

TEMPEST

specificaties en testmethoden voor elektronische stemapparatuur

Inhoudsopgave

1. Inleiding	4
1.1 Achtergrond.....	4
1.2 Doel	4
1.3 Reikwijdte en toepasselijkheid	5
2. TEMPEST-specificaties.....	6
3. Testmethoden.....	8
3.1 Testconfiguratie.....	8
3.2 Testprocedure	9
3.3 Testfrequentie	10
4. Richtsnoeren voor fabrikanten en andere randvoorwaarden	12
4.1 Richtsnoeren voor fabrikanten	12
4.2 Richtsnoeren voor software	13
4.3 Richtsnoeren met betrekking tot de omgeving.....	13
5. Aanhangsels.....	14
Aanhangsel A	14
Aanhangsel B	16
Aanhangsel C	19

Dit document is opgesteld door GBS mbH (Gesellschaft für Beratung und Schulung mbH – Company for economic consultancy and training).

Auteurs:

Dr. Markus Kuhn
Gerhard Friedrichs
Ahmet Aksoy
Enrico Koch
Lars Friedrichs

1. Inleiding

In dit document worden de TEMPEST-eisen ten aanzien van elektronische stemapparatuur¹ uiteengezet. Het document behandelt tevens de desbetreffende testmethoden en biedt richtsnoeren ten behoeve van de fabrikanten van elektronische stemapparatuur.

1.1 Achtergrond

Alle IT-apparatuur, ook die in een elektronisch stemapparaat, zendt elektromagnetische straling uit die informatie bevat; in technische termen wordt dit compromitterende straling of compromitterende emanatie genoemd. Deze emanatie bevat gegevens die op dat moment worden verwerkt. Noch firewalls, noch antivirusprogrammatuur kunnen spionnen verhinderen compromitterende emanatie te ontvangen en gevoelige gegevens uit te lezen; dit wordt een TEMPEST-aanval genoemd. Wanneer informatie als vertrouwelijk wordt beschouwd, behoort deze wijze van afluisteren te worden voorkomen. Aangezien verkiezingen uit hoofde van het nationale recht en internationale verdragen bij geheime stemming moeten plaatsvinden, dienen de bij een verkiezing individueel uitgebrachte stemmen als vertrouwelijke informatie te worden aangemerkt. Derhalve is het wenselijk dat elektronische stemapparatuur tegen afluisteren wordt beschermd door middel van het afvangen van de uitgezonden straling.

Er bestaan militaire normen waarin eisen op het gebied van TEMPEST worden gespecificeerd. Er zijn twee redenen waarom een nieuwe set is ontwikkeld.

Allereerst zijn de bestaande militaire voorschriften geheim en derhalve niet bruikbaar voor het toepassingsgebied. De in dit kader te formuleren eisen worden gepubliceerd, zodat geïnteresseerden deze informatie kunnen gebruiken.

Ten tweede zijn de militaire normen ontwikkeld vanuit een bepaald standpunt ten opzichte van computers en andere IT-hardware. Bij de militaire normen worden bepaalde aannames gedaan die niet per se voor elektronische stemapparatuur opgaan. Derhalve zijn de militaire normen niet rechtstreeks op elektronische stemapparatuur toepasbaar.

1.2 Doel

In dit document worden de grenswaarden gedefinieerd voor de straling die door elektronische stemapparatuur wordt uitgezonden, alsmede de desbetreffende testprocedures om vast te stellen of een apparaat al dan niet aan de eisen voldoet. Teneinde deze grenswaarden vast te stellen, worden aannames gedaan met betrekking tot de capaciteiten van de aanvaller. Meer in het bijzonder worden aannames gedaan met betrekking tot de antenneapparatuur waarover een eventuele aanvaller beschikt en de afstand waarop de afluisterapparatuur van de elektronische stemapparatuur kan worden geplaatst zonder te worden gedetecteerd.

Voorts worden richtsnoeren voor stemapparatuur beschreven die van nut kunnen zijn om aan de eisen te kunnen voldoen. Bovendien worden richtsnoeren geformuleerd ten behoeve van stemlokalen en stemprogrammatuur.

Deze eisen met alle details worden publiekelijk beschikbaar.

¹ Noot bij de vertaling: De termen "stemapparatuur" en "stemapparaat" kunnen zowel verwijzen naar stemmachines als naar stemprinters.

1.3 Reikwijdte en toepasselijkheid

Deze eisen zijn van toepassing op alle elektrische, elektronische, elektromechanische en optronische apparatuur die wordt gebruikt voor het selecteren en/of uitbrengen van een stem in een verkiezingsproces, hetzij in analoge hetzij in digitale vorm. Deze eisen zijn niet van toepassing op het tellen van de stemmen.

Het is de bedoeling dat dit document wordt gebruikt door lokale en nationale verkiezingsfunctionarissen, fabrikanten, dienstverleners en accreditatieorganisaties. Stemapparaten kunnen worden getest aan de hand van deze eisen. Na onderhoud of aanpassing van een stemapparaat moet het apparaat opnieuw aan een test worden onderworpen.

Dit document is niet bedoeld voor het testen van de kwaliteit van de individuele componenten waaruit de specifieke apparatuur is opgebouwd, en ook niet voor de gebruikte stemprogrammatuur.

2. TEMPEST-specificaties

Een elektronisch stemapparaat kan als TEMPEST-proof worden beschouwd indien de compromitterende emanatie niet door derden onder de volgende aannames kan worden opgevangen:

- De af luisteraar is niet in staat een antenne met een antenneopening van groter dan 1 vierkante meter dicht bij het doel te brengen dan 5 meter (of vier maal die antenneopening op twee maal die afstand, of $\frac{1}{4}$ van de antenneopening op de halve afstand, enz. Dit is uitsluitend ter informatie om aan te geven met welke problemen een af luisteraar te maken heeft. Het is niet mogelijk een exacte mathematische correlatie aan te geven tussen de afstand en opening van een antenne. De opening van een antenne hangt ook samen met het bereik van de antenne die wordt gebruikt.)
- De af luisteraar voert zijn aanval uit in een normale omgeving en niet binnen een speciaal afgeschermd ruimte; derhalve staat hij bloot aan het minimumniveau van atmosferische achtergrondruis die normaal gesproken kan worden verwacht op een stille ontvangerlocatie, overeenkomstig de referentiegegevens van ITU-R aanbeveling P.372.

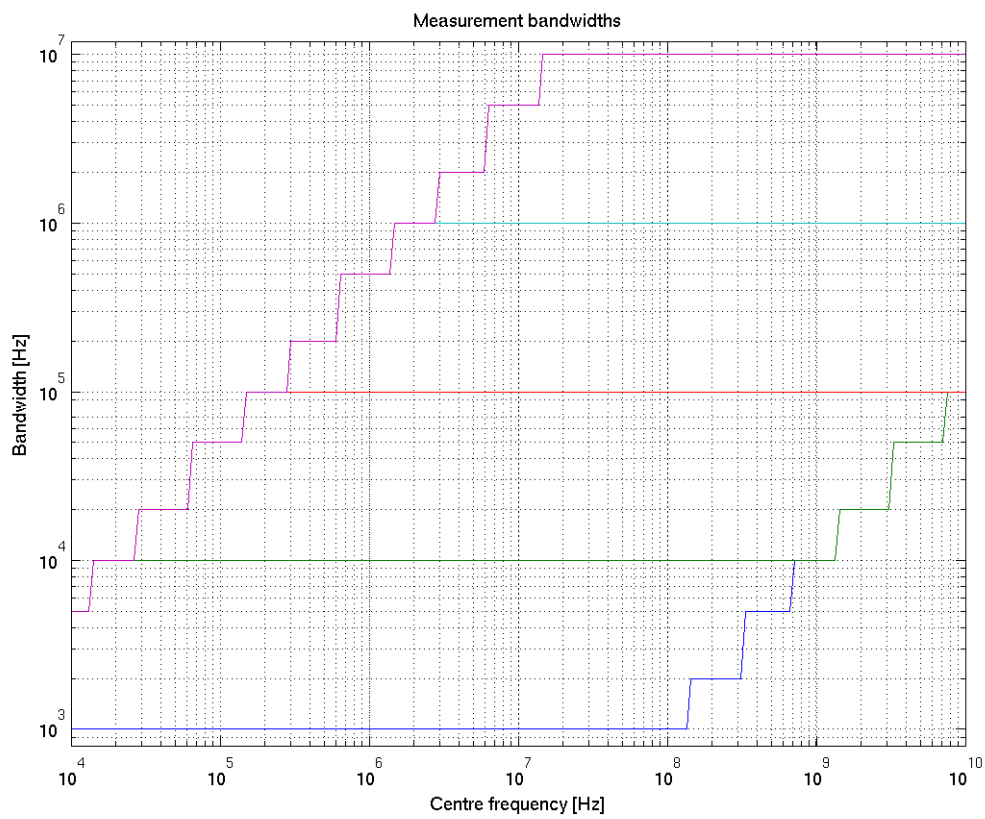
Alle elektronische apparatuur moet aan de TEMPEST-specificaties voldoen en worden getest voordat de apparatuur in gebruik wordt genomen. Om aan de TEMPEST-specificaties te voldoen, moet aan de hieronder beschreven eisen worden voldaan alsmede aan de Europese normen voor elektromagnetische compatibiliteit (EMC, hier gedefinieerd door EMV-norm 89/336/EWG en EMV-norm 2004/108/EG)² Indien de EMC-normen en de in dit document genoemde eisen verschillende emanatieniveaus toestaan, moet de zwaarste eis worden gehanteerd.

In deze paragraaf worden vijf emanatiecurves behandeld. Deze vormen de bovengrenswaarden voor de sterkte van de elektromagnetische signalen die door elektronische stemapparatuur mag worden uitgezonden. De emanatiecurves (ook wel elektronischestemcurves) zijn in de figuren 1 en 2 opgenomen. De eisen hebben betrekking op emanaties in het bereik van 10 kHz tot 10 GHz.

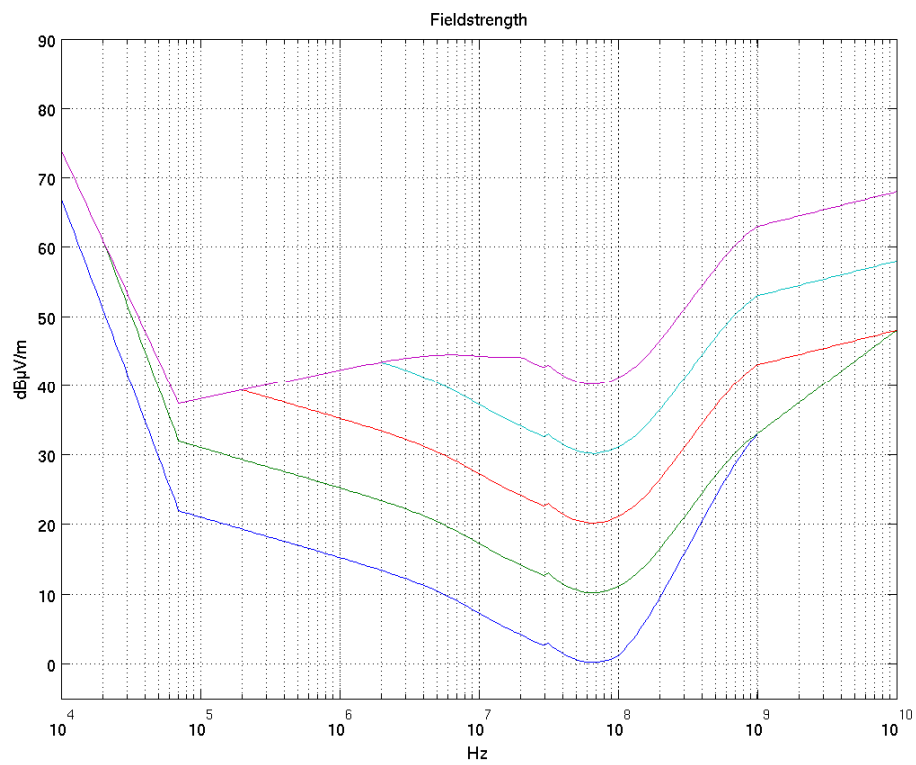
De figuren 1 en 2 moeten als volgt worden gelezen. De bovengrenzen worden gedefinieerd aan de hand van de veldsterkte van de uitgezonden straling in een specifieke bandbreedte B rond een middenfrequentie f. In figuur 1 wordt bandbreedte B getoond die bij elke middenfrequentie hoort. Figuur 2 geeft de maximum veldsterkte weer die is toegestaan in de frequentieband $f \pm \frac{1}{2} B$.

De op deze wijze gedefinieerde lijnen vormen de bovengrens voor de elektromagnetische veldsterkte van een elektronisch stemapparaat. Van apparatuur die de grenswaarden voor de maximum veldsterkte niet overschrijdt, wordt aangenomen dat deze voldoende beschermd is tegen het risico van elektromagnetisch af luisteren, uitgaande van bovengenoemde aannames.

² Een Europese fabrikant moet een verklaring afgeven waarin staat dat een nieuw apparaat aan de eisen van dit voorschrift voldoet



Figuur 1



Figuur 2

3. Testmethoden

De testmethoden en procedures voor het aantonen van de conformiteit met de in dit document genoemde TEMPEST-specificaties zijn algemeen toepasbaar, ongeacht het type stemapparaat of de door de fabrikant toegepaste TEMPEST-tegenmaatregelen.

Het is raadzaam het elektronische stemapparaat na afloop van de TEMPEST-meting te verzegelen zodat het onmogelijk is het apparaat te openen zonder dat dit zichtbaar is. Een intacte verzegeling in combinatie met een certificaat waaruit blijkt dat het elektronische stemapparaat door een geaccrediteerd laboratorium is goedgekeurd, biedt een TEMPEST-garantie wat betreft de integriteit van het elektronische stemapparaat.

In dit hoofdstuk wordt beschreven welke procedures en configuratie van de testapparatuur benodigd zijn om de test uit te voeren.

3.1 Testconfiguratie

Voordat de test wordt uitgevoerd, moet de testprogrammatuur in het elektronische stemapparaat worden geladen. Deze testprogrammatuur voert geen simulatie van het stemproces uit, maar veroorzaakt een situatie waarbij het elektronische stemapparaat zoveel mogelijk straling uitzendt. Op deze wijze kan het met de elektronische stemprogrammatuur uitgeruste elektronische stemapparaat geen sterkere emanaties veroorzaken dan het elektronische stemapparaat onder testomstandigheden, namelijk wanneer het stemapparaat van de testprogrammatuur is voorzien. Het doel is via metingen na te gaan of het met de testprogrammatuur uitgeruste apparaat de door de elektronische stemcurves aangegeven grenswaarden voor de maximale veldsterkte niet overschrijdt. Indien de gemeten straling onder de elektronische stemcurves blijft, luidt de gevolgtrekking dat het elektronische stemapparaat voldoende beschermd is tegen het risico van elektromagnetisch afluisteren. De testprogrammatuur is niet alleen nodig voor de accreditatiemeting, maar ook voor de latere compliancetests (zie paragraaf 3.2).

De testconfiguratie bestaat uit antennes voor verschillende frequenties, een ontvanger / spectrumanalyseapparaat en een PC met printer.

De ontvanger en/of het spectrumanalyseapparaat moeten de volgende specificaties bezitten:

- een frequentiebereik van 10 kHz tot 10 GHz; in dit bereik vinden doorgaans de activiteiten plaats waarop de TEMPEST-eisen van toepassing zijn. Daarom is het zeer belangrijk dit bereik bij de accreditatiemeting te testen.
- tussenliggende frequentiebandbreedtes (RBW) van 10 Hz tot 500 MHz in stappen van 1/2/5; deze RBW worden omgezet in de in figuur 1 en 2 getoonde meetcurves;
- ruisgetal van minder dan 3 dB; een ruisgetal van meer dan 3 dB is mogelijk. Uit ervaringen in het TEMPEST-veld blijkt dat een laag ruisniveau beter functioneert; daarom wordt voor TEMPEST-metingen een ruisgetal van 3 dB aanbevolen;
- frequentieresolutie 0,1 Hz. De ervaringen binnen het TEMPEST-veld wijzen in de richting van deze frequentieresolutie; een hogere resolutie is mogelijk, maar minder nuttig.

De piekwaardedetectormodus moet worden gebruikt en de scanduur moet worden aangepast om de vereiste intervaltijd in te stellen. De intervaltijd voor elke frequentie bedraagt ten minste 50 ms, of tweemaal zo lang als de lusinterval van de testprogrammatuur, naar gelang van welke tijd langer is.

De antennes moeten geschikt zijn voor metingen in een frequentiebereik van 10 kHz tot 10 GHz. De meetantennes worden op de ontvanger c.q. het spectrumanalyseapparaat aangesloten; dit apparaat wordt vervolgens aan de pc/printer gekoppeld.

Tijdens de testfase wordt de ontvanger / het spectrumanalyseapparaat gecontroleerd via een aangesloten PC, waarmee ook de gegevensregistratie wordt bijgehouden.

De metingen moeten worden uitgevoerd in een meetcabine die is afgeschermd tot 18 GHz. Dit is gebruikelijk voor TEMPEST-metingen. Buitenmetingen zijn voor dit doel niet geschikt.

3.2 Testprocedure

De meetprocedure bestaat uit twee fasen, namelijk een accreditatiemeting en een compliance-meting.

Accreditatiemeting vindt plaats bij elk type elektronisch stemapparaat. Indien een elektronisch stemapparaat wordt aangepast, wordt het apparaat als een nieuw type beschouwd en is een nieuwe accreditatiemeting nodig.

Voorbeelden van mogelijke aanpassingen zijn:

- een nieuw type moederbord of modificatie van het moederbord;
- andere schermgrootte, ander type scherm, aanpassing van het scherm, andere schermfabrikant;
- ander ontwerp van de behuizing;
- ander model printer of modificatie van de printer;
- elke andere aanpassing van elektrische of afschermingsonderdelen.

Een accreditatiemeting omvat een volledige test: er wordt gemeten of de uitgestraalde emanaties zich onder de vijf in figuur 1 en 2 afgebeelde emanatiecurves bevinden.

Vervolgens wordt op elk elektronisch stemapparaat van hetzelfde type uitsluitend een compliance-meting verricht. De compliance-meting neemt beduidend minder tijd in beslag dan de accreditatiemeting. Hieronder wordt nadere informatie verstrekt met betrekking tot beide meetprocessen.

A. Accreditatiemeting

- Elk meetproces wordt tweemaal uitgevoerd, eenmaal voor de verticale en eenmaal voor de horizontale polarisatie van de antenne.
- De emanaties van het te testen elektronische stemapparaat worden van twee zijden gemeten: met de antenne vóór het apparaat en met de antenne achter het apparaat.
- Bij de uitvoering van de metingen moeten in de meetcabine de volgende afstanden in acht worden genomen:

De afstand tussen de te testen apparatuur en de wanden moet ten minste 1 m bedragen;
de afstand tussen de antenne en de wanden moet ten minste 1 m bedragen;

de geringste afstand tussen de te testen apparatuur en het calibratiepunt van de antenne bedraagt 1 m;

- Het elektronische stemapparaat moet de testprogrammatuur booten en in de testmodus draaien.
- De testrun moet worden geregistreerd via een PC die zich buiten de meetcabine bevindt.
- Het meetresultaat moet worden geregistreerd door middel van een hardcopy waarin de gedefinieerde stemcurve als nominale waarde en het meetresultaat in de vorm van een grafiek wordt getoond.
- Deze meting neemt circa vier uur in beslag.

B. Compliance-meting

Bij de compliance-meting moet dezelfde procedure worden gevolgd als bij de accreditatiemeting, zij het met de volgende uitzonderingen:

- Er wordt uitsluitend getest of de uitgezonden stralingen zich onder de lijn voor breedbandstralingen bevinden (de rode lijn in figuren 1 en 2) en onder de twee lijnen voor smalbandmetingen (de groene en blauwe lijnen in figuren 1 en 2).
- De meting met de verticale polarisatie van de antenne wordt niet uitgevoerd.
- De meting waarbij de antenne achter het elektronische stemapparaat wordt aangebracht, wordt niet uitgevoerd.
- Deze metingen nemen circa 25 minuten in beslag.

3.3 Testfrequentie

De compliancetest van elektronische stemapparatuur moet op elk apparaat worden uitgevoerd. Dit is nodig om de volgende redenen:

- Identieke componenten van elektronische stemapparaten van een en hetzelfde type kunnen zich op TEMPEST-gebied verschillend gedragen. Stemapparaten van een en hetzelfde type kunnen zich op TEMPEST-gebied derhalve eveneens verschillend gedragen, zelfs indien de constructie en functies exact hetzelfde zijn. Het is mogelijk dat sommige apparaten voldoen aan de TEMPEST-voorschriften en andere niet.

- Indien de in paragraaf 4.3 genoemde richtsnoeren voor de stemlokalen niet kunnen worden gegarandeerd, kan het falen van een enkel stemapparaat tot gevolg hebben dat de verkiezingen niet langer geheim zijn. Vooral in gevallen waarin geen waarborgen wat betreft de stemlokalen mogelijk zijn, moet elk apparaat worden getest. Enkel een statistische meting van stemapparaten biedt geen waarborg voor een afdoende bescherming.

Om er zeker van te zijn dat een apparaat nog steeds aan de TEMPEST-voorschriften voldoet, moeten alle apparaten binnen een tijdsbestek van twee jaar opnieuw worden getest.

Een TEMPEST-meting toont slechts aan dat het geteste apparaat op het tijdstip van de meting voldoet aan de voorschriften voor de desbetreffende TEMPEST-producten. Deze kenmerken kunnen door verschillende activiteiten worden gewijzigd:

- Een component van het apparaat kan, net als een elektrische condensator, met het verstrijken van de tijd aan kleine veranderingen onderhevig zijn. Dit hoeft niet per se te leiden tot ondeugdelijk functioneren van het gehele apparaat, maar kan wel tot gevolg hebben dat niet langer aan de TEMPEST-eisen wordt voldaan.
- Het vervoeren of anderszins verplaatsen van het apparaat kan ertoe leiden dat niet langer aan de TEMPEST-eisen wordt voldaan. Elk TEMPEST-laboratorium zal de aansprakelijkheid ter zake afwijzen.

4. Richtsnoeren voor fabrikanten en andere randvoorwaarden

Dit hoofdstuk bevat adviezen voor fabrikanten om elektronische stemapparaten te construeren die aan de TEMPEST-normen voldoen. De adviezen betreffen ook de omstandigheden in en om het stemlokaal.

4.1 Richtsnoeren voor fabrikanten

In deze richtsnoeren worden specifieke aandachtspunten genoemd die bij het ontwerp van de hardware voor elektronische stemapparatuur in acht moeten worden genomen om compromitterende straling te voorkomen. Enkel voldoen aan deze richtsnoeren biedt echter geen garantie dat hiermee ook aan de in dit document vereiste TEMPEST-eisen wordt voldaan. Voor het laden van de TEMPEST-testprogrammatuur in het elektronische stemapparaat moet het apparaat van een DVD-speler of een ander 'read only'-invoerapparaat zijn voorzien.

- Het elektronische stemapparaat moet zijn vervaardigd van geleidend metaal; de enige noodzakelijke openingen zijn die voor het touchscreen, de datalinks, de voedingskabels en de opening die toegang geeft tot de uitvoer van de stemprint.
- De printer moet in het elektronische stemapparaat zijn geïntegreerd.
- Uit TEMPEST-oogpunt moeten speciale technische componenten en onderdelen worden geselecteerd voor de printer, het touchscreen en de hoofdtelefoons van het elektronische stemapparaat.
- Het stembureau is niet bevoegd het stemapparaat te openen, behalve de printer voor het bijvullen van papier; alleen het gedeelte waarbinnen de stemactiviteiten plaatsvinden moet worden verzegeld.
- Het papierformaat mag niet groter zijn dan A6.
- Het is van belang dat elektronische stemapparatuur zo min mogelijk openingen heeft. Als er openingen zijn, moeten deze rond zijn. Aangeraden wordt openingen, zoals de opening voor de uitvoer van de stemprint, met een afdekking te beschermen.
- De voedingskabels moeten worden afgeschermd. De communicatie tussen de elektronische stemapparatuur en het bedieningspaneel van de medewerkers van het stembureau moet verlopen via glasvezelkabels of via een afgeschermd kabel.
- Voor eventueel op de elektronische stemapparatuur aangesloten hoofdtelefoons, gelden de volgende eisen:
 - * de aansluiting van de hoofdtelefoon moet van het schroefbare type zijn en geen plug
 - * de kabel moet zijn afgeschermd
 - * de hoofdtelefoon zelf moet zijn afgeschermd.
- USB-aansluitingen moeten worden afgeschermd

4.2 Richtsnoeren voor programmatuur

In deze richtsnoeren worden aandachtspunten genoemd voor het ontwerp van de programmatuur die in elektronische stemapparatuur wordt gebruikt. Hoewel deze maatregelen de testresultaten niet beïnvloeden, kunnen ze het risico van geavanceerde TEMPEST-aanvallen aanzienlijk reduceren. Als besturingssysteem moet worden gedacht aan een speciale "uitgeklede" versie van Linux: Het Linux-besturingssysteem biedt de mogelijkheid overbodige functies van het besturingssysteem weg te laten.

- Via speciaal geprogrammeerde programmatuur moeten de op het scherm getoonde kleuren (in lichte mate) worden gewijzigd (zodanig dat dit voor de kiezer onmerkbaar is). Dit kan worden gedaan door het maken van een enkel frame "white noise" in de 5 minst significante bits van elke kleur.
- De programmatuur moet zodanig worden geprogrammeerd dat een "anti-aliasing"-systeem ontstaat. De programmatuur zorgt ervoor dat de op het scherm afgebeelde knoppen die door een kiezer kunnen worden "ingedrukt", zich over minieme afstand verplaatsen of roteren. De verplaatsing van de knoppen op het scherm is voor de kiezer onzichtbaar.
- De toepassing van zogeheten "rustling"-routines die de positie of lettergrootte van de op het scherm getoonde karakters (in lichte mate) veranderen (niet zichtbaar voor de kiezer).

4.3 Richtsnoeren met betrekking tot de omgeving

In deze paragraaf worden aanvullende richtsnoeren beschreven voor de omgeving waarin elektronische stemapparatuur wordt geplaatst, d.w.z. richtsnoeren voor een stemlokaal.

- Een elektronisch stemapparaat kan het best tegenover de ramen worden geplaatst.
- In het stemlokaal mag geen andere technische apparatuur worden gebruikt (ook mobiele telefoons moeten worden uitgeschakeld).
- Er moet beleid zijn voor het veilig controleren van een verzegeld apparaat wanneer een apparaat moet worden vervangen.

5. Aanhangsels

Aanhangsel A

Ontwerpachtergrond

Bij het meten van compromitterende emanaties moet bijzondere aandacht aan de bandbreedte worden besteed. Indien de meetbandbreedte te groot is, kan een zwak smalbandsignaal dat door een af luisteraar met een zorgvuldig gekozen IF-smalbandontvanger kan worden opgevangen bij de compliance test niet worden onderscheiden van de meetruis. Indien de meetbandbreedte te klein is, kan een breedbandpulssignaal dat door een aanvaller via een zorgvuldig gekozen bandbreedte kan worden opgevangen, tijdens de test evenmin worden onderscheiden. Aangezien een af luisteraar bruikbare signalen kan opvangen over een groot bandbreedtebereik dat uiteenloopt van 1 kHz tot meerdere tientallen MHz, bestaat er niet zoiets als een enkele meetbandbreedte waarmee zowel smal- als breedbandsignalen kunnen worden opgevangen.

Derhalve moeten meerdere sweeps worden uitgevoerd met verschillende drempelcurves en meetbandbreedtes. De keuze van 1 KHz als kleinste bandbreedte dekt de signaaltypes die een af luisteraar met een AM audio-ontvanger zou kunnen opvangen. De keuze van 10 MHz als grootste bandbreedte heeft vooral betrekking op videosignalen. Hier tussenin verkrijgt een af luisteraar die op zoek is naar een signaal van een bit of symbol rate f doorgaans de beste resultaten met meetbandbreedtes binnen het bereik $f/2$ tot $5f$. Een serie sweeps waarbij de opeenvolgende bandbreedtes met een factor 10 afwijken, vormt een goed compromis tussen de dekking van alle bandbreedtes die een aanvaller zou kunnen kiezen en de voltooiing van de compliance meting binnen een redelijk tijdsbestek.

Bij elke sweep wordt begonnen met 10 kHz en wordt de bandbreedte verruimd (normaliter in de reeks 1-2-5-10), zodanig dat de bandbreedte nooit groter is dan de helft van de centrumfrequentie. De eerste limiet voorkomt combinaties van frequentie en bandbreedte waarbij de ruisprestaties van sommige spectrumanalyseapparaten teruglopen, de tweede limiet reduceert de scanduur. Wanneer twee sweeps elkaar zowel qua frequentie als bandbreedte overlappen, hoeft de meting niet te worden herhaald, aangezien de overeenkomstige drempelcurves elkaar eveneens overlappen.

De drempelcurves worden als volgt bepaald:

- Eerst berekenen we de laagste atmosferische of galactische ruiswaarden die kunnen worden verwacht op een stille ontvangerlocatie, overeenkomstig ITU-R Aanbeveling p.372-7 (doorlopende lijn in de figuren 2 en 3), of een ruistemperatuur van de antenne van 290 K, naar gelang van welke waarde hoger is (om rekening te houden met het feit dat een af luisterdoel doorgaans een achtergrondtemperatuur van circa 20 graden Celsius (kamertemperatuur) heeft).
- Vervolgens wordt een compensatie toegepast voor het feit dat de antenne zich op een afstand van 1 m bevindt, terwijl de antenne van de af luisteraar zich op een afstand van ten minste 5 m bevindt.
- Vervolgens compenseren we voor het feit dat een af luisteraar niet alleen een eenvoudige dipoolantenne, maar ook een Aygi-Uda-, hoorn- of parabolantenne zou kunnen gebruiken, elk met een maximum opening van 1 vierkante meter (op een afstand van 5 m).
- Ook wordt rekening gehouden met de gevoeligheidslimiet van beschikbare actieve antennesets van het type dat doorgaans voor het meten van compromitterende emanaties wordt gebruikt.

- Ook wordt rekening gehouden met ontvangerruis.
- Al deze factoren worden meegenomen om uiteindelijk zodanige drempellimieten in te stellen dat een af luisteraar geen betere signaal-ruisverhouding kan verwachten dan 20 dB, waarbij de ruis wordt gemeten via een RMS-detector.

Magnetische metingen zijn niet nodig, want de afstand tussen het elektronische stemapparaat en een af luisteraar is zodanig dat de magnetische veldsterkte ten opzichte van de elektromagnetische veldsterkte verwaarloosbaar is. Magnetische emanaties zijn uitsluitend effectief op korte afstand, d.w.z. op minder dan 5 m.

Aanhangsel B

MATLAB-code voor het berekenen van de drempelcurves

```
% Derivation of compromising-emanations e-field limit curves
```

```
% sample frequencies
```

```
curves = 1:2;
```

```
freqs = logspace(4, 10, 200);
```

```
[f, curve] = meshgrid(freqs, curves); % [Hz]
```

```
d0 = 1; % measurement distance [m]
```

```
logfreqs = log10(freqs);
```

```
curves = 1:5;
```

```
[f, curve] = meshgrid(freqs, curves); % [Hz]
```

```
bw = max(f/1e5, [ min(1e3, freqs/2) ; ...
```

```
    min(1e4, freqs/2) ; ...
```

```
    min(1e5, freqs/2) ; ...
```

```
    min(1e6, freqs/2) ; ...
```

```
    min(1e7, freqs/2) ]);
```

```
bwr = round125(bw, [1 2 5 10]);
```

```
% thermal noise at 290 K [dB $\mu$ V/m] ( $\lambda/2$  dipole)
```

```
thermalnoise = 20 * log10(f/1e6) + 10 * log10(bw) - 96.8;
```

```
% SNR loss of eavesdropper compared to measurement antenna
```

```
d = 5; % distance of eavesdropping antenna [m]
```

```
pathgain = 20*log10(fieldstrength(d,f)/fieldstrength(d0,f));
```

```
receivernoise = (log10(f)-7)*5; % ITT Radio Engineers Handbook
```

```
sensitivity = sensitivity_am524(f, bw) + 20; % 20 dB above best R&S antenna kit
```

```
figure(1);
```

```
semilogx(freqs, ...
```

```
    dbpwradd(itunoise(f, bw, 1) - pathgain ...
```

```
        - antennagain(f, bw, 1), ...
```

```
        receivernoise + sensitivity));
```

```
title('Fieldstrength');
```

```
ylim([-5 90]);
```

```
xlabel('Hz');
```

```
ylabel('dB $\mu$ V/m');
```

```
grid on;
```

```
saveas(gcf, 'limitcurves.png');
```

```
saveas(gcf, 'limitcurves.eps');
```

```
figure(2);
```

```
loglog(freqs, bwr);
```

```
title('Measurement bandwidths');
```

```
ylim([0.8e3 1.2e7]);
```



```

xlabel('Centre frequency [Hz]');
ylabel('Bandwidth [Hz]');
grid on;
saveas(gcf, 'limitcurvesbw.png');
saveas(gcf, 'limitcurvesbw.eps');

% add up decibel power levels
function s = dbpwradd(a,b)
s = 10*log10(sum(10.^(cat(3,a, b)./10),3));

% output normalized field-strength value (covering both far field
% and lower alternative near field) of frequency f [Hz] at distance
% r [m] from an emitting short dipole or small loop antenna
function e=fieldstrength(r,f)
lambda = 3e8 ./ f; % wavelength [m]
e = abs(1./(r.*lambda) .* (1 + 1./(j*(2*pi*r./lambda)) + 0./(j*(2*pi*r./lambda)).^2));

% Routine for estimating the gain of practical antennas or arrays
% with centre frequency f [Hz], bandwidth b [Hz], maximum dimension l [m]
function gain=antennagain(f,bw,l)

% auxiliary variables
rb = bw ./ f; % relative bandwidth [1]
lambda = 3e8 ./ f; % wavelength [m]

% collect achievable gains as a factor (i.e., not dB)
% (along gains along dimension 3, while dimension 1 and 2 are reserved
% frequency and bandwidth, respectively)

% Dipole antennas (lambda/2 or shorter):
% Directivity: 1.5
% Passive lambda/2 usable if aperture > 0.13*lambda^2 (otherwise active)
% Ref: Kraus/Marhefka: Antennas. 3rd ed., McGraw-Hill, 2002, p. 35.
% Rothammels Antennanbuch. 11th ed., Franckh-Kosmos, 1995, p. 422.
gains = (f > 0) .* 1.63;

% Single Yagi-Uda
% Ref: UCAM-CL-TR-577, p. 95
yagigain = 10.^(7.8 * log10(l./lambda) + 11.3)./10;
gains = cat(3, gains, yagigain);

% parabolic antennas
% ref: Rothammel, p. 728
gains = cat(3, gains, 0.5 .* (pi .* l./ lambda) .^ 2);

[g, t] = max(gains, [], 3);

%figure(4); semilogx(f(1,:), t); figure(1);

gain = 10 * log10(g);

```

```

% Terrestrial ITU-R P.372 minimum noise [dbμV/m] at frequency f, bandwidth b,
% and antenna gain g
% (Ref: Kuhn, UCAM-CL-TR-577, p. 92)
% We set Fa >= 0, as we assume that the background temperature
% will not drop below 290 K for terrestrial targets
function e=itunoise(f,b,g)
itu = interp1(log10([1e4, 7e4, 1.5e8, 10e9]), [148, 86, 0, 0], log10(f));
e = max(0, itu - 10 * log10(g)) + ...
    20 * log10(f/1e6) + 10 * log10(b/1e6) - 36.8;

% Fieldstrength sensitivity of R&S AM524 active antenna system in dBμV/m
% for bandwidth b [Hz] (Ref: AM524 data sheet)
function s = sensitivity_am524(f, b)
s = interp1(log10([1e2 1e3 1e4 1e5 1e6 3e6 1e7 3e7 1e8 2e8 6e8 1e9]), ...
    [ 0 -20 -34 -43 -48 -50 -50 -51 -54 -50 -40 -37], log10(f), 'spline');
bcfi = find(f > 3e7 & f < 2e8); % biconical antenna frequency index
s(bcfi) = interp1(log10([3e7 1e8 2e8]), [-50 -54 -50], log10(f(bcfi)), 'spline');
s(find(f > 1e9)) = -37; % extrapolated (horn)
s = s + 10*log10(b); % adjust for bandwidths other than 1 Hz

% round to the nearest s-series member (e.g., [1 2 5 10] or [1 3 10])
function y = round125(x, s)
e = floor(log10(x));
m = x ./ 10.^e;
y = 10.^(e+interp1(log10(s), log10(s), log10(m), 'nearest'));

```

Aanhangsel C

1. Kostenraming

a. Productiekosten

De productiekosten bedragen circa 38.000 euro exclusief belasting; dit omvat de behuizing, het TFT-scherm, de printer, bekabeling en standaard IT-apparatuur.

b. Meetkosten

Een accreditatiemeting kost 5000 euro; wanneer de constructie identiek is, vindt dit type meting slechts eenmaal plaats.

De compliance-meting kost 400 euro; dit bedrag behelst uitsluitend de meting, inclusief arbeidsloon en de registratie van de meetresultaten.

2. Geschatte tijdsduur van de metingen

De accreditatiemeting neemt circa tien dagen in beslag en omvat de voorbereiding, de meting zelf en de nodige documentatie.

De compliance-meting neemt – wat de voorbereiding en de meting zelf betreft – slechts circa 40 minuten in beslag; alle andere, niet-tijdkritieke werkzaamheden, zoals vervoer, verpakking, documentatie e.d. kunnen door anderen worden verricht.

Uitgaande van een 5-daagse werkweek en van de mogelijkheid in twee ploegen te werken en twee meetruimten te gebruiken, duurt het ongeveer 50 weken om 10.000 apparaten te meten.

Indien met drie ploegen wordt gewerkt, duurt dit ongeveer 33 weken.