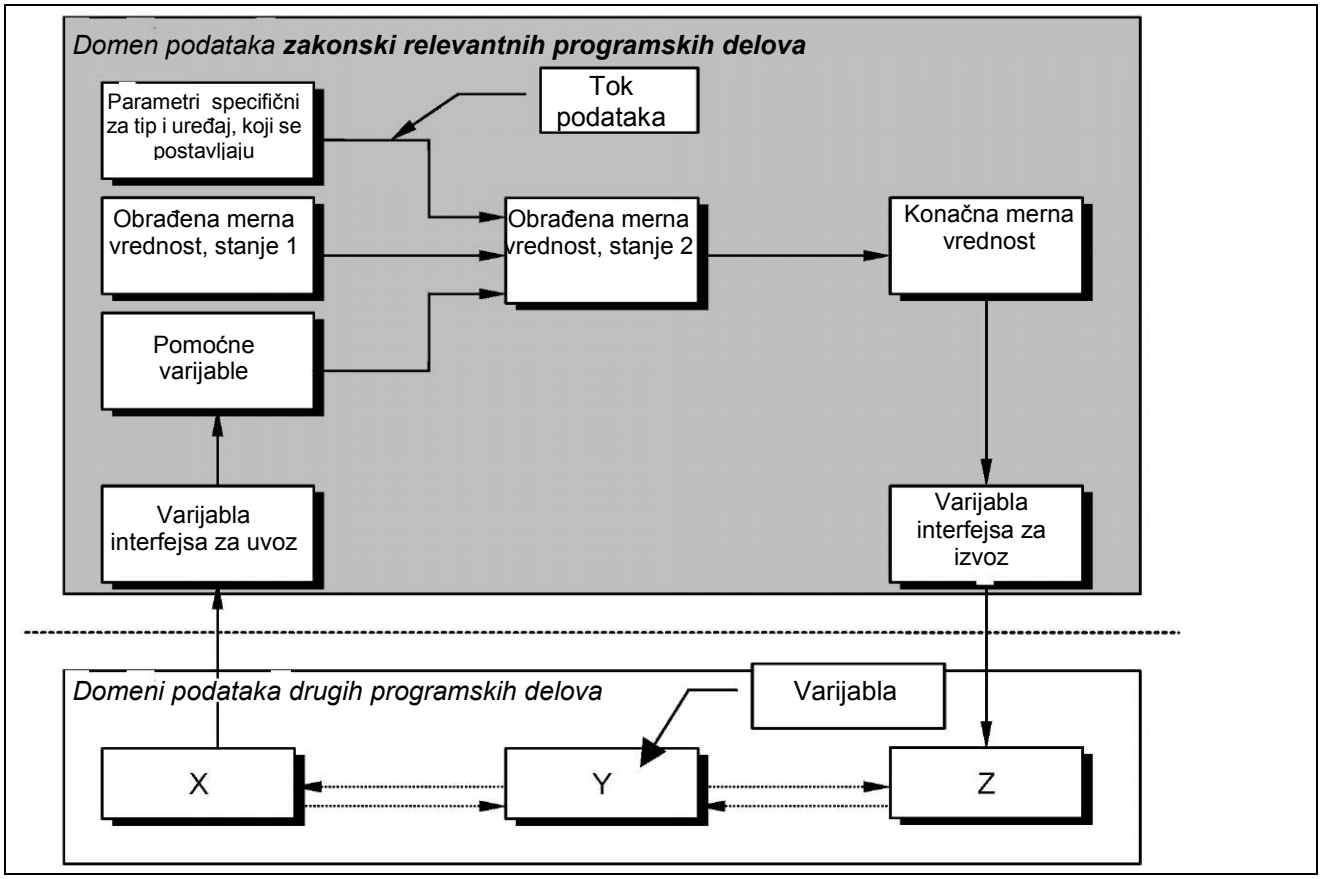
Programi i potprogrami obično imaju *domen podataka.* Domen podataka se sastoji od svih varijabli i konstanti kojima program ili potprogram može pristupiti očitavanjem ili upisivanjem. Ili samo jedan program, potprogram ili objekat poseduje domen i niko drugi ne može da upisuje u njega ili ga čak očitava, ili je domen podataka zajednički sa drugim programskim delovima koji svi imaju dozvolu za očitavanje ili upisivanje.

Slika 2-2 prikazuje domen podataka zakonski relevantnog programskog dela (iznad linije podele) i nekog drugog domena sa nekoliko varijabli koje pripadaju drugim programskim delovima. Spomenuti parametri i varijable pripadaju domenu podataka zakonski relevantnog programskog dela i pristup upisivanju u varijable od strane zakonski relevantnih programa je nemoguć. Samo pristup varijabli uvoznog interfejsa nije ograničen, Strelice pokazuju tok podataka od jednog elementa podataka do drugog.

Napomene:

a) Ako je softver projektovan da bude razdvojen u skladu sa Slikom 2-1, onda se i domeni podataka moraju razdvojiti u one koji podležu zakonskoj kontroli i one koji ne podležu.

b) Dok su podaci – na primer, konačne merne vrednosti – uskladišteni u datotekama ili preneti, oni nisu u okviru domena podataka zakonski relevantnog programa. (U tom slučaju, bitni softverski zahtevi moraju se tumačiti na drugačiji način nego u gore opisanom slučaju, ako će se ti podaci koristiti u zakonske svrhe (videti 5.7 i primer B, 6.2.4, ER2.2)).



Slika 2-2: Jedan primer tipičnog dijagrama toka podataka za softver sa razdvojenim zakonski relevantnim delom sa različitim tipovima parametara i varijablama

2.3 Izmene softvera

2.3.1 Nenamerne izmene

Izmene programskih delova ili podataka, koji podležu zakonskoj kontroli, do kojih dolazi slučajnim fizičkim ili softverskim efektima (pad sistema, zaraženost virusom) ili koje korisnik merila nenamerno vrši.

2.3.2 Namerne izmene (oštećenje, zloupotreba) pomoću jednostavnih zajedničkih softverskih alata

Izmene pomoću softverskih alata i znanja i iskustva (know-how) dostupnih širokoj javnosti. Sve vrste uređivača teksta, na primer, smatraju se jednostavnim zajedničkim softverskim alatom, dok se funkcije za otklanjanje grešaka ili uređivači diska ne smatraju.

2.3.3 Namerne izmene (oštećenje, zloupotreba) pomoću specijalnih soficistiranih softverskih alata

Manipulacija ili simulacija zakonski relevantnog softvera koja se vrši pomoću softverskog alata koji nije dostupan širokoj javnosti i koji zahteva specijalno znanje i iskustvo. Sofisticiranim softverskim alatima smatraju se, na primer, sve vrste funkcija za otklanjanje grešaka, uređivači diskova ili alati za razvoj softvera.

Zakonski relevantna funkcija	***Parametar specifičan za tip***	***Parametar specifičan za uređaj***	***Parametar koji se postavlja***	***Varijable***
Algoritam za izračunavanje konačne merne vrednosti	Korekcije nelinearnosti	Osetljivost	Prethodno postavljena tara	Konačna merna vrednost kako je prikazana
		Merne jednicie		Privremena merna vrednost
		Digitalna rezolucija, verifikacioni podeljak skale		
		Merni opseg (maks. i min. vrednost)		
Analiza stabilnosti merne vrednosti	Vremenska konstanta			Statusni signali (npr. nulto pokazivanje, stabilnost ravnotežnog stanja)
Brojački impulsi za kumulativna merenja		Faktor impulsa		Varijabla brojača
Izračunavanje maksimuma	Dužina bafera	Dužina mernog perioda		Bafer za vrednosti mernih perioda
				Privremena maksimalna vrednost
Programi za samoproveru	Nominalne vrednosti za proveru rezultata[1]		Režim aktivacije: na zahtev/ciklično	Indikatori (OK-FAIL)
Izračunavanje cene za direktnu prodaju stanovništvu			Jedinična cena	Cena za plaćanje
Algoritam za zaokruživanje				Privremena merna vrednost

Tabela 2-1: Primeri zakonski relevantnih funkcija, parametara i podataka.

2.4 Zaštita softvera

2.4.1 Zaštićeni softver

Softer, tj. programski kôd i podaci, čija izmena nije moguća ili je otkrivena i dokazana, npr, žigosanjem ili praćenjem proteklih aktivnosti.

2.4.2 Praćenje proteklih događaja

Softverski brojač i/ili informacioni zapis o izmenama parametara specifičnih za uređaj. Praćenje proteklih događaja može se realizovati, na primer, kao 'brojač događaja' ili kao 'dnevnik događaja':

- **Brojač događaja.** Brojač koji se ne može vratiti na početno stanje (zakonski relevantna varijabla, videti gore), sa po jednim inkrementom svaki put kada se unese poseban režim rada merila i kada se na parametrima specifičnim za uređaj ili drugim zakonski relevantnim podacima izvrši jedna ili više izmena.
- **Dnevnik događaja.** Datoteka koja sadrži niz zapisa od kojih svaki sadrži podatke koji opisuju vrstu i vreme događaja, npr. izmena parametra specifičnog za uređaj, uz identifikaciju parametra koji je izmenjen, vremena i datuma kada je parametar izmenjen i nove vrednosti parametra.

[1] U nekim slučajevima mogu biti specifične za uređaj.

Programski delovi koji izvršavaju evidentiranje događaja i datoteke koje sadrže podatke o događaju smatraju se zakonski relevantnim i moraju se na odgovarajući način zaštititi.

2.5 Interfejsi

2.5.1 Hardverski interfejs

Električni ulaz i/ili izlaz uređaja za razmenu podataka ili signala sa drugim uređajima. To mogu biti merila, moduli (komponente) merila ili periferni uređaji.

Termin 'interfejs' obuhvata sva mehanička, električna i logička svojstva u tački razmene podataka i značenje prenetih podataka i uputstava [5] (ISO 7498).

2.5.2 Zaštitni interfejs

Interfejs se definiše kao zaštitni

- ako se preko tog interfejsa može uticati samo na definisani skup dozvoljenih parametara, podataka i funkcija zakonski relevantnog softverskog dela ili se preko njega taj skup može deblokirati

  i

- ako nije moguće uvesti u merilo (ili modul merila) uputstva ili podatke namenjene ili podesne za:
  - prikazivanje podataka koji nisu jasno definisani i mogu se pomešati sa mernim rezultatom;
  - falsifikovanje prikazanih, obrađenih ili uskladištenih mernih rezultata ili drugih zakonski relevantnih podataka /npr. jedinična cena, cena za plaćanje, merna jedinica u slučaju direktne prodaje stanovništvu);
  - podešavanje ili konfigurisanje merila ili nedozvoljenu izmenu bilo kog parametra specifičnog za tip ili uređaj.
  - zloupotrebu zakonski relevantnog programskog kôda merila.

2.5.3 Softverski interfejs

Ako osim zakonski relevantnih delova softvera postoje i drugi delovi, ti delovi se mogu razdvojiti u smislu da komuniciraju preko softverskog interfesja. Komunikacijski softverski delovi razmenjuju podatke preko određenih varijabli (ili datoteka) kojima imaju oba pristupa (očitavanje ili upisivanje). Te varijable interfejsa i programski kôd koji upisuje podatke u varijable interfejsa ili očitava podatke od varijabli interfejsa, čine softverski interfejs. (Varijable interfejsa odgovaraju redovima hardverskog interfejsa).

Varijable interfejsa mogu se izvršavati, a primer, kao globalne programske varijable, kao funkcijski parametri ili kao datoteke.

2.5.4 Zaštitni softverski interfejs

Softverski interfejs između zakonski relevantnog softverskog dela i drugih softverskih delova, koji se sastoji od varijabli ili datoteka, definiše se kao zaštitni

- ako se preko tog interfejsa može uticati samo na definisani skup dozvoljenih parametara, podataka i funkcija zakonski relevantnog softverskog dela ili se preko njega taj skup može osloboditi
- ako oba dela razmenjuju informacije isključivo preko tog interfejsa, tj, ne preko neke druge veze.

Promenljive i programski kôd zaštitnog softverskog interfejsa deo su zakonski relevantnog softvera.

2.6 Zaštita podataka

Autentifikovani program. Programski kôd u koji korisnik i kupac imaju poverenje (obe strane uključene) koji treba da je identičan sa odobrenim kôdom. Njega ili isporučuje neko ko je ovlašćen i ko je odgovoran da programski kôd bude identičan (ili usaglašen) sa odobrenim kôdom ILI je njegov/njegova identitet/usaglašenost sa odobrenim kôdom (zakonski) verifikovana.

Autentifikovani podaci. Preneti podaci u složenom mernom sistemi čije poreklo primalac može da verifikuje.

ILI

u slučaju mernih vrednosti uskladištenih u memoriji sa javnim pristupom u svrhu kasnije upotrebe: vrednosti koje se mogu jasno pripisati određenom merenju.

Metoda autentifikacije. Metoda kojom se svakom zainteresovanom omogućuje da verifikuje da li su programi ili podaci autentični.
Primer: Generisanje elektronskog potpisa za relevantne podatke ili datoteke od strane autentifikovanog programa pre uskladištenja ili prenošenja. Po prijemu ili očitavanju: ponovno računanje elektronskog potpisa i poređenje rezultata sa nominalnom vrednošću sa autentifikovanim programom koji koristi zainteresovano lice.

Kontrolni zbir. Sabiranje svih bajtova programskog kôda ili skupa podataka. Često se koristi modularno sabiranje da bi se dobio rezultat sa fiksnim brojem cifara.

Ovde se kontrolni zbir često koristi kao ključ za heširanje. Ključ za heširanje je rezultat aritmetičke kombinacije svih bajtova programskog kôda ili skupa podataka. Rezultat algoritma za heširanje obuhvata samo neke bajtove, a algoritam je takav da svaka modifikacija programskog kôda ili podataka sa velikom verovatnoćom dovodi do nekog drugog rezultata.

(Elektronski) potpis. Potpis datoteke (programski kôd ili podaci) generiše se u dva koraka: najpre se izračunava ključ za heširanje (videti gore "kontrolni zbir") a zatim se ključ za heširanje šifruje.[2])

Potpis se po pravilu dodaje programskom kodu ili skupu podataka iz kojih je generisan.

Identifikacija softvera. Metod za verifikovanje autentičnosti i integriteta softvera.

ILI

Više ili niz znakova dodeljenih zakonski relevantnom softveru.[3]

Identifikacija zakonskog softvera. Identifikacija softvera koja je dodeljena zakonski relevantnom softveru.[4]

Jedno prihvatljivo tehničko rešenje za identifikaciju zakonskog softvera je "ABC metoda" koja se sastoji iz tri dela:

- *Deo A* je kôd koji je utvrdio proizvođač merila. Taj deo pokazuje, na njegovu odgovornost, svaku zakonski relevantnu izmenu na softveru.
- *Deo B* se formira algoritmom koji je deo zakonski relevantnog softvera i koji čini broj koji će se automatski promeniti ako je došlo do promene u parametrima specifičnim za uređaj.
- *Deo C* na isti način kao deo B ali sada preko programskog kôda koji je obuhvaćen stvarnim identifikacionim kôdom ABC.

Integritet softvera. Softver je identičan sa tačnom referentnom verzijom (npr. odobrenom verzijom); softver nije izmenjen namerno ili nenamerno.

---

2 Ovde se u nekim slučajevima jednostavno sveobuhvatno rešenje za hešovanje i šifrovanje prihvata kao tehničko rešenje: "ciklična provera redundanse" CRC [11,12] sa tajnom početnom vrednošću.

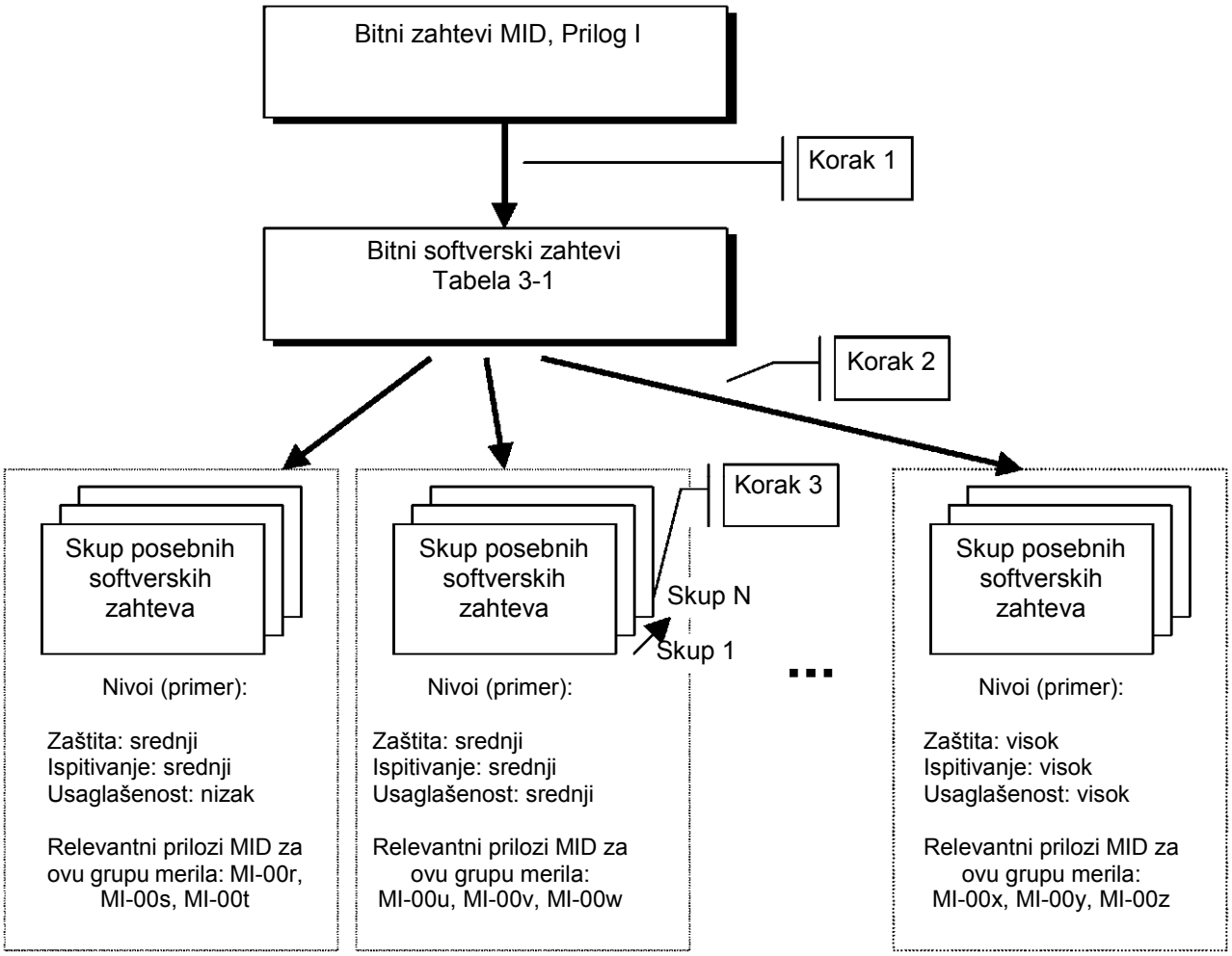
3 To može biti broj verzije softvera.

4 Identifikacija se može razdvojiti u nekoliko delova.

3 Bitni softverski zahtevi

Važna napomena: Softverski zahtevi i koncept opisan u ovom poglavlju u međuvremenu su znatno izmenjeni i ne treba ih primenjivati za Ocenjivanje usaglašenosti u skladu sa MID; milomo vas da pročitate PREDGOVOR ovog vodiča.

Osnovu ovog vodiča čini Direktiva o merilima MID [1]. Prilog I te direktive sadrži bitne zahteve koji su tumačeni vezano za *softver* merila. Rezultat tog tumačenja je 5 predmeta sa 11 *bitnih softverskih zahteva* koji su navedeni u Tabeli 3-1. Ti zahtevi su vrlo opšteg karaktera i za stvarnu praktičnu upotrebu oni se moraju još razraditi. S druge strane, ima mnogo različitih oblasti primene i mnogo mogućih tehničkih rešenja za merila. Da bi se izbeglo definisanje velikog broja detaljnih zahteva koji se primenjuju samo na neko specijalno tehničko rešenje i koji nemaju smisla ili dovode do zabune kod većine drugih primena, za sistem posebno prilagođenih softverskih zahteva odabran je pristup korak po korak.
Prvi korak prikazan je u ovom poglavlju: izvođenje bitnih softverskih zahteva iz zahteva MID (videti sliku 3-1). Naredni koraci su objašnjeni u poglavljima 4 i 5.



Korak 1: Izvođenje bitnih sovftverskih zahteva iz MID.
Korak 2: Definisanje grupa merila za koje se mogu odabrati *isti nivoi ta* tri kriterijuma, zaštite, ispitivanja i usaglašenosti.
Korak 3: Tumačenje bitnih softverskih zahteva za svaku grupu i definisanje skupova 1 do N posebnih softverskih zahteva uzimajući u obzir *tehničke karakteristike.*

Slika 3-1: Izvođenje posebnih softverskih zahteva iz MID (videti poglavlja 4 i 5)

Broj	Bitni softverski zahtevi [5]	Upućivanje na MID član/Prilog I [6]
	Projekat i struktura softvera	
ER1.1	Softver merila mora biti projektovan tako da omogućava lako ocenjivanje usaglašenosti svojih zakonski relevantnih funkcija sa zahtevima ovog vodiča.	AI-12 Article 10
ER1.2	Zakonski relevantan softver mora biti projektovan tako da drugi softver ne utiče na nedozvoljen način na njega .	AI-7.1, AI-7.2, AI-7.6, AI-10.2
ER1.3	Zakonski relevantan softver mora biti projektovan tako da se na njega ne može na nedozvoljen način uticati preko interfejsa uređaja.	AI-7.1, AI-8.1
	Zaštita softvera	
ER2.1	Zakonski relevantni programi i podaci moraju biti zaštićeni od slučajnih ili namernih izmena.	AI-7.1, AI-7.2, AI-8.4
ER2.2	Zakonski relevantni programi i podaci moraju biti zaštićeni od zloupotrebe ili namernih izmena od strane neovlašćenih lica	AI-7.1, AI-8.2, AI-8.3, AI-8.4
ER2.3	U zakonske svrhe dozvoljeno je koristiti samo odobreni i verifikovani softver. Mora biti jasno i nedvosmisleno da prikazivanje rezultata generiše zakonski relevantan program.	AI-7.1, AI-7.2, AI-7.6, AI-8.3, AI-10.2, AI-10.3, AI-10.4
ER2.4	Funkcionalne neispravnosti kojima se mogu falsifikovati merne vrednosti u softverski kontrolisanom hardveru moraju se otkriti što je to više moguće. Kada se otkriju, mora se preduzeti odgovarajuća mera.	AI-6, MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4
	Usaglašenost softvera [7]	
ER3.1	Softver se posle odobrenja tipa ne sme na nedozvoljen način menjati.	Član 20. Prilozi A do H1
ER3.2	Za verifikaciju usaglašenosti na raspolaganju moraju biti identifikacija zakonski relevantnog softvera i odgovarajuća uputstva.	AI-7.6, AI-8.3
	Mogućnost ispitivanja	
ER4.1	Funkcionalnost merila mora se moći ispitati. Napomena: Mogućnost ispitivanja znači da je moguće verifikovati usaglašenost merila sa zahtevima MID i ovog vodiča.	AI-12
	Dokumentacija za odobrenje tipa	
ER5.1	Zakonski relevantan softver, uključujući njegovo softversko i hardversko okruženje, mora biti na odgovarajući način dokumentovan.	AI-9.3, AI-12 član 10.

Tabela 3-1: Bitni softverski zahtevi

---

[5] ***Napomena:*** Ti zahtevi obuhvataju i neke karakteristike hadrvera mernog sistema.

[6] **Upućivanja na Direktivu 2004/22/EZ (MID); AI = MID Prilog I**

Član 10.	Tehnička dokumentacija
Član 20.	Nepropisno stavljene oznake
AI-6	Pouzdanost
AI-7.1, AI-7.2, AI-7.6	Podesnost
AI-8.1, AI-8.2, AI-8.3, AI-8.4	Zaštita od oštećenja
AI-9.3	Informacije koje treba da se nalaze na merilu ili da su uz njega priložene
AI-10.2, AI-10.3, AI-10.4	Pokazivanje rezultata
AI-12	Ocenjivanje usaglašenosti
MI-001-7.1, MI-002-3.1, MI-003-4.3.1, MI-004-4	Posebni zahtevi za merila koja koriste javna preduzeća
Prilozi A do H1	Ocenjivanje usaglašenosti

[7] ***Napomena:*** Ovde se misli na usaglašenost sa odobrenim modelom (softverom) ili primenjivim zahtevima.

4 Definicija nivoa

Iskustvo u praksi odobrenja tipa pokazuje da se različite vrste merila ne tretiraju jednako u okviru jedne zemlje i da se ista vrsta merila različito tretira u različitim državama bez jasno objektivnog razloga. Radna grupa je pokušala da identifikuje činjenice ili kriterijume koji dovode do različitog ocenjivanja merila prilikom odobrenja tipa. Za te činjenice i kriterijume definisana su tri nivoa i radna grupa će odabrati i utvrditi (kao predlog) jedan nivo svake činjenice za određenu vrstu merila ili određeno područje primene i tako harmonizovati odobrenje tipa.

Činjenice i kriterijumi koji imaju uticaja na različit tretman merila u gore opisanom smislu su:

- Jačina ***zaštite*** softvera od izmena
- Intenzitet ***ispitivanja*** softvera kod odobrenja
- *Stepen* ***usaglašenosti*** između softvera primenjenog u verifikovanom merilu i odobrenog softvera.

U ovom poglavlju (4) definisani su nivoi za te činjenice i kriterijume.
Korist od definisanja i utvrđivanja nivoa je ta što je sada moguće jedno sveobuhvatno i dobro utemeljeno tumačenje bitnih softverskih zahteva. To je drugi korak na slici 3-1. U poglavlju 6 detaljno su opisana dva primera za tumačenje.

Pored opisanih činjenica i kriterijuma postoji još jedan apekat koji treba uzeti u obzir: tehničke karakteristike mernog sistema. Zavisno od tih karakteristika, tumačenje bitnih softverskih zahteva mora biti različito po dubini i po načinu. To je treći korak u razvoju posebnih softverskih zahteva prikazanih na slici 3-1. Klasifikacija merila prema njegovim tehničkim karakteristikama razmatra se u poglavlju 5, a u poglavlju 6 učinjen je pokušaj da se to demonstrira pomoću dva primera.

Napomena:

a) Koraci 2 i 3 se sprovode u potpunosti. To je budući posao za stručnjake za razne vrste merila.

b) Iako su definisani nivoi za samo dva predmeta bitnih softverskih zahteva (poglavlje 3), ispostavlja se da se tumačenje bitnih zahteva drugih premeta mora tumačiti prema tim nivoima. Na primer, za visoki nivo zaštite može biti neophodno tumačiti zahtev u pogledu "Projekta i strukture softvera" na način da nije moguće realizovati otvoreni sistem.

4.1 Nivo zaštite softvera

Zaštita softvera podrazumeva adekvatne mere protiv slučajnog ili namernog oštećenja. Nivo zaštite softvera ima uticaja na tehničko rešenje i stoga se odnosi uglavnom na proizvođača, tj. projektanta. Definicija nivoa zaštite daje odgovor na pitanja:

- Koliko jaka mora biti zaštita od zloupotrebe merila?
- Koji se alati koje napadač koristi mogu očekivati?

Definicije nivoa zaštite su:

Nizak: Nisu potrebe posebne mere zaštite od namernih izmena.

Srednji: Softver je zaštićen od namernih izmena, korišćenjem lako dostupnog i jednostavnog zajedničkog softverskog alata (mpr. uređivači teksta):

Visoki: Softver je zaštićen od namernih izmena korišćenjem sofisticiranih softverskih alata (programi za otklanjanje grešaka i uređivači čvrstog diska, alati za razvoj softvera, i dr.).

Napomene:

a) U daljem tekstu definicija različitih nivoa zaštite primenjuje se samo na zaštitu od namernih izmena. Što se tiče nenamernih izmena, nivoi nisu definisani, a bitni softverski zahtevi se tumače i merilo ispituje u skladu sa najnovijim dostignućima u toj oblasti.

b) Ako je to u njegovu korst, proizvođač je slobodan da ispuni zahteve višeg nivoa zaštite od dodeljenog.

c) Uobičajeni metod zaštite/žigosanja, kojim se nedozvoljena intervencija dokazuje, ekvivalentan je sredstvima za zaštitu softvera za srednji i visoki nivo.

4.2 Nivo ispitivanja softvera (Isptivanje tipa ili pregled projekta)

Nivo ispitivanja softvera uglavnom se tiče imenovanog tela odgovornog za odobrenje tipa. Definicija nivoa ispitivanja daje odgovor na pitanja:

- Koji se resursi moraju koristiti za ispitivanje?
- Koja se vrsta ispitivanja mora obaviti?

- Koja je veličina dokumentacije o merilu potrebna za ispitivanje?
- Kakve su posledice po podnosioca zahteva? Definicije nivoa ispitivanja su:

Nizak: Obavlja se standardno funkcionalno ispitivanje tipa merila. Nije potrebno dodatno ispitivanje softvera.

Srednji: Pored niskog nivoa, softver se ispituje na osnovu dokumentacije. Dokumentacija uključuje opis softverskih funkcija, opis parametara i dr. Praktična ispitivanja funkcija koje softver podržava (nasumične provere) mogu se vršiti radi provere prihvatljivosti dokumentacije i efektivnosti mera zaštite.

Visok: Pored srenjeg nivoa, vrši se dubinsko ispitivanje softvera, koje se obično zasniva na izvornom kôdu.

Napomene:

a) Nivo se odnosi samo na dubinu ispitivanja softvera. U svakom slučaju, metrološka svojstva merila ocenjuju se sprovođenjem uobičajenog ispitivanja metrološke performanse.

b) Ako je to povoljnije, proizvođač i imenovano telo se mogu dogovoriti o višem nivou ispitivanja umesto onog koji je dodeljen.

4.3 Stepen usaglašenosti softvera

Stepen usgalašenosti softvera i sposobnost softvera da bude proveren prilikom verifikacije od značaja su za sve uključene strane, tj. za proizvođača, imenovano telo odgovorno za odobrenje tipa i odgovarajuće organe. Problem je za industrijsku proizvodnju merila koja podležu zakonskoj kontroli da relevantne i odobrene karakteristike proizvoda održi neporomenjenim tokom njegovog životnog ciklusa. S jedne strane, vremenom se povećavaju potrebe da se proizvod poboljša ili prilagodi prema datim činjenicama. S druge strane, odobrenje se zasniva na preduslovu da svojstva ostaju konstantna. Sledeća definicija tri nivoa usaglašenosti uzorka i modela pokušava da obuhvati taj spektar. Usaglašenost u tom slislu obuhvata ove aspekte:

- Koje su izmene dozvoljene posle odobrenja tipa ili pregleda projekta bez dopunskog odobrenja?
- Koje izmene podnosilac zahetva mora najaviti imenovanom telu ili ispitivaču?
- Kako se usaglašenost može proveriti?
- Da li je potrebno deponovati odobrenu verziju softvera?

Definicije nivoa usaglašenosti su:

Nizak: Funkcionalnost softvera koji se primenjuje za svako pojedinačno merilo u skladu je sa odobrenom dokumentacijom.

Srednji: Pored nivoa usaglašenosti "nizak", zavisno od tehničkih karakteristika, delovi softvera moraju se kod odobrenja tipa definisati kao nepromenljivi, tj. da se ne mogu menjati bez odobrenja NB. Nepromenljivi delovi moraju biti identični kod svakog pojedinačnog merila.

Visok: Softver koji se primenjuje na pojedinačnim merilima u potpunosti je identičan sa odobrenim softverom.

Napomena: *Ako je to u njegovu korist, proizvođač je slobodan da ispuni zahteve višeg nivoa usaglašenosti od onih koji su određeni.*

5 Tehničke karakteristike merila i mernih sistema

Predviđeno je da ovaj vodič bude primenjiv na sve vrste merila. Kada je reč o zahtevima iz poglavlja 3, ovo je tačno zbog njihove opšte definicije. U praksi su potrebni detaljniji zahtevi, a bitnim softverskim zahtevima je potrebno dodatno tumačenje, u zavisnosti od hardverske i softverske konfiguracije merila ili mernog sistema čiji tip treba odobriti.

U poglavlju 4, definisani su nivoi za tri kriterijuma koji moraju biti ili će biti utvrđena. Za razliku od toga, nije potrebno definisati i utvrditi nivoe za tehničke karakteristike pošto se one mogu objektivno posmatrati i klasifikovati. U daljem tekstu, za klasifikovanje harverske konfiguracije i softverskih karakteristika koje je dodelio proizvođač, predlaže se sistem nekoliko "slučajeva". Različiti "slučajevi" navedeni su u poglavlju 6 u kome je formulisan skup posebnih zahteva (videti takođe treći korak na Slici 3-1). U odeljcima 6.1. i 6.2. navedena su samo dva skupa, ali su oni prilično tipični i mogu služiti kao primeri za dalje skupove zahteva.

Napomena: *Neke tehničke karakteristike, koje su u daljem tesktu opisane, mogu biti neprihvatljive za određena merila odnosno zakonske oblasti primene. Prihvatljive karakteristike biće odabrane naknadno, u specifičnim dodacima za razna merila (biće objavljeno naknadno). Ovde su sadržani samo relevantni skupovi specifičnih zahteva.*

Napomena: *Teorijski je moguć veliki broj skupova posebnih zahteva. Međutim, u praksi je broj zaista različitih harverskih konfiguracija mnogo manji. Većina jednostavnih konfiguracija (videti 6.1) vrlo je slična jedna drugoj i zbog toga je potreban samo mali broj skupova posebnih zahteva.*

5.1 Hardverska konfiguracija

Promenljivost hardvera mernog sistema predstavljena je pomoću 5 osnovnih modela konfiguracije, slučajevi (a) do (e), videti sliku 5-1). Moduli ili uređaji prikazani na toj slici mogu se realizovati kao namenski uređaji – po pravilu slučajevi (a) do (d) – ili kao nenamenski uređaji – po pravilu slučaj (e) – ovi drugi mogu biti lični računari, radne stanice ili čak centralni računari.

5.2 Korisnički interfejs (komandni)

Korisnički komandni interfejs sastoji se od ulaznog medijuma (npr. tastatura, miš) i izlanog medijuma (npr. displej, video monitor ili štampač).

(f) Korisnički komandni interfejs je uvek u radnom režimu koji podleže zakonskoj kontroli.

(g) Korisnički komandni interfejs se može prebaciti sa radnog režima koji podleže zakonskoj kontroli na radni režim koji ne podleže zakonskoj kontroli i obrnuto.
(Na primer, korisnik može zaustaviti merni program, pokrenuti procesor teksta a zatim ponovo pokrenuti merni program.)

(h) Slobodni korisnički komandni interfejs sa radnim režimima koji podležu kontroli i radnim režimima koji ne podležu kontroli, uporedo.
(Na primer, postoji jedan prozor u Windows operativnom sistemu koji predstavlja korisnički interfejs koji podleže kontroli.)

5.3 Učitavanje softvera

(i) Nikakvo učitavanje nije moguće, programi su nepromenljivi (firmer, obično smešten u trajnoj memoriji, np. na neodvojivom, zalemljenom EPROM).

(j) Proizvođač utvrđuje sve programe koji podležu kontroli i sve programe od onih koji ne podležu kontroli koji se mogu učitati. Učitavanje se može realizovati pomoću izmenljivih uređaja za čuvanje podataka (CD-ROM, itd.) ili preuzimanjem sa servera preko interefejsa (na disk, Flash ROM, EEPROM i dr.).

(k) Svaki program se može učitati. Učitavanje se može obaviti pomoću izmenljivih uređaja za čuvanje podataka (disketa, CD-ROM i dr.) ili preuzimanjem sa servera preko inetrefejsa (na disk, Flash ROM, EEPROM i dr.).

5.4 Softverska struktura

(l) Softver podleže zakonskoj kontroli kao celina i nije predviđeno da se nakon odobrenja menja.
(m) Delovi softvera podležu zakonskoj kontroli. Za ostale delove koji nisu zakonski relevantni predviđeno je da se menjaju posle odobrenja.

Videti Sliku 2-1 i Sliku 2-2.

5.5 Softversko okruženje

(o) Softversko okruženje je nepromenljivo. Softver merila je u celini izrađen u merne svrhe.
(p) Softver koji podleže kontroli ugrađen je u okruženje kao i standardni operativni sistem koji nije posebno izrađen u merne svrhe.

5.6 Otkrivanje defekata

(q) Prisustvo defekta je očigledno ili se može jednostavno proveriti ili postoje hardverska sredstva za otkrivanje defekata.

(r) Prisustvo defekta nije očigledno i ne može se jednostavno proveriti pomoću drugih uređaja osim samog merila i nema hardverskih sredstava za otkrivanje defekata.

5.7 Dugoročno skladištenje mernih vrednosti

(s) Nema dugoročnog skladištenja podataka u sistemu.

(t) Merne vrednosti se skladište u sistemu u svrhe kasnije zakonske upotrebe.

5.8 Merni princip

5.8.1 Vremenska zavisnost

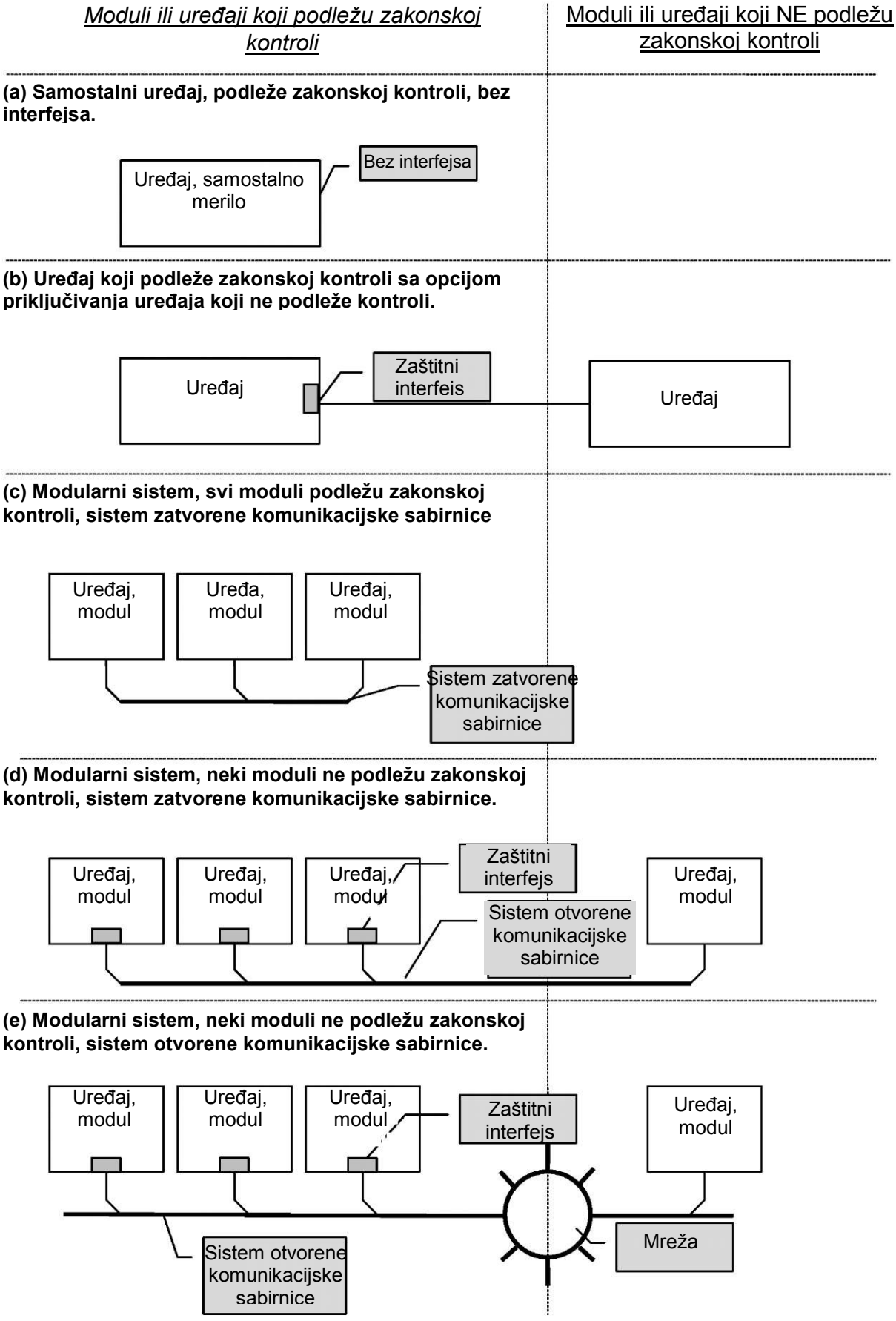
(u) Kumulativno merenje (npr. brojilo, agregat za istakanje goriva)
(v) Pojedinačno nezavisno merenje

5.8.2 Ponovljivost

(w) Ponovljivo merenje
(x) Neponovljivo merenje

5.8.3 Složenost

(y) Jednostavno, direktno ili statičko merenje
(z) Složeno ili dinamičko merenje



Slika 5-1: Primer mogućih hadrverskih konfiguracija mikroprocesorski kontrolisanih i na PC baziranih merila i mernih sistema

6 Tumačenje bitnih softverskih zahteva za odabrana merila i merne sisteme

Koncept predloga čini pristup korak po korak. Posle primene nivoa zaštite, isptivanja i usaglašenosti sa tipovima merila i njihovim oblastima primene (videti poglavlje 4), za svaku oblast primene i svako merilo mora se definisati skup posebnih zahteva koji uzimaju u obzir razna tehnička svojstva merila. Kod svakog ispitivanja, ispitivač mora odabrati pravi skup posebnih zahteva za merilo, u zavisnosti od tehničkih karaktersika koje treba da ispita.

Da bi se ilustrovalo šta tumačenje bitnih softverskih zahteva podrazumeva (videti 3, skraćenica *ER),* u tekstu koji sledi govori se o dva primera tehničke realizacije mernih sistema. To nije zamena za celokupan skup posebnih priloga za svaku vrstu merila koji će se naknadno objaviti. Međutim, predviđeno je da se izborom tih primera već obuhvati veliki deo spektra mogućih tehničkih rešenja.

U ovom odeljku, softver primernih sistema klasifikuje se prema poglavljima 4 i 5, tj. prikazani su tehnički uticaji i netehnički uslovi za tumačenje bitnih softverskih zahteva (klasifikacija softvera). Kod netehničkih uslova, misli se na nivoe zaštite, ispitivanja i usaglašenosti (4.1 do 4.3).

Primeri su

A) jednostavno samostalno merilo, realizovano kao namenski uređaj sa svim komponentama unutar kućišta i

B) složeni merni sistem baziran na PC sa raznim komponentama priključenim na mrežu.

Napomena: *Do sada, vrstama merila i njihovim oblastima primene nisu dodeljeni određeni nivoi netehničkih uslova (nivo zaštite, nivo ispitivanja, nivo usaglašenosti). Zbog toga se u daljem tekstu govori o* ***svim*** *nivoima čak i ako je tumačenje određenog opšteg zahteva pod nekim uslovima samo hipotetičko. Tako će biti lakše definisati nivoe za svaku vrstu merila i svaku oblast primene.*

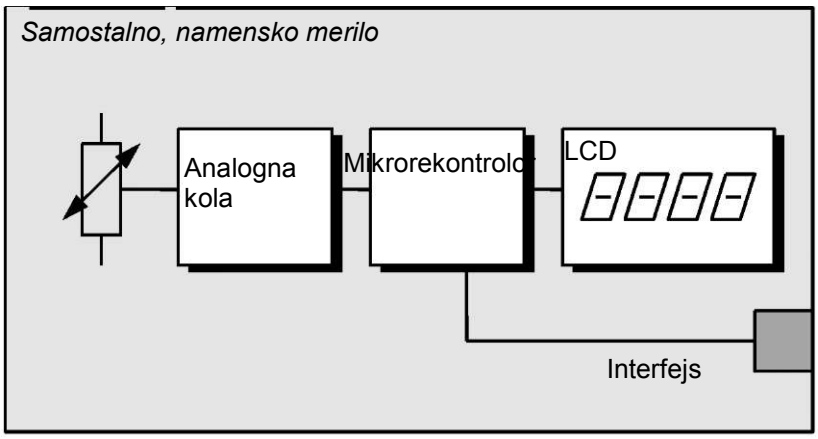
6.1 Primer A: Jednostavno samostalno merilo

U principu, ovaj primer važi za mnoštvo merila koja se koriste za komercijalne transakcije kao što su mesta za punjenje goriva, taksimetri i dr.

6.1.1 Opis merila

Recimo da je jednostavno samostalno merilo namensko merilo. Merilo karakterišu sledeća opšta tehnička svojstva (Slika 6-1):

- *Zatvoreno kućište. Sve komponente merila nalaze se unutar kućišta, žigosanje moguće.*
- *Merilo se sastoji od senzora (pretvarač, uključujući analognu elektroniku), analognih komponenti (npr. A/D pretvarač), mikroprocesorska ploča i LC displej.*
- *Uređaj ima hardverski interfejs koji je predviđen za priključivanje perifernog uređaja koji ne podleže zakonskoj kontroli.*
- *Softver se skladišti u trajnoj memoriji (neodvojivi Flash ROM, EEPROM, EPROM ili PROM).*
- *Celokupan softver nije predviđen za izmene nakon odobrenja tipa. Nema softverskog razdvajanja zakonski relevantnih programskih delova i drugih delova koji se realizuju.*
- *Otkrivanje defekata: izračunavanje kontrolnog zbira preko memorijskih sadržaja.*



Slika 6-1: *Primer A* – Jednostavno samostalno merilo

6.1.2 Zakonska klasifikacija

Po pravilu, zakonska klasifikacija bi sledila Tabelu A-1 iz Priloga 1. Pošto nivoi još nisu odabrani, u sledećim tumačenjima u obzir se uzimaju ***svi*** nivoi za "zaštitu, ispitivanje i usaglašenost".

Napomena: Da bi tumačenja i primedbe bili uporedivi sa primerom B (videti 6.2), prema predlogu za kategoriju "Merila koja se koriste za komercijalne transakcije" odabrani su sledeći slučajevi (videti Tabelu A-1):

Nivo zaštite softvera: ***srednji***

Nivo ispitivanja softvera: ***srednji***

Stepen usaglašenosti softvera: ***nizak***

Ti nivoi i rezultirajuća tumačenja označeni su u odeljku 6.1 sivom pozadinom kakva je i pozadina ove napomene.

6.1.3 Tehnička klasifikacija

Prema poglavlju 5 merilo se može klasifikovati kako sledi:

Karakteristika	Slučaj	Objašnjenje
Hardverska konfiguracija	*b*	Uređaj koji podleže zakonskoj kontroli sa opcijom priključivanja uređaja koji ne podleže kontroli.
Korisnički interfejs (komandni)	*f*	Korisnički komandni interfejs je uvek u radnom režimu koji podleže zakonskoj kontroli.
Učitavanje softvera	*i*	Nikakvo učitavanje nije moguće, programi su nepromenljivi (firmver, obično uskladišten u trajnoj memoriji).
Softverska struktura	*l*	Celokupan softver podleže zakonskoj kontroli i nije predviđeno da se menja posle odobrenja tipa.
Softversko okruženje	*o*	Softversko okruženje je nepromenljivo. Softver merila je u celini izrađen u merne svrhe.
Otkrivanje defekata	*r*	Prisustvo defekta nije očigledno i ne može se jednostavno proveriti pomoću drugih uređaja osim samog merila i nema hardverskih sredstava za otkrivanje defekata.
Dugoročno skladištenje mernih vrednosti	*s*	Nema dugoročnog skladištenja podataka u sistemu.
Merni princip	*v, w, y*	Pojedinačno nezavisno, ponovljivo, jednostavno i statičko merenje.

U narednim odeljcima slučajevi su jednostavno skraćeni, na primer, (b).

6.1.4 Tumačenje bitnih softverskih zahteva

ER1.1: Softver merila se mora projektovati tako da omogućava lako ocenjivanje njegove usaglašenosti sa zahtevima ovog vodiča.

U ovom primeru jednostavnog samostalnog merila proizvođač softvera ne namerava da menja softver nakon odobrenja tipa (l)[8l)]. U tom slučaju projekat ili struktura softvera (razdvojenog ili ne) nisu važni za ciljeve isptivanja tipa. Za ER1.1 nije potrebno dalje tumačenje.

Primedbe u pogledu nivoa ispitivanja:

Pošto projekat ili struktura softvera iz ovog primera nisu relevantni za ispitivanja o kojima je u nastavku reč, nema potrebe za njihovim ispitivanjem na bilo kom nivou.

ER1.2: Zakonski relevantan softver mora biti projektovan tako da drugi softver ne utiče na njega na nedozvoljen način.

Ovaj zahtev se zadovoljava nezavisno od softverske strukture, zbog toga što, osim zakonski relevantnog softera na merilu, ne postoji nijedan drugi softver (I, o)[9o)] i softver se ne može učitati (i)[10i)].

---

[8] l) Celokupan softver podleže zakonskoj kontroli i nije predviđeno da se menja posle odobrenja tipa.

[9] o) Softversko okruženje je nepromenljivo. Softver merila je u celini izrađen u merne svrhe.

Primedbe u pogledu nivoa ispitivanja:

Pošto osim zakonski relevantnog softvera ne postoji nijedan drugi softver, prepostavlja se da su uobičajena metrološka ispitivanja merila dovoljna za ocenjivanje softvera i da nije potrebno nikakvo dodatno ispitivanje softvera u pogledu njegove strukture čak i ako su nivoi *srednji* ili *visok* predviđeni.

Primedbe u pogledu nivoa usaglašenosti :

Softverska struktura ima uticaj na pouzdanost usaglašenosti u toku životnog ciklusa softvera. Kod jednostavne konfiguracije iz ovog primera (i, I, o), za ER1.2 nije potrebno dalje tumačenje. Međutim, ER3.1 se mora uzeti u obzir.

ER1.3: Zakonski relevantan softver mora biti projektovan tako da se na njega ne može uticati preko interfejsa uređaja.

U ovom primeru uređaj ima interfejs (b)[11b)], i može se priključiti svaki uređaj koji ne podleže zakonskoj kontroli. Ako se može dokazati da je interfejs zaštitni, nije potrebno žigosati ga.

Primedbe u pogledu nivoa zaštite:

Nizak: Interfejs nije potrebno žigosati, čak i ako nije dokazano da je zaštitni.

Primedbe u pogledu nivoa ispitivanja*:*

Nizak:	Proizvođač izjavljuje da je interfejs zaštitni, tj. da ni na merne vrednosti ni na funkcije merila ne mogu uticati komande ili podaci koji se posredstvom interfejsa prenose na merilo. U ovom slučaju ne vrši se nikakvo posebno istivanje softvera interfejsa.
Srednji:	Proizvođač isporučuje kompletan opis komandi i parametara koje dobija preko zaštitnog interfejsa, uključujući izjavu o kompletnosti tog opisa. Pri ovom ispitivanju mora se verifikovati, na osnovu te dokumentacije, da podaci primljeni preko interfejsa ne utiču na nedozvoljen način na merilo.
Visok:	Mora se verifikovati na osnovu izvornog kôda da nijedan od podataka dobijenih preko interfejsa ne utiče na nedozvoljen način na merilo.

ER2.1: Zakonski relevantni programi i podaci moraju biti zaštićeni od slučajnih ili nenamernih izmena.

Postoje dva razloga za nedozvoljene izmene: fizički efekti i pogrešno rukovanje od strane korisnika. Ako se merilo ispituje prema propisima u pitanju (EMC, temperatura, vlažnost i dr.), slučajne izmene podataka ili programa ne treba uzimati u obzir. Što se tiče pogrešnog rukovanja od strane korisnika, korisnički interfejs je u ovom primeru uvek u radnom režimu koji podleže zakonskoj kontroli, a softver koji podleže zakonskoj kontroli je izdvojen (f, I, o)[12f)]. nenamerne izmene mogu nastati samo zbog nedozvoljenih svojstava softvera koji podleže zakonskoj kontroli (npr. ne sme biti moguće nenamerno izmeniti parametre specifične za uređaj).

Primedbe u pogledu nivoa zaštite:

Nivo zaštite u smislu koji se ovde koristi odnosi se na *nenamerne* manipulacije (videti ER2.2).

Primedbe u pogledu nivoa ispitivanja:

Nizak:	Rukovanje merilom mora se praktično ispitati uz pomoć radnog priručnika.
Srednji*:*	Pored praktičnih ispitivanja, ispravnost i konzistentnost rukovanja merilom analizira se na osnovu dokumentacije (radni priručnik i posebna softverska dokumentacij).
Visok:	Pored spomenutih ispitvanja, mora se ispitati izvorni kôd softvera da bi se proverilo da li su nepravilnosti u radu moguće.

ER2.2: Zakonski relevantni programi i podaci moraju biti zaštićeni od oštećenja ili namernih izmena od strane neovlašćenih lica.

Pošto je korisnički interfejs uvek u radnom režimu koji podleže zakonskoj kontroli, a softver koji podleže kontroli je izdvojen (f, I, o), *namerne* izmene mogu nastati samo zbog nedozvoljenih svojstava sâmog softvera (npr. ne sme biti moguće da korisnik menja posebne parametre za uređaj.

[10 i)] Učitavanje nije moguće, programi su nepromenljivi (firmver, obično uskladišten u trajnoj memoriji).
[11 b)] Uređaj koji podleže zakonskoj kontroli sa opcijom priključivanja uređaja koji ne podleže kontroli.
[12 f)]Komandni korisnički interfejs je uvek u radnom režimu koji podleže zakonskoj kontroli.

Primedbe u pogledu nivoa zaštite:

Nizak:	Nisu potrebne nikakve posebne mere zaštite od oštećenja.
Srednji/visok:	Ili se mora zaštititi kućište merila ili se program i memorija podataka moraju zaštititi od neovlašćenog uklanjanja.

Primedbe u pogledu nivoa ispitivanja:

Nizak:	Sve operacije se moraju praktično ispitati na osnovu radnog priručnika: preko korisničkog interfejsa ne smeju se moći menjati nikakvi podaci niti programi.
Srednji:	Pored spomenutih ispitvanja, periodično se moraju ispitati sve mere zaštite navedene u dokumentaciji kako bi se proverilo da li funkcionišu kako je dokumentovano.
Visok:	Pored spomenutih ispitvanja, mora se analizirati softver komandnog korisničkog interfejsa kako bi se proverilo da li je samo defnisani skup operacija moguć i da li softver blokira sve druge manipulacije.

ER2.3: U zakonske svrhe može se koristiti samo odobreni i verifikovani softver. Mora biti jasno i nedvosmisleno da prikazivanje rezultata generiše zakonski relevantan program.

Merilo u ovom primeru je namenski uređaj koji ima restriktivne tehničke karakteristike (f, i, I, o).Tehnički nije moguće promeniti radni režim. Zbog toga se prikazivanje mernih vrednosti i drugih funkcija lako može označiti kao nedvosmisleno zakonski relevantno, žigovima, verifikacionim oznakama ili otiscima.

Primedbe u pogledu nivoa zaštite:

Srednji/visok:	Program i memorija podataka moraju se zaštititi od neovlašćenog uklanjanja.

Primedbe u pogledu nivoa usaglašenosti:

Nizak:	Proizvođaču je dozvoljeno da ispravi programski kôd bez promene identifikacije zakonskog softvera. Međutim, što se tiče zakonski relevantnih softverskih delova imenovano telo mora u svakom slučaju biti informisano. Kod verifikacije, odgovarajući organ ili odgovorno lice proverava pomoću identifikacije zakonskog softvera da li je softver koji je primenjen u merilu **usaglašen** sa odobrenim softverom.
Srednji:	Pošto merilo vrši jednostavna, direktna merenja, primenjuje se isto kao i za nizak nivo.
Visok:	Proizvođač primenjuje tačno isti softver u svakom pojedinačnom merilu, bez ikakvih izmena. Kod verifikacije odgovarajući organ ili odgovorno lice proverava pomoću identifikacije zakonskog softvera (potpis) da je softver merila ***identičan*** sa odobrenim softverom. Korisnik se može osloniti na ***verifikacionu oznaku*** da prikazivanje mernih vrednosti generiše odobreni program.

ER2.4: Funkcionalni defekti koji mogu falsifikovati merne vrednosti u softverski kontrolisanom hardveru moraju se otkriti i na njih se mora reagovati.

U primeru su otkrivene neke vrste funkcionalnih defekata i softver izvršava odgovarajući reakciju (r)[13r)] .

Primedbe u pogledu nivoa ispitivanja:

Nizak:	Merilo se praktično ispituje uz pomoć radnog priručnika. Pošto do funkcionalnih defekata dolazi prilično retko, mehanizam za otkrivanje defekata se po pravilu ne ispituje.
Srednji:	Mehanizam za otkrivanje defekata opisan u dokumentaciji proverava se simuliranjem odgovarajućih defekata.
Visok:	Mehanizam za otkrivanje defekata ispituje se kao u slučaju srednjeg nivoa. Pored toga, simuliraju se drugi defekti i ocenjuje se reakcija merila.

ER3.1: Softver se ne sme na nedozvoljan način menjati posle odobrenja tipa.

Koja je vrsta izmena dozvoljena, zavisi od nivoa potrebnog nivoa usaglašenosti:

Primedbe u pogledu nivoa usaglašenosti:

Nizak:	Primenjeni softver svakog pojedinačnog merila u skladu je sa odobrenom dokumentacijom. Bez obzira na manje korekcije izvornog kôda, funkcionalnost ostaje identična sa tehničkom dokumentacijom: ° Modifikacije softvera nisu dozvoljene sve dok dokumentovane funkcije i karakteristike

[13 r)] Prisustvo defekta nije očigledno i ne može se lako i jednostavno proveriti korišćenjem drugog uređaja osim samog merila i nema hardverskih sredstava za otkrivanje defekata.

odobrenog merila ostaju nepromenjene. Međutim, NB mora biti obavešteno. Promene dokumentovanih funkcija i karakteristika zahtevaju dopunsko odobrenje od NB i novu zakonsku identifikaciju softvera.

- Kod verifikacije, usaglašenost sa odobrenim softverom proverava se pomoću identifikacije zakonskog softvera koja je navedena u sertifikatu o odobrenju tipa.
- Dokumentacija odobrenog softvera čuva se kod NB. Pored toga, izuzetno se može deponovati kompletan programski kôd (izvršni kôd) merila.

Srednji: Za namenski uređaj sa jednostavnim, direktnim mernim principom (y) i kod koga celokupan softver podleže kontroli kao u ovom primeru (f, i, l, o), primenjuje se isto kao i za nivo *nizak*.

Visok: Celokupan softver svakog pojedinačnog merila identičan je sa odobrenim softverom:

- Zbog identita, izmena nekog dela softvera automatski dovodi do nove identifikacije zakonskog softvera. NB u tom slučaju daje dopunsko odobrenje.
- Kod verifikacije, usaglašenost sa odobrenim softverom proverava se pomoću identifikacije zakonskog softvera (potpis) koja je navedena u sertifikatu o odobrenju tipa.
- Dokumentacija odobrenog softvera i kompletan programski kôd (izvršni kôd) merila čuvaju se kod NB.

ER3.2: Za verifikaciju usaflašenosti na raspolaganju mora biti identifikacija zakonski relevantnog softvera kao i odgovarajuća upustva.

Od nivoa zahtevanog nivoa usaglašenosti zavisi kako se nivo usaglašenosti pojedinačnog merila proverava:

Primedbe u pogledu nivoa usaglašenosti:

Nizak: Primenjeni softver svakog pojedinačnog merila u skladu je sa odobrenom dokumentacijom. Bez obzira na manje korekcije izvornog kôda, funkcionalnost ostaje identična sa tehničkom dokumentacijom::

° Kod verifikacije, usaglašenost sa odobrenim softverom proverava se pomoću identifikacije zakonskog softvera koja je navedena u sertifikatu o odobrenju tipa. Identifikacija zakonskog softvera može se prikazati na zahtev ili automatski kod pokretanja ili ciklično.

Srednji: Za namenski uređaj sa jednostavnim, direktnim mernim principom (y) i kod koga celokupan softver podleže kontroli kao u ovom primeru (f, i, l, o), primenjuje se isto kao i za *nizak* nivo.

Visok: Celokupan softver svakog pojedinačnog merila identičan je sa odobrenim softverom:

° Kod verifikacije, usaglašenost sa odobrenim softverom proverava se pomoću identifikacije zakonskog softvera (potpis) koja je navedena u sertifikatu o odobrenju tipa.

ER4.1: Funkcionalnost merila mora se moći ispitati.

Kada se radi o metrološkim delovima softvera, taj zahtev je zadovoljen jer je moguće uoobičajeno ispitivanje metrološke performanse kompletnog merila i njegovih funkcija.

Primedbe u pogledu nivoa ispitivanja:

Nizak: Samo se metrološki delovi softvera merila ispituju uobičajenim praktičnim ispitivanjem. Nije potrebno da proizvođač ispita ostale karakteristike softvera koje nisu obuhvaćene tim ispitivanjima: dovoljno je da izjavi da su neispitane karakteristike uasglašene sa zahtevima (zaštićenost interfejsa, ortkrivanje defekata i reakcija, itd.).

Srednji: Pored uobičajenih ispitivanja tipa (videti *"nizak")* softver se ispituje na osnovu opisa softverskih funkcija koji je proizvođač dostavio. Praktičnim ispitivanjima se verifikuje da li su dokumentovane funkcije kompletne i konzistentne.

Visok: Mora se dostaviti izvorni kôd. Isptivanje metrološke performanse još nije zastarelo jer je vrlo efektivno. Međutim, delovi softvera se mogu ispitati ili "ručno" (dobro poznate metode: kontrolisanje kôda, proba, itd.) ili pomoću alata za analizu. Tipični primeri za takva praktična ispitivanja su zaštićenost interfejsa, odvajanje delova, itd.

ER5.1: Zakonski relevantan softver, uključujući i njegovo hardversko i softversko okruženje, mora biti na odgovarajući način dokumentovan.

Za namenski uređaj čiji celokupan softver podleže kontroli kao u ovom primeru (f, i, l, o), proizvođač mora obezbediti najmanje sledeću dokumentaciju:

Primedbe u pogledu nivoa ispitivanja:

Nizak: Proizvođač dostavljaa radni priručnik i tehničku dokumentaciju. Ne zahteva se nikakva dodatna softverska dokumentacija. Dokumentacija mora da sadrži izjave proizvođača o nekim karakteristikama merila koje nisu ispitane (npr. da je interfejs izrađen kao zaštitni) i identifikaciju zakonskog softvera.

Srednji: Pored dokumentacije niskog nivoa, posebna softverska dokumentacija mora da obuhvata:

- detaljan opis svih funkcija zakonski relevantnog softvera, zakonski relevantne parametre koji određuju funkcionalnost merila
- opis algoritama za merenje (npr. izračunavanje cene i algoritmi za zaokruživanje)
- identifikaciju zakonskog softvera
- kompletan opis komandi i parametara preko zaštitnog interfejsa, uključujući izjavu o kompletnosti tog opisa
- upućivanje na zahteve iz ovog vodiča
- radni priručnik

Visok: Pored dokumentacije nivoa "srednji", proizvođač mora dostaviti zvorni kôd (kao datoteku) zajedno sa pomoćnom dokumentacijom kao što je:

- logički dijagram softvera (npr. dijagram toka ili Nasi-Šnejdermanov (Nassi-Shneidermann diagram))
- detaljan opis funkcija svakog modula zakonski relevantnog softvera
- opis strukture podataka (preneti skupovi podataka)

6.2 Primer B: PC-baziran, modularni, složeni merni sistem

Merni sistem opisan u ovom primeru može se, na primer, naći u primenama kao što su merni mostovi automatskih šinskih vaga, dimenzionalna merila, često u kombinaciji sa sistemima za vaganje, sistemi prodajnih mesta (POS) i dr.

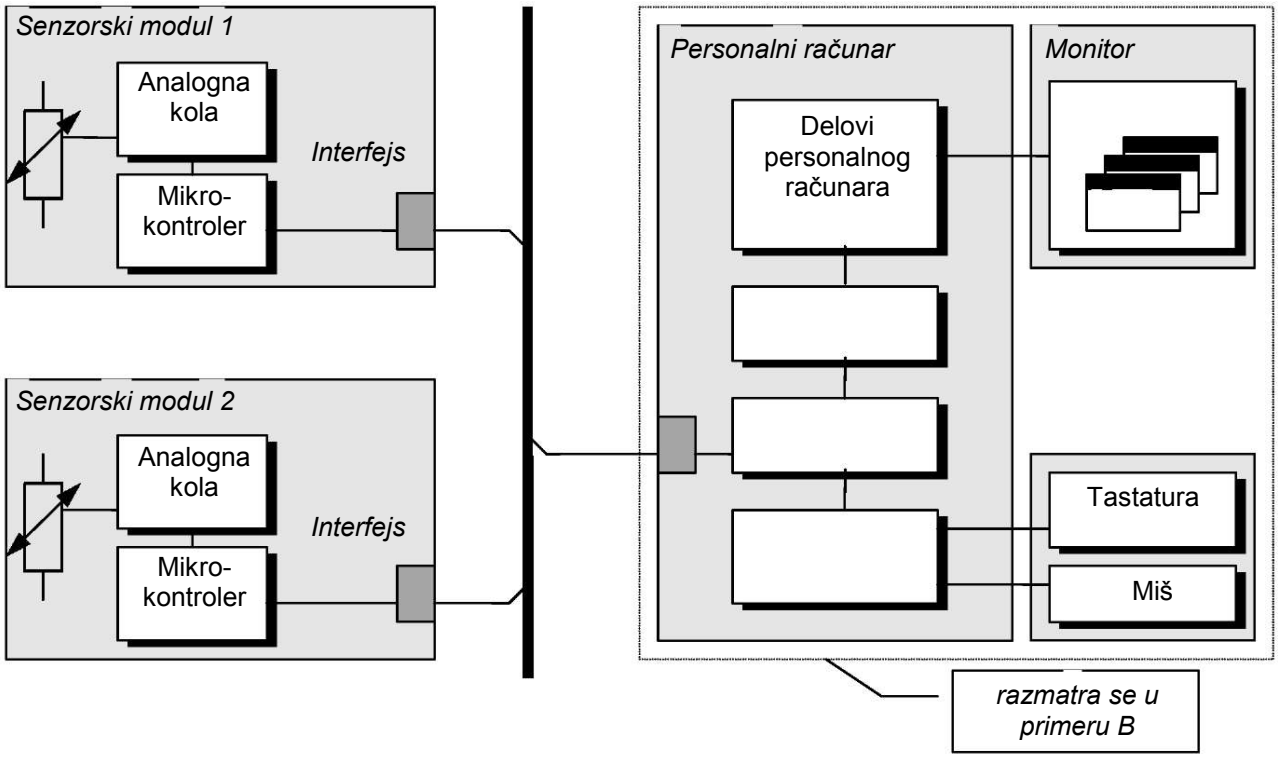
6.2.1 Opis sistema

Recimo da se kompletan merni sistem sastoji od nekoliko komponenti (modula) povezanih pomoću otvorene mreže. Sistem možgu obeležiti sledeće karakteristike (Slika 6-2):

- *"Senzorksi moduli" se sastoje od senzora, analogne elektronike, A/D konvertora, mikrokontrolora i digitalnog interfejsa sa mrežom ali nemaju pokazivanje.*
- *Postoji "centralni uređaj" kojeg realizuje lični računar. Njegov monitor se koristi kao indikator konačnih mernih vrednosti i uskladištenih vrednosti.*
- *Svaki senzorski modul prenosi merne vrednosti centralnom uređaju i prima komande od njega preko mreže.*
- *Centralni uređaj izvršava skladištenje podataka u zakonske svrhe.*
- *Centralni uređaj ima Windows operativni sistem.*
- *Zakonski relevantne funkcije centralnog uređaja izvršavaju se pomoću programa koji se učitava sa jedinice čvrstog diska kompjutera. On se kompilira u tzv. biblioteku[14].*
- *Zakonski relevantan softver u centralnom uređaju prima merne vrednosti iz senzorskih modula, prikazuje ih u prozoru, skladišti ih za kasniju zakonsku upotrebu i izvozi ih u druge programe koji ne podležu zakonskoj kontroli.*
- *Izmerena roba se ne može meriti statički, tj. merni proces je dinamičan i složen. (Na primer, primenjuje se na merne mostove automatskih šinskig vaga. Za dimenzionalno merenje i statičko vaganje proces je jednostavan i statičan.)*

U dlajem tekstu razmatra se samo centralni uređaj. Senzorski moduli se mogu tretirati na sličan način kao i merilo koje se razmatra u primeru A.

[14] ***Napomena**:* (Dinamička) softverska biblioteka je zbirka potprograma (ili klasa u objektno orijentisanom jeziku) koju može koristiti svaki program (aplikacija). Biblioteka se može napraviti odvojeno od aplikacionog softvera. Interna struktura biblioteke je sakrivena od programera aplikacije.



Slika 6-2: *Primere B:* PC-baziran, modularni, složeni merni sistem

6.2.2 Zakonska klasifikacija

Po pravilu, zakonska klasifikacija bi sledila Tabelu A-1 iz Priloga 1. Pošto nivoi još nisu odabrani, u sledećim tumačenjima u obzir su uzeti **svi** nivoi za "zaštitu, ispitiivanje i usaglašenost ".

Napomena: Pošto je primer B prilično složen sistem, potrebno je mnogo tumačenja opštih zahteva. Da bi tumačenja i primedbe bili sveoubuhvatniji, sledeći slučajevi su odabrani prema predlogu za kategoriju "Merila koja se koriste za komercijalne transakcije" (videti Tabelu A-1):

Nivo zaštite softvera: ***srednji***

Nivo ispitivanja softvera: ***srednji***

Nivo usaglašenosti softvera: ***nizak***

Ti nivoi i rezutirajuća tumačenja označeni su u odeljku 6.2.4. sivom pozadinom kakva je i pozadina ove napomene. Oni su u skladu sa zahtevima WELMEC Vodiča 2.3 koji se već primenjuje na vage.

Napomene: *Ako je propisani nivo usaglašenosti "visok", tehničko rešenje iz ovog primera neće biti podesno za postizanje tih nivoa za neke zahteve (ER1.1, ER1.2, ER2.3 i dr.).*

6.2.3 Tehnička klasifikacija

Klasifikacija prema poglavlju 5 ovde primenjuje se samo na centralni uređaj (personalni računar) iz primera.

Karakteristika	Slučaj	Objašnjenje
Hardverska konfiguracija	*e*	Modularmi sistem, neki moduli ne podležu zakonskoj kontroli, sistem otvorene komunikacijske sabirnice.
Korisnički interfejs (komandni)	*h*	Slobodni komandni korisnički interfejs sa radnim režimima koji podležu kontroli i radnim režimima koji ne podležu kontroli, uporedo.
Učitavanje softvera	*k*	Svaki program se može učitati. Učitavanje se može izvršiti pomoću izmenljivih uređaja za čuvanje podataka (disketa, CD-ROM i dr.) ili preuzimanjem sa servera preko inetrefejsa (na disk, Flash ROM, EEPROM itd.).
Softverska struktura	*m*	Delovi softvera podležu zakonskoj kontroli. Za ostale delove koji nisu zakonski relevantni predviđeno je da se menjaju posle odobrenja.
Softversko okruženje	*p*	Softver koji podleže kontroli ugrađen je u okruženje kao i standardni radni sistem koji nije posebno izrađen u merne svrhe.
Otkrivanje defekata	*r*	Prisustvo defekta nije očigledno i ne može se jednostavno proveriti pomoću drugih uređaja osim samog merila i nema hardverskih sredstava za otkrivanje defekata.
Dugoročno skladištenje mernih vrednosti	*t*	Merne vrednosti se skladište u sistemu u svrhe kasnije zakonske upotrebe.
Merni princip	*v, x, z*	Pojedinačno, neponovljivo, složeno merenje

U narednim odeljcima slučajevi su jednostavno skraćeni, na primer, (k).

6.2.4 Tumačenje bitnih softverskih zahteva

Ovde navedeno tumačenje primenjuje se samo na centralni uređaj (personalni računar) iz primera.

ER1.1: Softver merila mora biti projektovan tako da omogućava lako ocenjivanje svoje usaglašenosti sa zahtevima ovog vodiča.

U ovom primeru proizvođač namerava da posle odobrenja tipa menja delove softvera koji ne podležu zakonskoj kontroli (m) . Stoga je potrebno razdvojiti softver na dva dela (kao dobra programerska praksa danas): jedan deo mora sadržavati sve programske module koji obavljaju zakonski relevantne funkcije ili koji utiču na zakonski relevantne parametre i podatke. Dozvoljeno je da se svi programski moduli menjaju, formiraju drugi/druge deo/delove.

Primedbe u pogledu nivoa isptivanja *(ER1.1):*

Nizak: Projekat i strukturu softvera nije moguće ispitati uobičajenim metrološkim ispitivanjima. Proizvođač *deklariše* (bez dostavljanja dokazne dokumentacije) sva zahtevana svojstva softvera koja se ispravno primenjuju (npr. softverska razdvojenost, zaštićenost softverskog interfejsa, predviđene izmene samo na zakonski nerelevantnom delu). Ne vrši se nikakav pregled kojim se deklaracija verifikuje.

Srednji: Projekat i struktura softvera (razdvajanje softvera, softverski interfejs i dr.) ispituju se na osnovu opisa softverskih funkcija koje je dostavio proizvođač. Verifikuje se da li dokumentacija sadrži sve funkcije koje čine merilo i da li su one definisane tačno i konzistentno.

Visok: Projekat i struktura softvera (softverska razdvojenost, softverski interfejs idr.) ispituju se pomoću izvornog kôda, pored koraka za srednji nivo.

***Primedbe u pogledu nivoa usaglašenosti** (ER1.1):*

Nizak:	Proizvođač *izjavljuje* da primenjeni softver svakog pojedinačnog merila jeste i da će biti *usaglašen* sa odobrenom dokumentacijom: razdvajanje zakonski relevantnih softverskih delova od ostalih delova, za sve verzije zakonski nerelevantnog dela softvera, ostaviće se za realizaciju u budućnosti. Proizvođač mora obavestiti NB o izmenama koje se tiču razdavajanja softvera. Odobrenu softversku dokumentaciju čuva NB. Pored toga, izuzetno se može deponovati kompletan programski kôd (izvršni kôd) merila.
Srednji:	Proizvođač mora da čuva softverski deo koji podleže zakonskoj kontroli, a koji je *identčan* sa odobrenim delom. Izmene dela koji ne podleže zakonskoj kontroli dozvoljeno je vršiti bez obaveze obaveštavanja NB o tome sve dok se softverska razdvojenost poštuje. Proizvođač izjavljuje da će se softverska razdvojenost očuvati za sve verzije zakonski nerelevantnog dela i obaveštava NB o modifikacijama koje se tiču razdvajanja softvera. Odobrena softverska dokumentaciju i kompletan programski kôd (izvršni kôd) merila čuvaju se kod NB.
Visok:	Modifikacije softvera uopšte nisu dozvoljene. Projekat i struktura opisani u primeru ***nisu dozvoljeni*** ako je nivo usaglašenosti propisan!

ER1.2: Zakonski relevantan softver mora biti projektovan tako da drugi softver ne utiče na njega na nedozvoljen način.

Da bi se realizovao protok podataka između dva softverska dela i da se razdvojenost ne bi narušila (videti ER1.1), između zakonski relevantnog softverskog dela i softvera koji ne podleže kontroli mora se realizovati zaštitni softverski interfejs. Taj interfejs obuhvata

° interfejs između softverskih delova (npr. pozivi potprograma) i

° protok podataka između delova.

U ovom primeru, softver koji podleže kontroli kompiliran je u biblioteku i programi koji ne podleže kontroli mogu pozivati određene funkcije te biblioteke radi dobijanja podataka ili kontrole nekih funkcija (objektno orijentisan stil). Softverski interfejs se izvršava pomoću parametara pozvanih potprograma.

Zakonski relevantan softverski deo mora se projektovati tako da softversko okruženje ne utiče ni na zakonski relevantne funkcije, parametre i podatke. Pošto učitavanje softvera nije tehnički ograničeno na personalne računare kao u ovom primeru, "softversko okruženje" može biti svaki program koji se paralelno izvršava. U ovom primeru, višeprogramski operativni sistem (p) dodeljen je za zaštitu funkcija relevantnog softvera od nedozvoljenih uticaja softverskog okruženja.

Moraju se preduzeti mere kojima se sprečava zaobilaženje zaštitnog softverskog interfejsa od strane korisnika (videti primedbe u pogledu nivoa zaštite i ER2.2) ili programera softvera koji ne podleže zakonskoj kontroli (videti primedbe u pogledu nivoa usaglašenosti). Dodatne preventivne mere mogu biti potrebne za zaštitu prikazivanja mernih vrednosti (videti ER2.3).

***Primedbe u pogledu nivoa zaštite (**ER1.2):*

Nizak:	Ne zahteva se nikakva zaštita od zaobilaženja softverskog interfejsa ili od uticaja iz softverskog okruženja.
Srednji:	Videti ER2.2.
Visok:	Prema propisanim tehničkim i zakonskim uslovima, tehničko rešenje iz ovog primera nije pogodno za ostvarivanje visokog nivoa zaštite od neovlašćenih promena!

***Primedbe u pogledu nivoa ispitivanja** (ER1.2):*

Nizak:	Projekat i strukturu softvera nije moguće ispitati uobičajenim metrološkim ispitivanjima. Proizvođač *deklariše* (bez dostavljanja dokazne dokumentacije) sva zahtevana svojstva softvera koja se ispravno primenjuju (npr. softverska razdvojenost, zaštićenost softverskog interfejsa, predviđene izmene samo na zakonski nerelevantnom delu). Ne vrši se nikakav pregled kojim se deklaracija verifikuje.
Srednji:	Softverski interfejs ispituje se na osnovu softverske dokumentacije koju je proizvođač dostavio. Verifikuje se ° da li je softverski interfejs zaštitni, tj. da li nijedna komanda i ulaz podataka preko varijabli interfejsa u zakonski relevantan softverski deo ne utiču na nedozvoljen način na njega i da li je proizvođač izjavio da nisu prihvaćene nikakve komande osim dokumentovanih; ° da li su preduzete mere kojima se obezbeđuje da nije verovatno da će se softverski interfejs zaobići (ovo bi

se ispunilo prevođenjem zakonski relevantnog softvera u biblioteku sa odgovarajućom dokumentacijom za aplikacionog programera);

- da li je operativni sistem u mogućnosti da zaštiti zakonski relevantan softver od uticaja softverskog okruženja (višeprogramski operativni sistem bi to ostvario, međutim, videti ER2.2)

Visok: Pored koraka za srednji nivo, softverski interfejsi se ispituju pomoću izvornog kôda.

***Primedbe u pogledu nivoa usaglašenosti** (ER1.2):*

Nizak: Proizvođač izjavljuje da je softverski interfejs između softvera svakog pojedinačnog merila zaštitni.

Proizvođač dostavlja dokumentaciju softverskog interfejsa za programera aplikacija. Pored opisa upotrebe interfejsa, ta dokumentacija sadrži ograničenja koja programer mora da poštuje kako bi se garantovalo da interfejs nije zaobiđen.

Proizvođač mora obavestiti NB o izmenama koje se tiču softverskog interfejsa između softverskih delova.

Odobrena dokumenatcija softverskog interfejsa čuva se kod NB. Pored toga, izuzetno se može deponovati kompletan programski kôd (izvršni kôd) merila. .

Srednji: Proizvođač čuva softver koji realizuje zaštini interfejs koji je *identičan* sa odobrenim.

Proizvođač izrađuje dokumentaciju softverskog interfejsa za programera aplikacija. Pored opisa upotrebe interfejsa koji ta dokumentacija sadrži, programer mora poštovati ograničenja kako bi se garantovalo da interfejs nije zaobiđen.

Modifikacije dela koji ne podleže zakonskoj kontroli dozvoljene se a da se o tome ne obaveštava NB sve dok zaštitni softverski interfejs nije zaobiđen. Proizvođač mora obavestiti NB o izmenama koje se tiču softverskog interfejsa.

Odobrena softverska dokumentacija i kompletan programski kôd (izvršni kôd merila čuvaju kod NB.

Visok: Menjanje softvera uopšte nije dozvoljeno. Projekat i struktura opisani u primeru ***nisu dozvoljeni*** ako je nivo usaglašenosti propisan!

ER1.3: Zakonski relevantan softver mora biti projektovan na tako da se na njega ne utiče na nedozvoljen način preko interfejsa uređaja.

Merni sistem u primeru sastoji se od nekoliko senzorskih modula koji su priključeni na centralni uređaj pomoću otvorene sabirnice. Razmena podataka između senzorskih modula koji su priključeni na centralni uređaj preko sabirnice je potrebna da bi se dobio konačni merni rezultat:

1. *softver u centralnom uređaju bi mogao imati nedozvoljene karakteristike koje bi ulazi preko mrežnog interfejsa mogli aktivirati i kontrolisati,*
2. *na podatke primljene pomoću centralnog uređaja moglo se uticati ili su se oni mogli oštetiti na njihovom putu od senzorskih modula preko mreže,*
3. *podatke primljene iz mreže pomoću centralnog uređaja mogao je generisati pošiljalac koji nije verifikovani senzorski modul.*

Što se tiče br. 2, on se odnosi na prenos podataka (videti ER2.2). Što se tiče br. 3, on se odnosi na neovlašćene izmene (videti ER2.2). Br. 1 se odnosi na svojstva softvera koja kontrolišu interfejs uređaja. Da bi se ER1.3 zadovoljio u tom smislu, interfejs mora biti zaštitni; videti sledeće primedbe.

***Primedbe u pogledu nivoa zaštite** (ER1.3):*

Nizak: Ne zahteva se nikakva zaštita od neovlašćenog menjanja prenetih podataka ili uticaja na zakonski relevantan softver preko mrežnog interfejsa.

Srednji/visok: Ako softver koji kontroliše interfejs samo pusti da prođu komande koje ne mogu nedozvoljeno uticati na zakonski relevantne funkcije i podatke softvera, neovlašćeno menjanje preko interfejsa nije moguće; on je zaštitni. Ako programer realizuje softver interfejsa na taj način, tehničko rešenje iz ovog primera može da garantuje *srednji* i *visok* nivo zaštite od neovlašćenih promena.
Što se tiče zaštite podataka u otvorenoj mreži, videti ER2.2.

Primedbe u pogledu nivoa ispitivanja *(ER1.3):*

Nizak: Nije moguće ispitati uobičajenim metrološkim ispitivanjima da li je interfejs zaštitni. Proizvođač *izjavljuje* (bez dostavljanja dokazne dokumentacije) da se preko interfejsa ne može dobiti nijedna komanda koja na nedozvoljen način utiče na zakonski relevantne funkcije ili podatke softvera. Ne obavlja se nikakvo ispitivanje kojim se ta izjava verifikuje.

Srednji: Interfejs se ispituje na osnovu softverske dokumentacije kojom se
- *definišu i dokumentuju funkcije koje se mogu kontrolisati preko interfejsa,*
- *definišu i dokumentuju parametri koji se mogu postavljati ili menjati preko interfejsa,*
- *specificiraju funkcije koje se kontrolišu i parametri koji su postavljeni, a koji su zakonski relevantni.*

Ispituje se da li je interfejs zaštitni, tj. da li su sve dokumentovane komande i ulazi podataka preko interfejsa takvi da ne utiču na nedozvoljen način na njegove funkcije i podatke i da li je proizvođač deklarisao da nisu prihvaćene druge komande od dokumentovanih.

Visok: Pored koraka za srednji nivo, softver koji kontroliše interfejs ispituje se pomoću izvornog koda.

***Primedbe u pogledu nivoa usaglašenosti** (ER1.3):*

Nizak: Proizvođač *izjavljuje* da se preko interfejsa ne mogu dobiti komande koje na nedozvoljen način utču na zakonski relevantne funkcije ili podatke softvera.

Srednji/visok: Proizvođač čuva softver koji kontroliše zaštitni interfejs, koji je identičan sa odobrenim softverom. On mora obavestiti NB o izmenama koje se odnose na softver koji kontroliše interfejs.

ER2.1: Zakonski relevantni programi i podaci moraju biti zaštićeni od slučajnih i nenamernih izmena.

Sledeći efekti mogli bi dovesti do slučajnih ili nenamernih izmena u primernom sistemu:
- *fizički efekti (elektormagnetni, temperatura, vlažnost i dr.) unutar uređaja.*
- *elektromagnetni efekti u prenosnom kanalu,*
- *otkazi softvera, virusi,*
- *nenamerno učitavanje, uređivanje i skladištenje programskog fajla sa uređivačem teksta,*
- *nedozvoljena svojstva softvera koji podleže kontroli (npr. ne sme biti moguće nenamerno menjati parametre specifične za uređaj).*

***Primedbe u pogledu nivoa zaštite** (ER2.1):*

Nivo zaštite u smislu u kome se ovde korsti odnosi se na *nenamerne manipulacije* (videti ER2.2).

***Primedbe u pogledu nivoa ispitivanja** (ER2.1):*

Nizak: Proizvođač *izjavljuje* (bez dostavljanja dokazne dokumentacije) da su preduzete mere za otkrivanje slučajnih promena (unutar uređaja kao i u prenosnom kanalu) i da te mere na odgovarajući način reaguju. Ne obavlja se nikakvo ispitivanje kojim se ta izjava verifikuje.

Što se tiče nenamernih promena, rukovanje korisničkim komandnim interfejsom praktično se ispituje uz pomoć radnog priručnika.

Potrebni su sertifikati o ispitivanju prema propisu u pitanju (EMC, temperatura, vlažnost i dr.).

Srednji: Mere za otkrivanje promena i programi ispituju se na osnovu softverske dokumentacije koju je proizvođač dostavio. Verifikuje se
- da li je algoritam za samoproveru opisan (u ovom primeru: program proverava svoj integritet automatski, npr. izračunavanjem kontrolnog zbira preko izvršnog koda, poredeći ga sa nominalnom vrednošću i zaustavljajući ga ako je kod izmenjen,
- da li prenosni protokol omogućava prijemnom programu da otkrije slučajne promene u skupu podataka koji senzorski moduli prenose do centralnog uređaja (ako je zaštita od *namernih* promena ostvarena, obuhvaćen je i taj zahtev ER2.1 koji se odnosi na nenamerne promene,
- proizvođač mora u potpunosti dokumentovati rukovanje od strane korisnika.

Što se tiče nenamernih promena, rukovanje korisničkim komandnim interfejsom praktično se ispituje uz pomoć radnog priručnika.

Potrebni su sertifikati o ispitivanju prema propisu u pitanju (EMC, temperatura,vlažnost i dr.)

Visok: Pored koraka za srednji nivo, softver koji izvršava prenos podataka i korisnički komandni interfejs ispituju se pomoću izvornog koda.

ER2.2: Zakonski relevantni programi i podaci koji se moraju zaštititi od oštećenja ili namernih izmena od strane neovlašćenih lica.

Zaštita programskog koda *(ER2.2)*

Centralni uređaj ima otvoreni korisnički komandni interfejs (h) i mogu se učitavati alati kao što je uređivač.

***Primedbe u pogledu nivoa zaštite** (ER2.2, programski kod):*

Nizak: Nisu potrebne nikakve mere za zaštitu od provaljivanja.

Srednji: Zakonski relevantan program mora se zaštiti od namernih izmena pomoću jednostavnih, zajedničkih softverskih alata (uređivači teksta). U ovom primeru program automatski proverava svoj integritet, npr. izračunavanjem kontrolnog zbira preko izvršnog koda, poredeći ga sa nominalnom vrednošću i zaustavljajući ga ako je kod izmenjen. Pretpostavlja se da će za napadača biti dovoljno teško da izmeni programski kod, nađe kontrolni zbir u kodu, izračuna novi kontrolni zbir za izmenjenii kod i zameni stari kontrolni zbir samo uz pomoć uređivača teksta.

Na program nije moguće uticati pomoću uređivača teksta.

Visok: Zakonski relevantan softver mora biti zaštićen od namernih izmena pomoću specijalnih soficistiranih softverskih alata (funkcije za otklanjanje grešaka, uređivači čvrstog diska, alati za razvoj softvera), tj. imati nivo zaštite u skladu sa najnovijim dostignućima u oblasti zaštite podataka, kao što je, na primer, za finansijske transakcije.

Tehničko rešenje iz ovog primera ***ne*** bi bilo pogodno za postizanje ovog nivoa zaštite. Bile bi potrebne dodatne hardverske jedinice u personalnom računaru centralnog uređaja da prekinu otkrivanje grešaka (traganje za greškama) i da garantuju integritet zakonski relevantnog programskog koda.

***Primedbe u pogledu nivoa ispitivanja** (ER2.2, programski kod):*

Nizak: Proizvođač *izjavljuje* (bez dostavljanja dokazne dokumentacije) da su preduzete mere za otkrivanje slučajnih promena i da te mere na odgovarajuči način reaguju na te promene.

Rukovanje korisničkog komandnog interfejsa praktično se ispituje uz pomoć radnog priručnika.

Srednji: Mere za otkrivanje promena zakonski relevantnog programa ispituju se na osnovu softverske dokumentacije koju je proizvođač dostavio. Verifikuje se

° da li je algoritam za samoproveru opisan (u ovom primeru: program proverava svoj integritet automatski, npr. izračunavanjem kontrolnog zbira preko izvršnog koda, poredeći ga sa nominalnom vrednošću i zaustavljajući ga ako je kod modifikovan.

Softver se ispituje praktično. Posebno se uz pomoć uređivača teksta ispituje otkrivanje izmene koda.

Visok: Pored koraka za srednji nivo, softver koji realizuje otkrivanje namernih promena i korisnički komandni interfejs ispituju se pomoću izvornog koda.

Zaštita parametara specifičnih za tip *(ER2.2)*

Parametri specifični za tip po pravilu su deo programskog koda. U ovom slučaju važe sve primedbe u pogledu "Zaštite programskog koda" (videti gore). Ako se parametri specifični za tip skladište odvojeno od programskog koda, primenjuju se primedbe iz "Zaštita parametara specifični za uređaj" (videti dole).

Zaštita parametara specifičnih za uređaj *(ER2.2)*

Nema razlike između parametara specifičnih za tip i parametara specifičnih za uređaj: za razliku od konstantnih specifičnih podataka za tip mora postojati mogućnost podešavanja podataka specifičnih za uređaj pre zakonske verifikacije. Podešavanje posle zakonske verifikacije ne sme biti moguće za korisnika i druga neovlašćena lica. ER2.2 se stoga mora tumačiti neznatno drugačije od tumačenja u pogledu programskog koda, parametara specifičnih za tip u okviru programskog koda i dr.

***Primedbe u pogledu nivoa zaštite** (ER2.2, parametri* specifični *za uređaj):*

Nizak: Nisu potrebne nikakve mere za zaštitu od provaljivanja.

Srednji/visok: Iako se za ovaj nivo pretpostavlja da je uređivač teksta jedini alat i za provaljivanje, to nije dovoljno zbog mogućnosti podešavanja parametara specifičnih za uređaj. Opremu za podešavanje potrebno je žigosati mehanički ili pomoću elektronskog žigosanja *(*treba dodati *definiciju prema WG2).* To tehnički ***nije*** moguće realizovati kod standardnog personalnog računara kakav je u ovom primeru.
U ovom primeru, svi specifični parametri za uređaj uskladišteni su u senzorskim modulima gde se

mogu lako osigurati (slično primeru A, 6.1)

Primedbe u pogledu nivoa ispitivanja *(ER2.2, parametri specifični za uređaj):*

Nizak: Proizvođač *izjavljuje* (bez dostavljanja dokazne dokumentacije) da u okviru centralnog uređaja nisu uskladišteni nikakvi parametri specifični za uređaj. Ne obavlja se nikakvo ispitivanje kojim se ta izjava verifikuje.

Softver se prakično ispituje uz pomoć radnog priručnika da bi se proverilo kako su parametri specifični za uređaj postavljeni i da li je zaštita moguća.

Srednji: Proizvođač dokumentuje sve parametre specifične za uređaj. On opisuje gde su oni uskladišteni i kako se mogu zaštititi.

Pri ispitivanju se na osnovu dokumentacije verifikuje da korisnik ili druga neovlašćena lica ne mogu te parametre podešavati ili menjati.

Korisnički komandni interfejs se ispituje praktično. Posebno se mora proveriti način na koji se parametri specifični za uređaj moraju postaviti.

Visok: Pored koraka za srednji nivo, softver se ispituje pomoću izvornog koda. Posebno se ispituju oni delovi koji su odgovorni za skladištenje parametara specifičnih za uređaj. Softverski deo se mora blokirati pomoću nekog hardverskog sredstva.

Zaštita od zaobilaženja softverskog interfejsa *(ER2.2)*

U ovom primeru, zaštitni softverski interfejs je realizovan. Zaobilaženje interfejsa *od strane korisnika* omogućava korisniku da utiče na funkcije zakonski relevantnog softverskog dela ili da menja varijable ili parametre koje nije dozvoljeno postavljati. Videti tačke gore u vezi sa zaštitom programskog koda, podataka i parametara.

Zaštita prenetih podataka *(ER2.2)*

U ovom primeru, merne vrednosti se prenose preko mreže i prima ih centralni uređaj za završnu obradu (e). Preneti podaci se moraju zaštiti iz dva razloga:

- *na podatke koje je primio centralni uređaj moglo se uticati ili su se oni mogli oštetiti na svom putu od senzorskih modula (podaci su izgubili svoj integitet),*
- *podatke koje je centralni uređaj primio iz mreže mogao je generisati pošiljalac koji nije verifikovani senzorski modul (podaci nisu autentični).*

Primedbe u pogledu nivoa zaštite *(ER2.2, preneti podaci):*

Nizak: Nisu potrebne nikakve mere za zaštitu od provaljivanja.

Srednji: Integritet. Zakonski relevantni preneti podaci moraju biti zaštićeni od namernih promena uz pomoć jednostavnih zajedničkih softverskih alata (uređivači teksta). To se može realizovati, na primer, elektronskim potpisom (videti 2.6) ili šifrovanjem.

Nivo zaštite zavisi od algoritma i dužine ključa za potpis (ili šifrovanje). Prihvatljivo rešenje za srednji nivo zaštite bilo bi CRC [11, 12] algoritam sa dužinom ključa/potpisa od 2 bajta za svaki skup podataka jedne merne vrednosti.

Autentičnost. Primalac mernih vrednosti ili drugih zakonski relevantnih podataka mora biti u stanju da proveri da li je podatke poslao ovlašćeni pošiljalac i da li su ti podaci stvarni. Prihvatljivo rešenje za zaštitu srednjeg nivoa bilo bi, na primer,

- *the registracija adresa svih zakonskih pošiljalaca na mreži kod primaoca, kombinovanjem adrese pošiljaoca sa mernom vrednošću, a potom, proverom kod primaoca da li je adresa validna;*
- *kombinovanjem vremenske oznake sa mernom vrednošću, a potom njenim prenošenjem i proveravanjem kod primaoca da li je stvarna.*

Svi relevantni podaci potrebni za konačnu obradu ili ponovno verifikovanje merne vrednosti, uključujući potpis, adresu pošiljaoca, vremensku oznaku i dr. moraju se grupisati u jedan skup podataka i potpis mora obuhvatiti sve oblasti skupa podataka.

Podaci za koje je otkriveno da su oštećeni ne smeju se koristiti.

Ključ koji se koristi za proveru ili generisanje potpisa mora se tretirati kao zakonski relevantni podaci.

Visok: Zakonski relevantan softver mora se zaštititi od namernih promena uz pomoć specijalnih sofisticiranih softverskih alata (funkcija za otklanjanje grešaka i uređivači čvrstog diska, alati za razvoj softvera) tj.

mora imati nivo zaštite u skladu sa najnovijim dostignućima u oblasti zaštite podataka kao što je, na primer, za finansijske transakcije.

Primenjuje se isto kao i za srednji nivo, međutim, gore navedeni algoritam za potpis i dužina ključa su suviše slabi. Prihvatljivo rešenje za algoritam za potpis bilo bi, na primer, DEA[15] sa minimalnom dužinom ključa od 128 bajtova.

Ali čak i ako algoritam i ključ zadovoljavaju visok nivo, tehničko rešenje iz ovog primera ***ne*** bi bilo podesno za dostizanje ovog nivoa zaštite jer je primalac (centralni uređaj) standardni personalni računar bez odgovarajućih zaštitnih sredstava (videti primedbu u pogledu ER1.2, visok nivo zaštite).

Primedbe u pogledu nivoa ispitivanja *(ER2.2, preneti podaci):*

Nizak: Proizvođač *izjavljuje* (bez dostavljanja dokazne dokumentacije) da su preduzete mere za otkrivanje namernih promena skupa podataka dobijenog od drugog modula i da te mere na odgovarajući način reaguju na te promene. Ne obavlja se nikakvo ispitivanje kojim se ta izjava verifikuje.

Srednji: Mere za otkrivanje promena zakonski relevantnih podataka ispituju se na osnovu softverske dokumentacije koju je proizvođač dostavio. Verifikuje se

° *da li su podesan algoritam za potpis i dovoljna dužina ključa realizovani,*

° *da li su svi podaci potrebni za završnu obradi i za zaštitu prenetih mernih vrednosti kombinovani u skup podataka (neophodna polja u skupu podaka su, na primer, merna vrednost, adresa pošiljaoca, vremenska oznaka i tekući broj merenja),*

° *da li se ključ za potpis ne može pročitati ili istražiti pomoću uređivača teksta.*

Praktično ispitivanje: Skup podataka je falsifikovan i poslat centralnom uređaju. Reakcija na tu grešku se proverava.

Visok: Pored koraka za srednji nivo, softver koji izvršava otkrivanje namernih promena i generisanje potpisa ispituje se pomoću izvornog koda.

Zaštita dugoročno uskladištenih podataka *(ER2.2)*

U ovom primeru, merne vrednosti se skladište pomoću centralnog uređaja u svrhu kasnije zakonske upotrebe (t). Postoji program koji podleže kontroli, za prikazivanje uskladištenih vrednosti korisniku. On korisniku omogućava da nađe i jasno dodeli neki raniji rezultat merenja određenom uskladištenom skupu podataka (u okviru određenog vremenskog prostora).

Primedbe u pogledu nivoa zaštite *(ER2.2, dugoročno uskladišteni podaci):*

Nizak: Nisu potrebne nikakve mere za zaštitu od provaljivanja.

Srednji: *Integritet.* Zakonski relevantni uskladišteni podaci moraju biti zaštićeni od namernih promena uz pomoć jednostavnih zajedničkih softverskih alata (uređivači teksta). To se može realizovati, na primer, elektronskim potpisom (videti 2.6) ili šifrovanjem.

Nivo zaštite zavisi od algoritma i veličine ključa za potpis (ili šifrovanje). Prihvatljivo rešenje za srednji nivo zaštite bilo bi, na primer, CRC [11, 12] algoritam sa veličinom ključa/potpisa od 2 bajta za svaki skup podataka jedne merne vrednosti.

Autentičnost. Korisnik uskladištenih mernih vrednosti mora biti u stanju da svaku vrednost dodeli određenom merenju. Prihvatljivo rešenje za zaštitu srednjeg nivoa bilo bi, na primer,

° kombinovanje ID poput jedinstvenog (tekućeg) broja i merne vrednosti

° kombinovanje vremenske oznake i merne vrednosti.

Svi relevantni podaci potrebni za ponovnu verifikaciju merne vrednosti, uključujući potpis, ID broj fajla, vremensku oznaku i dr., moraju se grupisati u jedan skup podataka, a potpis mora obuhvatati sva polja skupa podataka.

Podaci za koje je otkriveno da su oštećeni ne smeju se koristiti.

Ključ koji se koristi za proveru potpisa mora se tretirati kao zakonski releventan podatak.

Visok: Zakonski relevantan softver mora se zaštititi od namernih promena uz pomoć specijalnih sofisticiranih softverskih alata (funkcija za otklanjanje grešaka i uređivači čvrstog diska, alati za razvoj softvera) tj. mora imati nivo zaštite u skladu sa najnovijim dostignućima u oblasti zaštite podataka kao što je, na primer, za finansijske transakcije.

[15] Specifikacija algoritma DEA iz [10]

Primenjuje se isto kao i za srednji nivo, međutim, gore navedeni algoritam za potpis i dužina ključa su suviše slabi. Prihvatljivo rešenje za algoritam za potpis bilo bi, na primer, DEA[16] sa minimalnom dužinom ključa od 128 bajtova.

Ali čak i ako algoritam i ključ zadovoljavaju visok nivo, tehničko rešenje iz ovog primera ***ne*** bi bilo podesno za dostizanje ovog nivoa zaštite jer je primalac (centralni uređaj) standardni personalni računar bez odgovarajućih zaštitnih sredstava (videti primedbu u pogledu ER1.2, visok nivo zaštite).

Primedbe u pogledu nivoa ispitivanja *(ER2.2, dugoročno uskladišteni podaci):*

Nizak: Proizvođač *izjavljuje* (bez dostavljanja dokazne dokumentacije) da su preduzete mere za otkrivanje namernih promena uskladištenih skupova podataka i da te mere na odgovarajuči način reaguju na te promene. Ne obavlja se nikakvo ispitivanje kojim se ta izjava verifikuje.

Srednji: Mere za otkrivanje promena uskladištenih zakonski relevantnih podataka ispituju se na osnovu softverske dokumentacije koju je proizvođač dostavio. Verifikuje se

- *da li su podesan algoritam za potpis i dovoljna dužina ključa realizovani;*
- *da li su svi podaci potrebni za zaštitu uskladištenih mernih vrednosti kombinovani u skup podataka (neophodna polja u skupu podata su, na primer, merna vrednost, adresa pošiljaoca, vremenska oznaka i tekući broj merenja);*
- *da li se ključa za potpis ne može pročitati ili istražiti pomoću uređivača teksta.*

Praktično ispitivanje: Uskladišteni skup podataka je falsifikovan u centralnom uređaju korišćenjem uređivača teksta. Reakcija na tu grešku se proverava.

Visok: Pored koraka za srednji nivo, softver koji realizuje otkrivanje namernih promena i generisanje potpisa ispituje se pomoću izvornog koda.

ER2.3: U zakonske svrhe je dozvoljeno korstiti samo oodbreni i verifikovani softver. Mora biti jasno i nedvosmisleno da prikazivanje rezultata generiše zakonski relevantan program.

Ako je standardni personalni računar sa Windows operativnim sistemom kao u ovom primeru deo mernog sistema, moraju se rešiti dva problema da bi se ER2.3 zadovoljilo:

- *program koji nije odobreni program mogao bi učitati ili proizvođač, prilikom instaliranja, ili neovlašćeno lice kada je sistem u upotrebi (k)[17k)]*
- *programi koji nisu odobreni program mogli bi kontrolisati prozore na ekranu, a prikazivanje mernih vrednosti moglo bi biti ometano ili blokirano (h, p)[18 h), p)]*

Instalranje programskog koda koji podleže zakonskoj kontroli *(ER2.3)*

U zakonske svrhe, proizvođač sme instalirati na sistem samo odobreni softver.

Primedbe u pogledu nivoa usaglašenosti *(ER2.3):*

Nizak: Proizvođaču je dozvoljeno da koriguje programski kod a da pri tome ne menja identifikaciju zakonskog softvera. Što se tiče zakonski relevantnih delova softvera (u primeru: biblioteka sa potprogramima koji podležu zakonskoj kontroli) imenovano telo mora, međutim, biti obavešteno u svakom slučaju. Prilikom verifikacije, odgovarajući organ ili odgovorno lice proverava pomoću identifikacije zakonskog softvera da li je softver koji se primenjuje u merilu ***usaglašen*** sa odobrenim softverom.

Srednji: Zakonski relevantan deo primenjenog softvera (u ovom primeru: biblioteka) mora biti identičan sa odobrenim softverom. Prilikom verifikacije, odgovarajući organ ili odgovorno lice proverava pomoću identifikacije zakonskog softvera (npr. potpis) da li je softver koji se primenjuje u merilu ***identičan*** sa odobrenim softverom.

Korisnik se može osloniti na ***žigove*** i ***verifikacionu oznaku*** u pogledu toga da je odobreni program instaliran.

Visok: Ako je nivo usaglašenosti propisan, tehničko rešenje iz ovog sistema primera ***nije*** pogodno. Celokupan softver, uključujući zakonski nerelevantne delove, mora biti identičan sa odobrenim softverom, a izmene softverskih delova nakon odobrenja tipa nisu dozvoljene.

---

[16] Specifikacija algoritma DEA iz [10]

[17 k)] Može se učitati bilo koji program. Učitavanje se može izvršiti pomoću izmenljivih uređaja za čuvanje podataka (disketa, CD-ROM i dr.) ili preuzimanjem sa servera preko interfejsa (na jedinicu čvrstog diska, Flash ROM, EEPROM i dr.).

[18 h)] Slobodan korisnički komandni interfejs sa uporednim radnim režimima koji podležu kontroli i radnim režimima koji ne podležu kontroli.

[18 p)] Softver koji podleže kontroli ugrađen je u okruženje kao i standardni operativni sistem koji nije posebno izrađen u merne svrhe.

Zamena programskog koda koji podleže zakonskoj kontroli, posle verifikacije *(ER2.3)*

Softver standardnog personalnog računara poput centralnog uređaja u ovom primernom sistemu može slobodno učitati čak i korisnik (k).

Primedbe u pogledu nivoa zaštite *(ER2.3):*

Nizak: Nisu potrebne nikakve mere zaštite od promene i zamene odobrenog programa.

Srednji: Pretpostavlja se da je uređivač teksta jedini alat koji se koristi za provaljivanje sistema, a ne prevodilac. Međutim, prevodilac bi bio potreban za pisanje novog programa koji ima slične funkcije sa odobrenim programom. Pretpostavlja se da je kazneno delo napisati takav program i zameniti njime odobreni tip. Zbog toga nisu potrebne nikakve mere za blokiranje učitavanja programa. (Što se tiče provaljivanja koda odobrenog programa kao i podataka i parametara, videti ER2.2.)

Napomena: *Ako proizvođač pravi programe slične odobrenom programu, ne sme ih instalirati na sistem koji se zakonski verifikuje i ne sme ih činiti dostupnim korisniku odobrenog sistema.*

Visok: Ako je nivo usaglašenosti propisan, tehničko rešenje iz ovog sistema primera ***nije*** podesno.

Primedbe u pogledu nivoa usaglašenosti *(ER2.3):*

Nizak/srednji: Korisnik i službenik za verifikaciju ili odgovorno lice mogu verifikovati da li je odobreni softver učitan i da li je aktiviran, poređenjem označene identifikacije zakonskog softvera sa identifikacijom koja je navedena na glavnoj pločici uređaja ili u sertifikatu o odobrenju tipa.

Visok: Ako je nivo usaglašenosti propisan, tehničko rešenje iz ovog sistema primera ***nije*** podesno.

Identikovanje zakonski relevantnog prikazivanja *(ER2.3)*

U ovom primeru može da se izvršava nekoliko programa uporedo. Moguće je da se na ekranu personalnog računara ne vidi samo prikazivanje zakonski relevantnog programa (h, p). Neka ograničenja se moraju poštovati kako bi se dao prioritet zakonski relevantnom prikazivanju.

Primedbe u pogledu nivoa zaštite *(ER2.3):*

Nizak: Nisu potrebne nikakve mere zaštite od pokazivanja falsifikovanih mernih vrednosti.

Srednji: Preptostavlja se da se za provaljivanje u sistem koristi uređivač teksta. Ne može se isključiti da se prikazivanje (fasifikovanih vrednosti) generiše pomoću modemskog (prozor) uređivača teksta. Zbog toga se u programu koji podleže kontroli moraju preduzeti tehničke mere da se to spreči. Postoje tri mere koje prihvatljivo tehničko rešenje treba da realizuje:

- *Merne vrednosti dobijene od senzorskih modula može obraditi samo programski deo koji ne podleže kontroli, a drugi programi nemaju pristup sve dok merne vrednosti još nisu pokazane (ili uskladištene u dugoročno skladište koje podleže kontroli). U trenutku kada su prikazane i/ili uskladištene one mogu se izvesti u programske delove koji ne podležu kontroli.*
- *Program koji podleže kontroli generiše prozor na ekranu za prikazivanje relevantnih podataka koji su uvek na vrhu, piše preko svih drugih prozora i osvežava se u određenim vremenskim intervalima. Ako prozor nije više na vrhu, obrada mernih vrednosti se prekida.*
- *Prozor za prikazivanje mernih vrednosti mora biti projektovan tako da se ne može pomešati sa prozorom koji generiše uređivač teksta. U radnom priručniku mora postojati kopija prozora kojeg generiše program koji podleže kontroli.*

Napomena: Pretpostavlja se da je kriminalna radnja napisati program koji je u stanju da obrađuje i pokazuje merne vrednosti umesto odobrenog programa ili uporedo s njim.

Visok: Ako je nivo usaglašenosti propisan, tehničko rešenje iz ovog sistema primera ***nije*** podesno.

Primedbe u pogledu nivoa ispitivanja *(ER 2.3):*

Nizak: Proizvođač *izjavljuje* (bez dostavljanja dokazne dokumentacije) da su preduzete mere kojim se prozor programa koji podleže kontroli uvek postavlja na vrh i da se merne vrednosti ne eksportuju u druge programe sve dok nisu prikazane ili uskladištene.

Srednji: Mere za zaštitu zakonski relevantnog prikazivanja ispituju se na osnovu softverske dokumentacije koju je proizvođač dostavio. Verifikuje se

- *da li merne vrednosti obrađuje isključivo zakonski relevantan program, sve dok se one ne prikažu ili uskladište;*
- *da je prozor za prikazivanje mernih vrednosti uvek na vrhu;*
- *da projekat tog prozora nije sličan prozoru uređivača teksta.*

	Praktično ispitivanje: Praktično se ispituje da se merni prozor ne može potisnuti i da je uvek na vrhu sve dok se merne vrednosti ne obrade.
Visok:	Pored koraka za srednji nivo, softver koji realizuje, npr. osvežava merni prozor, ispituje se koristeći izvorni kod.

ER2.4: Funkcionalni defekti koji mogu falsifikovati merne vrednosti u softverski kontrolisanom harveru moraju se otkriti i na njih se mora reagovati.

U primeru, neki delovi funkcionalnih defekata su otkriveni i softver realizuje odgovarajuću reakciju (r)[19r)].

Primedbe u pogledu nivoa ispitivanja:

Nizak:	Merilo se praktično ispituje uz pomoć radnog priručnika. Pošto se funkcionalni defekti događaju prilično retko, mehanizam za otkrivanje defekata se po pravilu ne ispituje.
Srednji:	Mehanizam za otkrivanje defekata koji je opisan u dokumentaciji proverava se simuliranjem odgovarajućih defekata.
Visok:	Mehanizam za otkrivanje defekata ispituje se u slučaju "srednji". Dodatno se simuliraju drugi defekti i ocenjuje se reakcija merila.

ER3.1: Softver koji se ne sme nedozvoljeno menjati nakon odobrenja tipa.

Koja vrsta modifikacija je dozvoljena zavisi od nivoa zahtevanog nivoa usaglašenosti:

Primedbe u pogledu nivoa usaglašenosti:

Nizak:	Primenjeni softver svakog pojedinačnog merila u saglasnosti je sa odobrenom dokumentacijom. Bez obzira na manje korekcije izvronog koda, funkcionalnost ostaje identična sa tehničkom dokumentacijom: ° Izmene zakonski relevantnog softvera dozvoljene su sve dok dokumentovane funkcije i karakteristike odobrenog merila ostaju nepromenjene. Međutim, NB[20]) mora o tome biti obavešten. Promene dokumentovanih funkcija i karakteristika zahtevaju dodatno odobrenje od strane NB i novu identifikaciju zakonskog softvera. ° Izmene dela koji ne podleže zakonskoj kontroli dozvoljene su bez informisanja NB sve dok se softverska razdvojenost poštuje i dok se isključivo koristi odobreni softverski interfejs. ° Odobrena softverska dokumentacija se čuva kod NB. Pored toga, izuzetno se može deponovati programski kod (izvršni kod) merila.
Srednji:	Zakonski relevantan deo primenjenog softvera svakog pojedinačnog merila identičan je sa odobrenim softverom: ° Zbog identiteta, izmene zakonski relevantnog softvera dovode do nove identifikacije zakonskog softvera. NB u tom slučaju daje dopunsko odobrenje. ° Izmene dela koji ne podleže zakonskoj kontroli dozvoljene su bez obaveštavanja NB sve dok se softverska razdvojenost poštuje i dok se isključivo koristi odobreni softverski interfejs. ° Odobrena softverska dokumentacija i kompletan programski kod (izvršni kod) merila čuvaju se kod NB.
Visok:	Celokupan softver svakog pojedinačnog merila identičan je sa odobrenim softverom: ° Zbog identiteta, izmene zakonski relevantnog softvera dovode do nove identifikacije zakonskog softvera. NB u tom slučaju daje dopunsko odobrenje. ° Odobrena softverska dokumentacija i kompletan programski kod (izvršni kod) merila čuvaju se kod NB.

ER3.2: Za verifikaciju usaglašenosti na raspolaganju mora biti identifikacija zakonski relevantnog softvera kao i odgovarajuće uputstvo.

Mora se obezbediti uputstvo za korisnika i službenika za verifikaciju kojim se objašnjava kako se označava identifikacioni broj zakonskog softvera. Od nivoa zahtevanog nivoa usaglašenosti zavisi kako se usaglašenost pojedinačnog merila proverava:

[19 r)] Prisustvo defekta nije očigledno i ne može se lako i jednostavno proveriti pomoću drugog uređaja osim samog merila i nema harverskih sredstava za otkrivanje defekata.

[20] NB – Imenovano telo ili ispitivač projekta

Primedbe u pogledu nivoa usaglašenosti:

Nizak: Primenjeni softver svakog pojedinačnog merila u saglasnosti je sa odobrenom dokumentacijom. Bez obzira na manje korekcije izvornog koda, funkcionalnost ostaje identična sa tehničkom dokumentacijom:

° Prilikom verifikacije, usaglašenost sa odobrenim softverom proverava se pomoću identifikacije zakonskog softvera koja je navedena u sertifikatu o odobrenju tipa. Identifikacija zakonskog softvera može se prikazati na zahtev ili automatski pri pokretanju ili ciklično).

Srednji: Zakonski relevantan deo primenjenog softvera svakog pojedinačnog merila identičan je sa odobrenim softverom:

° Prilikom verifikacije, usaglašenost sa odobrenim softverom proverava se pomoću identifikacije zakonskog softvera (potpis) koja je navedena u sertifikatu o odobrenju tipa.

Visok: Celokupan softver svakog pojedinačnog merila identičan je sa odobrenim softverom:

° Prilikom verifikacije, usaglašenost sa odobrenim softverom proverava se pomoću identifikacije zakonskog softvera (potpis) koja je navedena u sertifikatu o odobrenju tipa.

ER4.1: Funkcionalnost merila mora biti moguće ispitati.

Kako se pretpostavlja u opisu primernog sistema, ovde je realizovan složen merni proces. Metrološka ispitivanja su teška i ne mogu se često ponavljati.

Primedbe u pogledu nivoa ispitivanja:

Nizak: Proizvođač dostavlja rezultate niza merenja, opis uslova u toku merenja i izjavu da su te merne vrednosti dobijene pomoću softverske verzije koju treba odobriti. Rezultate merenja proverava ispitivač. Druge karakteristike softvera osim onih koje ova merenja ne obuhvataju, proizvođač ne mora da ispita. Dovoljno je da izjavi da su te neispitane karakteristike u skladu sa zahtevima (zaštitni interfejs, otkrivanje defekata i reakcija i dr.).

Posledice po proizvođača/podnosioca zahteva: Dovoljno merenja mora se obaviti i uporediti sa nazivnim vrednostima. Rezultati moraju biti dokumentovani. Raspored merne opreme i uslovi u toku merenja moraju biti dokumentovani.

Srednji: Metrološki ulazni signali za tumačenje delova softvera simuliraju se pomoću posebnog ispitnog uređaja ili ispitnog softvear. Rezultati koje izračunava softver merila tretiraju se kao da su stvarne merne vrednosti. U ovom primeru ne postoji specijalan interfejs neophodan za unos simuliranih skupova podataka.

Pored tih simuliranih ispitivanja vrše se neka praktična ispitivanja na osnovu specijalne softverske dokumentacije. Iz rezultata te analize ispitivač može izvesti dodatna ispitivanja na stvarnom merilu (npr. ispitivanje funkcionisanja otkrivanja defekata i reakcija).

Posledice po proizvođača/podnosioca zahteva: Merilo mora biti opremljeno sa jednim ili više interfejsa za praćenje mernih signala ili tokova podataka ili za unošenje simuliranih signala ili tokova podataka. U slučaju potrebe, mora se staviti na raspolaganje odgovarajući simulatorski uređaj ili program.

Visok: Metrološki ulazni signali za tumačenje delova softvera simuliraju se pomoću posebnog ispitnog uređaja ili ispitnog softvera. Rezultati koje izračunava softver merila tretiraju se kao da su stvarne merne vrednosti. U ovom primeru nema posebnog interfejsa koji je potreban za unos simuliranih vrednosti jer je komunikacijska sabirnica pogodna za povezivanje simulatora i unos simuliranih skupova podataka.

Mora se dostaviti izvorni kod. Ispitivanje performanse metrološkim simulatorom još nije zastarelo jer je vrlo efektivno. Međutim, delovi softvera mogu se ispitati "ručno" (dobro poznate metode, kontrolisanje koda, proba, itd.) ili pomoću softverskih alata za analizu. Tipični primeri tih praktičnih ispitivanja su zaštitni interfejs, razdvajanje softvera na delove i dr.

Posledice po proizvođača/podnosioca zahteva: Merilo mora biti opremljeno sa jednim ili više interfejsa za praćenje mernih signala ili tokova podataka ili za unošenje simuliranih signala ili tokova podataka. U slučaju potrebe, mora se staviti na raspolaganje odgovarajući simulatorski uređaj ili program.

ER5.1: Zakonski relevantan softver, zajedno sa svojim hardverskim i softverskim okruženjem, mora biti na odgovarajući način dokumentovan.

Za module mernog sistema kao u ovom primeru (tehnička klasa videti 6.2.3), proizvođać mora da dostavi najmanje sledeću dokumentaciju:

Primedbe u pogledu nivoa ispitivanja:

Nizak: Proizvođač dostavlja radni priručnik i tehničku dokumentaciju. Nije potrebna nikakva posebna softverska dokumentacija. Dokumentacija treba da sadrži izjave proizvođača o nekim karakteristikama merila koje nisu ispitane (npr. da je interfejs izrađen kao zaštitni) i identifikaciju zakonskog softvera.

Srednji: Pored dokumentacije za nizak nivo, posebna softverska dokumentacija mora obuhvatati:

- detaljan opis svih zakonski relevantnih softverskih funkcija, zakonski relevantnih parametara koji određuju funkcionalnost merila,
- opis algoritama za merenje (npr. algoritmi za izračunavanje cene i za zaokruživanje)
- opis menija i dijaloga
- identifikacija zakonskog softvera
- kompletan opis komandi i parametara preko zaštitnog interfejsa, uključujući izjavu o kompletnosti tog opisa
- kompletan opis komandi i parametara preko zaštitnog softverskog interfejsa, uključujući izjavu o kompletnosti tog opisa
- opis skupova podataka uskaldištenih ili prenetih podataka
- neophodne karakteristike radnog sistema i hardvera računara
- upućivanje na zahteve iz ovog vodiča
- radni priručnik.

Visok: Pored dokumentacije za nivo "srednji", proizvođač mora dostaviti izvorni kod (kao fajl), zajedno sa određenom pomoćnom dokumentacijom poput

- logičkog dijagrama softvera (npr. dijagram toka ili Nase-Šnejdermanov dijagram (Nassi-Shneidermann diagram))
- detaljanog opisa funkcija svakog zakonski relevantnog softverskog modula
- opis struktura podataka (skupovi prenetih podataka).

7 Reference i ostala literatura

[1] Direktiva 2004/22/EZ Evropskog parlamenta i Saveta od 31. marta o merilima. Službeni list Evropske unije L 135/1, 30.4.2004.

[2] Direktiva Saveta 90/384/EEZ o harmonizaciji zakonodavstava država članica u vezi sa vagama sa neautomatskim funkcionisanjem. Službeni list Evropskih zajednica, L 189, Vol. 33, 20.7.1990, 1-16

[3] Vodič za ispitivanje softvera (vage sa neautomatskim funkcionisanjem), WELMEC 2.3, 1995.

[4] IEC 65(Sec)183 Sofverska dokumentacija, 1994.

[5] ISO 7498-1 to -4, Informaciona tehnologija – Međusobno povezivanje otvorenih sistema, 1989 - 1997

[6] ISO/IEC 9126 Informaciona tehnologija; Vrednovanje softverskih proizvoda, oktobar 1994.

[7] ISO/IEC 12119 Informaciona tehnologija; Softverski paketi; Zahtevi kvaliteta i ispitivanje, avgust 1995.

[8] Kriterijumi za vrednovanje sigurnosti informacione tehnologije (ITSEC), juni 1991, Verzija 1.2, Dokument COM(90) 314, Luksemburg

[9] ISO 8731-1:1987 Bankarstvo – Odobreni algoritmi za utvrđivanje verodostojnosti poruke - Deo 1 : DEA

[10] ISO 10126-2:1991 Bankarstvo – Postupci pri šifrovanju poruka - Deo 2: DEA algoritam

[11] ITU-T (bivši CCITT) V.42

[12] ISO/IEC 13239 Informaciona tehnologija – Telekomunikacije i razmena informacija između sistema – Postupci za kontrolu veze podataka visokog nivoa (HDLC), 1996

[13] Security of computerized instruments, Jean-François Magana, OIML Bulletin Volume XL, Number 3, July 1999

[14] ISO 2382-1, Informaciona tehnologija , Deo 1: Osnovni termini, 1993 ISO 2382-7, Informaciona tehnologija, Deo 7: Kompjutersko programiranje, 1989

[15] Vodič za softverske zahteve i validaciju, Verzija 1.00, 29.oktobar 2004, Evropska mreža za razvoj *"MID-Softver",* broj ugovora G7RT-CT-2001-05064, 2004

[16] Vodič za softver (Direktiva o merilima 2004/22/EZ), WELMEC 7.2, Izdanje 1, 2005

8 Revizije ovog dokumenta

Izdanje	Datum	Značajne izmene u odnosu na prethodno izdanje
2	Maj 2005.	Izmene i dopune naslova i sledećih odeljaka (radi usklađivanja sa WELMEC Vodičem 7.2): 1.1, 3, 4, 4.1, 7
		Novi odeljci koji su dodati: Mapa na omotu, Predgovor, 8
		Prilog I izbrisan.