RÖS

RÖJANDE SIGNALER

- Uppkomst
- Utbredning
- Skyddsmetoder
- Krav

FMV

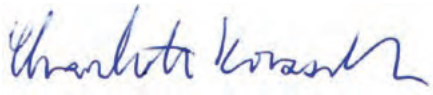
RÖS
Röjande signaler – uppkomst, utbredning, skyddsmetoder, krav

Förord

Svenska myndigheter och företag har de senaste åren kraftigt ökat sitt internationella engagemang. Detta har lett till att allt fler kommer i kontakt med sekretessbelagda uppgifter av betydelse för rikets säkerhet eller uppgifter som vi i avtal med andra länder förbundit oss att hantera på motsvarande sätt. I en del av de avtal som finns med EU och NATO förbinder vi oss även att uppfylla EU:s och NATO:s TEMPEST-krav. EU håller på att anpassa sitt regelverk så att det blir ekvivalent med NATO:s. Detta är bra för Sverige genom att vi inte behöver rätta oss efter tre regelverk.

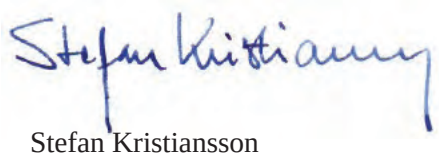
Denna broschyr, som har tagits fram av FMV:AK Led i samarbete med FM MUST, ger en kortfattad bild av hur RÖS uppstår och vilka möjligheter som finns att minska utbredningen av RÖS. Den beskriver den svenska RÖS-policyn som har till mål att minimera risken för informationsförluster genom RÖS.

Broschyren är även avsedd att ge bakgrundskunskap inför en diskussion om Sverige ska anpassa sitt regelverk till EU/NATO:s, för att slippa hantering av flera icke helt samstämmiga regelverk, eller fortsätta med krav på att uppfylla olika regelverk i de system som bearbetar eller lagrar Svensk respektive EU/NATO sekretessbelagd information.



Charlotte Korssell

Chef för FMV:s Anskaffningskontor Ledningssystem



Stefan Kristiansson

Chef för Militära Underrättelse- och Säkerhetstjänsten

Förrådsbeteckning:	M7773-001851
Förrådsbenämning:	BROSCHYR RÖS
Utgivningsår:	2009
Fastställelse:	FMV:AK Led 10 755:818/2009
Distribution:	Försvarets bok- och blankettförråd
Tryck:	Lenanders Grafiska 33326, 2009

Innehåll

1 Inledning

I vårt moderna informationssamhälle förbises ofta de hot och risker som finns i samband med nyttjandet av datorer. Inom Försvarsmakten och dess samverkande myndigheter är det viktigt att upprätthålla en hög och ensad standard då sekretessbelagd information behandlas.

Man talar om informationsteknologisk säkerhet, *IT-säkerhet*, som innefattar flera viktiga komponenter, till exempel spårbarhet, riktighet och oavvislighet, men begreppet innefattar även mekanismer mot förlust av data och mekanismer för att skydda data det vill säga *signalskydd*.

Traditionellt har kryptoapparater använts som *signalskyddssystem* för att skydda såväl text som trafik. Då dessa kryptoapparater blev elektroniska, infördes tidigt ett krav på att dataläckage inte får förekomma. Inom signalskyddsområdet infördes begreppet *röjande signaler (RÖS)* och mätmetoder togs fram för i första hand kryptoapparater. Utvecklingen har gått mot att de flesta kryptoapparater idag innehåller någon form av dator och att datoriserade kryptoapparater ingår i *IT-system* med sammankopplade datorer.

Användningen av IT-system för att stödja olika verksamheter är nu helt förhärskande och i vissa av dessa IT-system finns behov av att skydda sig mot röjande signaler. Skydd mot RÖS är således en av många åtgärder för att förbättra IT-säkerheten.

Behovet av RÖS-skydd uppfylls genom att installera utrustning i RÖS-skyddade rum och containrar eller genom att utrustningen, främst signalskyddsmateriel och PC-relaterad materiel, konstrueras så att den blir RÖS-skyddad. Under 2008 fastställdes en mätmetod för RÖS-skyddade kabinett, i första hand avsedda som RÖS-skydd av PC-relaterad materiel.

Inom det svenska försvaret är det FMV som ansvarar för RÖS-områdets teknikutveckling. I detta ingår att ta fram nya gränsvärden, mätmetoder och skyddsfilosofier vartefter tekniken förändras. Verksamheten leds av Försvarsmakten HKV/MUST.

Det övergripande syftet med denna broschyr är att ensa begreppen inom teknikområdet RÖS. I broschyren ges en populärvetenskaplig beskrivning av fenomenet RÖS och en vägledning vid överväganden om hur RÖS skall betraktas för att uppnå bästa skydd i olika situationer. Vidare behandlas försvarsmaktens krav på skydd mot röjande signaler, kopplade mot IT-system och signalskyddssystem. Broschyren avslutas med en kortfattad orientering om nya EU-regler för TEMPEST[1].

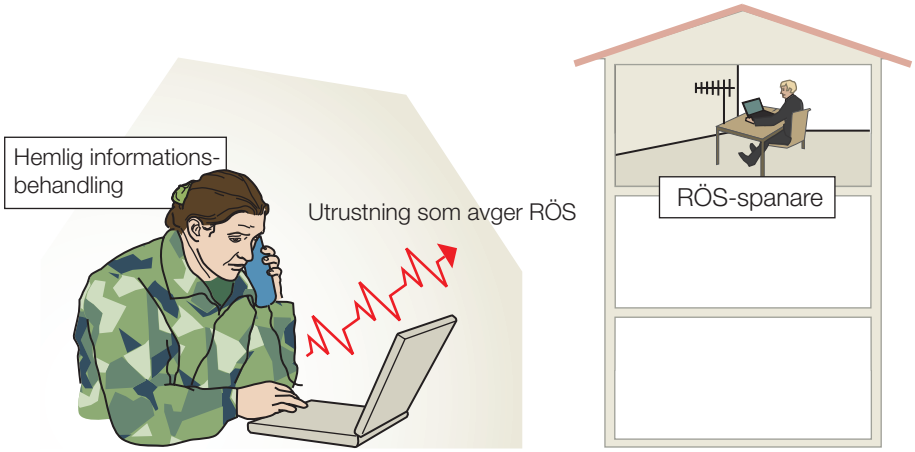
I broschyren finns två fördjupningsavsnitt vars innehåll inte är avgörande för förståelsen av den fortsatta texten. Om så önskas, kan dessa avsnitt lämnas därhän.

---

1 TEMPEST är ett samlingsbegrepp för standarder, analyser, mätningar etc som rör röjande signaler, på engelska ”compromising emanation”.
Ordet TEMPEST myntades i slutet av 60-talet och början av 70-talet som ett kodord för den klassificerade verksamhet som National Security Agency i USA bedrev för att dels säkra egna kommunikationssystem mot otillåten avlyssning, dels samla in och tolka signaler från främmande kommunikationssystem.
I USA har man på myndighetsnivå fastställt att ordet TEMPEST inte är en akronym och ordet saknar således innebörd.

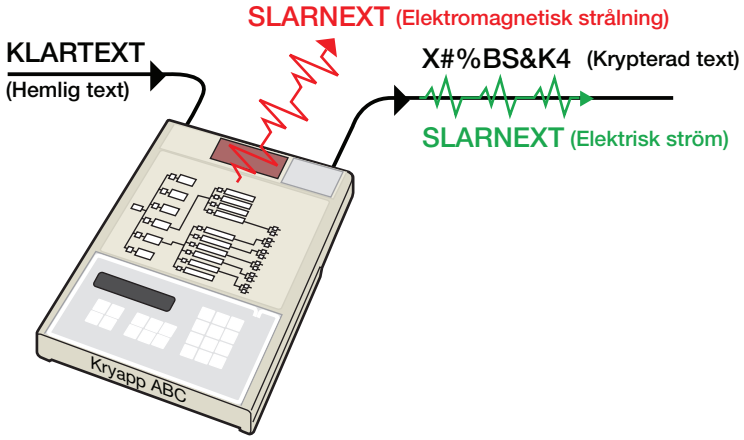
2 Röjande signaler

Röjande signaler (RÖS) är orsaken till en säkerhetsrisk som uppstår genom att oavsiktligt genererade radiosignaler (radiostörningar) kan vara bärare av den information som behandlas eller överförs i informationsteknologisk utrustning, se figur 1.



Figur 1: Röjande signaler - RÖS

En kryptoapparat enligt figur 2 kan tjäna som exempel. Det skydd som kryptering ger kan avslöjas genom att fragment av den hemliga texten läcker ut till obehöriga i form av elektromagnetisk strålning eller elektrisk ström på anslutna ledningar för strömförsörjning och telekommunikation (el- och teleledningar).



Figur 2: RÖS kan avslöja hemlig information

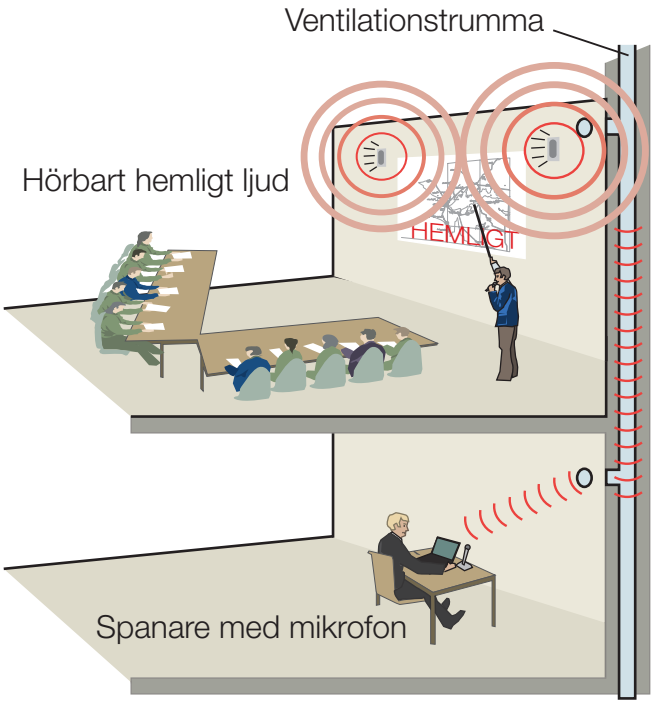
> *Med röjande signaler (RÖS) förstås: Oavsiktligt genererade elektromagnetiska signaler som, om de kan tydas av obehöriga, kan bidra till att sekretessbelagd information röjs.*

Observera att:

- En RÖS-skyddad utrustning ger inte en garanterad låg emissionsnivå. Detta innebär att icke informationsbärande störningar från en RÖS-skyddad utrustning kan ha höga nivåer och kan därmed störa radiokommunikation.
- Elektronisk avlyssning av apparater som otillåtet manipulerats, definieras inte som RÖS. Följande två avlyssningsexempel ska således *inte* hänföras till området röjande signaler:
  - ”Skimning” (smygkopiering) av TAK-kort (”smartcard”) i anslutning till RÖS-plomberad kortläsare.
  - ”Key-logger” ansluten på tangentbordskabeln utanför RÖS-skyddad systemenhet.

Förutom RÖS i form av elektromagnetiska signaler har tidigare *akustiskt RÖS*, det vill säga RÖS i form av ljudvågor som breder ut sig från mekanisk eller elektromekanisk utrustning, behandlats såsom ett hot. Ofta förknippades akustiskt RÖS med så kallad matris-RÖS från matrisskrivare. Elektronisk utrustning som idag används för behandling av hemlig information, avger inga informationsbärande akustiska signaler och akustisk RÖS är därför inte längre något hot. Akustiska enheter kan däremot ge upphov till betydande elektromagnetisk RÖS i det akustiska frekvensområdet.

Till skillnad mot akustisk RÖS är hemlig rumsavlyssning, *buggning*, ett hot. Med buggning avses avlyssning av tal, närmare bestämt att tal i enrum, samtal mellan andra eller förhandlingar vid sammanträde eller annan sammankomst som allmänheten inte har tillträde till, i hemlighet avlyssnas eller tas upp genom ett tekniskt hjälpmedel för återgivning av ljud, se figur 3. Observera att buggning inte definieras som RÖS.

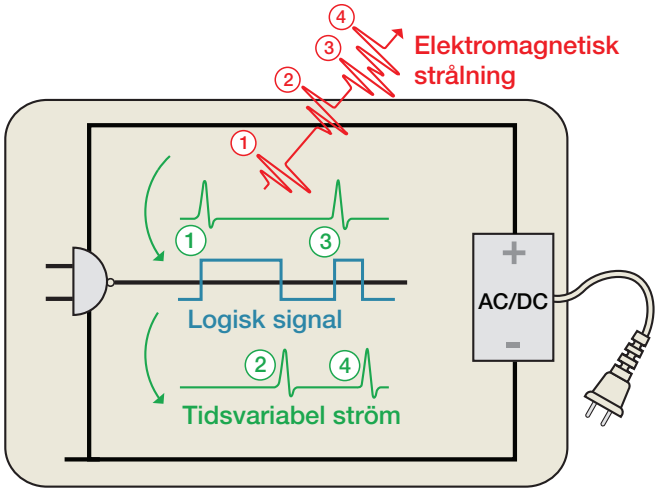


Figur 3: Buggning

Inom Försvarsmakten hanteras hörbart hemligt ljud som kan utsättas för buggning, även med andra åtgärder än tekniska skydd.

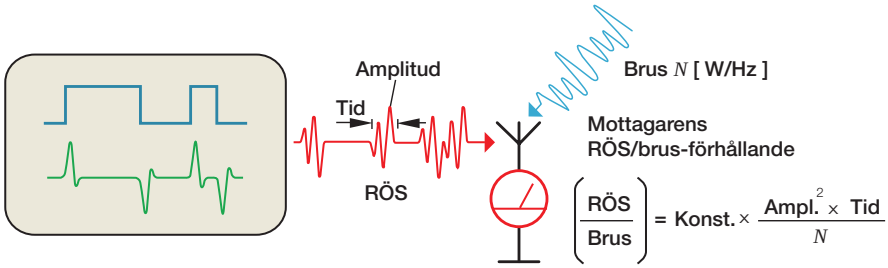
Förekomsten av RÖS beror på att alla signalförändringar orsakar tidsvariabla strömmar. För en datasignal kan detta illustreras med ett kretsexempel enligt figur 4. Här är det logiska signalförändringar, från noll till ett eller omvänt, på NAND-kretsens utgång som orsakar tidsvariabla strömmar från AC/DC-omvandlaren. Dessa tidsvariabla strömmar utgörs av accelererade och retarderade elektriska laddningar. Från fysiken vet man att acceleration eller retardation av elektriska laddningar orsakar elektromagnetisk strålning, vars styrka beror på den specifika konstruktionen. Den elektromagnetiska strålningen får ett tidsförlopp som är korrelerat till signalförändringarna i den logiska signalen, se numreringar i figur 4, och strålningen är därmed att betrakta som RÖS.

Det bör betonas att samma resonemang gäller för signalförändringarna i en analog signal.



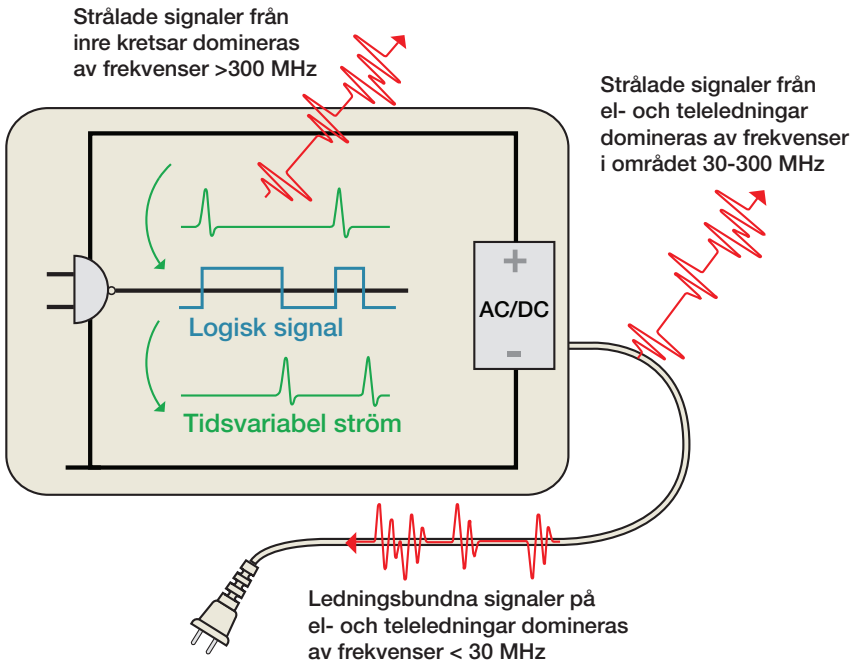
Figur 4: Dynamiska strömmar ger upphov till RÖS

En signal som lämnar en utrustning i form av strålning är oftast en förvrängd (distorderad) version av den ursprungliga signalen i apparaten. En förutsättning för att faktiskt lyckas med avlyssning av en sådan oavsiktligt genererade signal är därför att informationsinnehållet i den distorderade signalen är så stor att den ursprungliga signalen går att rekonstruera. Vidare måste bakgrundsbruset vid mottagaren ge ett signal/brusförhållande som tillåter en korrekt detektering, se figur 5.



Figur 5: Signal (RÖS)/brus-förhållandet för avlyssnaren

Signalens amplitud och distorsion vid avlyssnarens mottagare bestäms också av de ledare i apparaten som fungerar som antenner. För att en ledare skall fungera som effektiv antenn måste den ha en längd av cirka en halv våglängd. I intervallet 30-300 MHz varierar längden av en halvvågsantenn från 5 till 0,5 meter och det yttre kablaget kan då utgöra en bra antenn. Vid högre frekvenser strålar signalen direkt från inre kretsar i apparaten. För lägre frekvenser kan el- och teleledningar fungera som transmissionsledningar och överföra RÖS-signaler ledningsbundet, se figur 6.



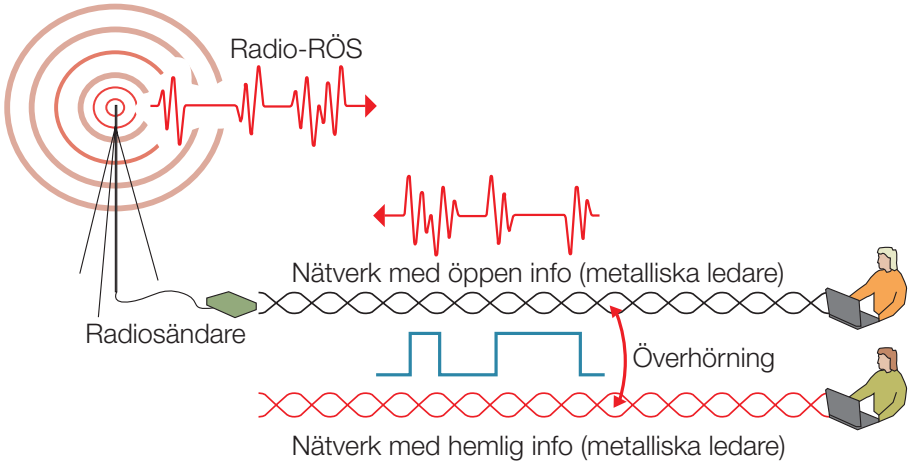
Figur 6: Dominerande frekvensområden för strålat och ledningsbundet RÖS

3 RÖS-källor och RÖS-signaler

Man skiljer mellan två principiellt olika slags RÖS-källor, informationskälla respektive fysisk källa. Informationskälla är den hemliga information som behandlas eller överförs i eller mellan apparater, fysisk källa är elektriska kretselement som genererar strålningen eller strömmen. Med uttrycket ”RÖS-signal” avses en fysisk representation av informationen från en informationskälla, till exempel elektromagnetisk strålning eller elektrisk ström.

RÖS-signalerna ges i bland namn efter den typ av information som överförs mellan apparater eller mellan olika funktionsenheter inom en apparat. Man talar exempelvis om *tecken-RÖS* som kan vara RÖS från information som överförs från tangentbord till dator med metalliska ledare. Ett annat exempel är *video-RÖS* som är RÖS från information som genereras i grafikkort och överförs från dator till bildskärm med metalliska ledare enligt den gamla VGA-standarden. Vid användning av videostandarden DVI i RÖS-skyddad utrustning kan optofiber användas för överföring av information från dator till bildskärm vilket sannolikt minskar förekomsten av video-RÖS.

RÖS via radio, vanligen benämnd radio-RÖS är en speciellt förrädisk form av RÖS som kan förekomma i utrustningar innehållande någon typ av radiosändare, till exempel krypterad radio eller krypterad mobiltelefon. Det förrädiska ligger i att de röjande signalerna blir överlagrade på en bärvåg och kan via sändarantennen spridas över mycket stora avstånd. Radio-RÖS kan uppstå genom elektromagnetisk överhörning, det vill säga oavsiktlig elektromagnetisk koppling mellan kretsar och ledare i anläggningar som innehåller radiosändare. Figur 7 visar ett exempel på hur överhörning i nätverk av metalliska ledare kan orsaka radio-RÖS. Med fiberoptiska nätverk skulle överhörningen elimineras.



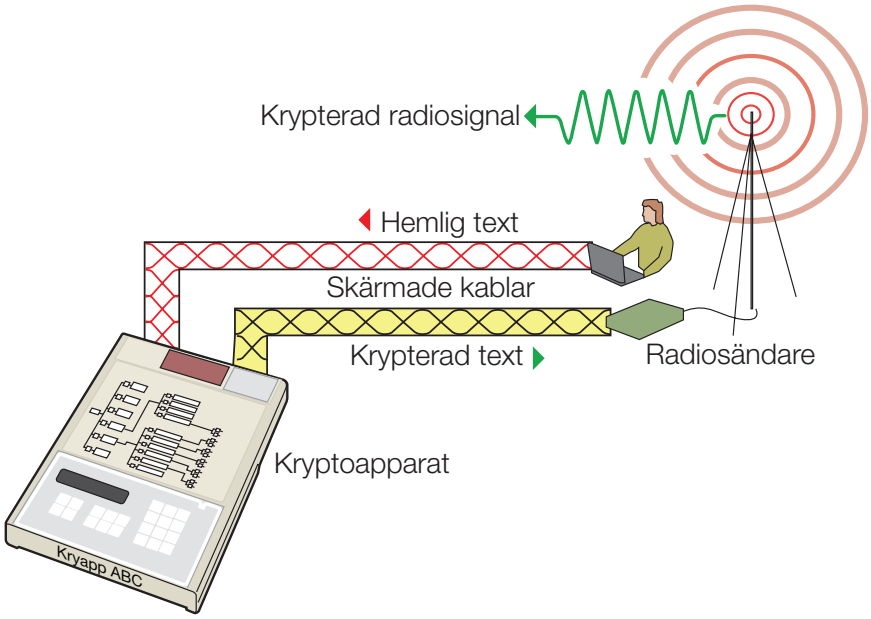
Figur 7: Elektromagnetisk överhörning mellan metalliska ledare kan ge upphov till radio-RÖS

3.1 Överhörning

Inom signalskyddsområdet skiljer man på elektromagnetisk överhörning och akustisk överhörning.

Elektromagnetisk överhörning, EM-överhörning, innebär att signaler i en elektrisk krets överförs i mer eller mindre distorderad form till en annan elektrisk krets genom någon form av elektromagnetisk koppling. Kopplingen mellan kretsarna kan vara konduktiv, induktiv eller kapacitiv. Är signalerna informationsbärande kan ett RÖS-problem uppstå, således är EM-överhörning den främsta orsaken till radio-RÖS.

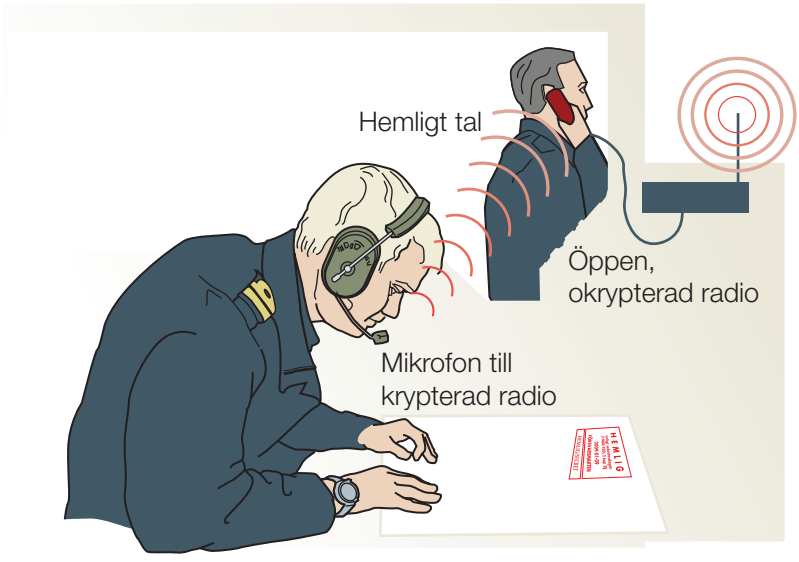
I anslutning till ovanstående figur 7 påpekades att EM-överhörning kan elimineras genom användandet av fiberoptiska nätverk. En alternativ metod är att använda skärmade kablar som, om de dimensioneras och ansluts på ett fackmannamässigt sätt, kan förhindra EM-överhörning, se exempel i figur 8.



Figur 8: Skärmade kablar kan förhindra elektromagnetisk överhörning

Det är således viktigt att utrustning installeras på ett sätt som förhindrar EM-överhörning från informationssystem med hemlig text till system med öppen eller krypterad information som utnyttjar förbindelser via radiosändare. En systemundersökning med avseende på radio-RÖS bör alltid göras och efter bedömning eventuellt verifieras med mätningar.

Akustisk överhörning innebär att akustiska signaler (ljudsignaler) avsedda för ett system oavsiktligt ”läcker över” till ett annat system. Ett exempel är då två radiosystem, ett oskyddat och ett signalskyddat, samtidigt används på en plattform, exempelvis i en ledningscontainer, i ledningscentralen på ett fartyg eller i cockpiten i ett flygplan. Talet till det signalskyddade systemets mikrofon kan då oavsiktligt koppla in i det oskyddade systemets mikrofon varvid hemlig information i klartext sänds ut via det oskyddade systemets radioantenn, se figur 9.



Figur 9: Akustisk överhörning

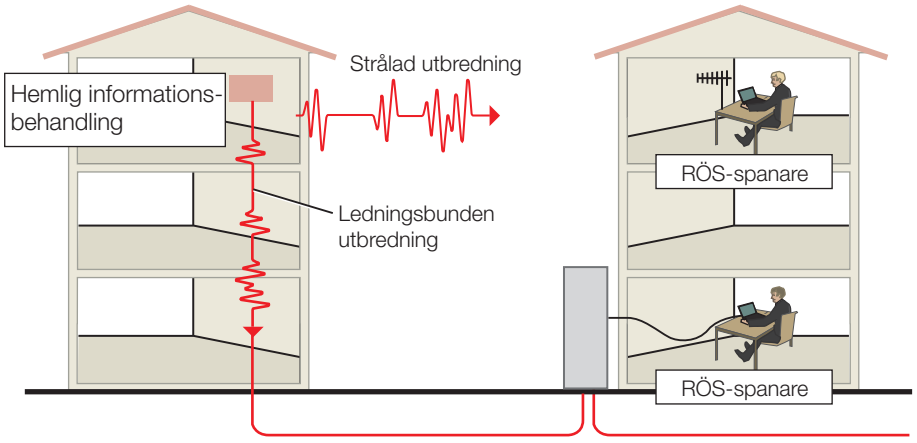
Observera att i exemplet i figur 9 är det inte fråga om radio-RÖS utan om akustisk överhörning av hemlig information som förstärks och sänds ut som radiosignaler. För att förhindra akustisk överhörning kan man använda metoder som akustisk avskärmning, teknisk ”nyckling” som förhindrar samtidig användning av öppna och signalskyddade kommunikationssystem eller att endast tillåta signalskyddade system.

4 Utbredningsvägar

RÖS breder ut sig som ledningsbunden och strålad vågutbredning, se figur 10.

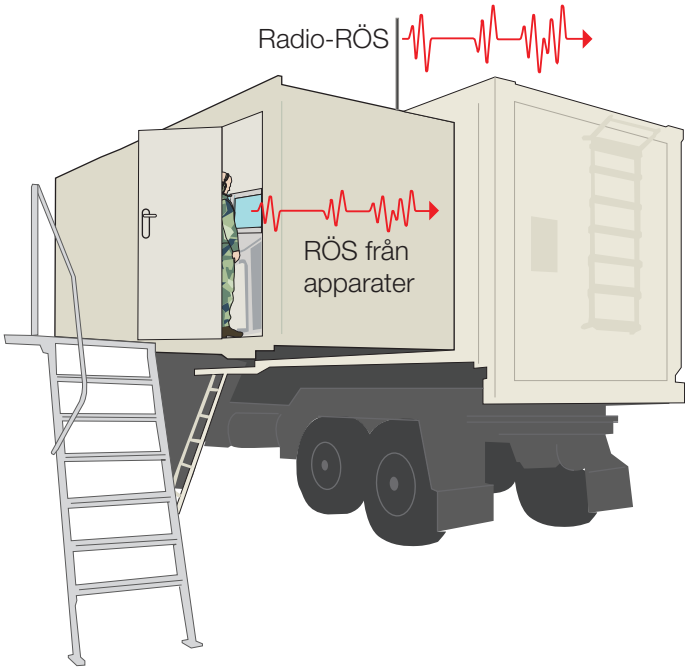
Ledningsbunden utbredning sker främst utefter kraft- och teleledningar men också utefter andra metalliska ledare såsom vattenledningsrör och armeringsjärn. Den ledningsbundna utbredningen är i huvudsak begränsad till frekvenser under 30 MHz, detta beroende på att förlusterna i ledningsnäten ökar med frekvensen.

Strålad utbredning sker från apparater som innehåller RÖS-källor och är i huvudsak begränsad till frekvenser över 30 MHz där ledningar med typiska längder i och utanför apparaten kan fungera som sändarantenner. För lägre frekvenser minskar antenneffektiviteten.



Figur 10: Ledningsbunden och strålad utbredning av RÖS

Förutom att strålad utbredning kan ske direkt från apparater som innehåller RÖS-källor, kan strålad utbredning ske i form av radio-RÖS, se föregående kapitel 3, ”RÖS-källor och RÖS-signaler”. Detta åskådliggörs i figur 11 där en mobil ledningscentral antas innehålla både apparater som avger RÖS och informationssystem som genom elektromagnetisk överhörning ger radio-RÖS.



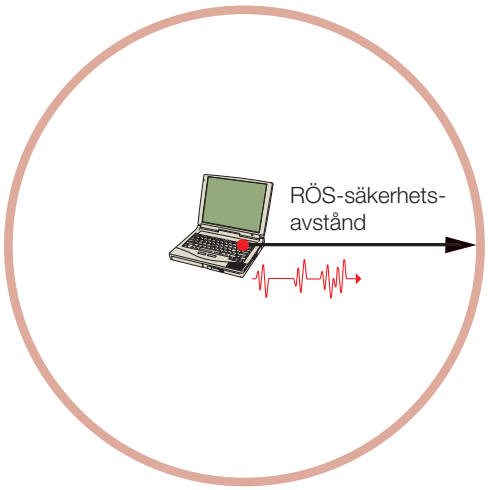
Figur 11: Strålad utbredning av RÖS från utrustningen i en mobil ledningscentral

5 RÖS-säkerhetsavstånd

RÖS-säkerhetsavstånd definieras som ett avstånd inom vilket risk finns för att röjande signaler kan registreras. Om inte annat specificeras, är RÖS-säkerhetsavståndet för en apparat det största av de säkerhetsavstånd som gäller för ledningsbundna respektive strålade röjande signaler.

Säkerhetsavståndet för ledningsbundet RÖS bestäms genom mätningar på en apparats alla ledningar och med användning av en speciell, klassificerad beräkningsalgoritm.

Det säkerhetsavstånd för strålat RÖS som bestäms vid en RÖS-undersökning av en apparat, avser fri rymd under ideala omständigheter. Observera att säkerhetsavståndet endast gäller RÖS från apparater, inte radio-RÖS som kan spridas över mycket stora områden.



Figur 12: Säkerhetsavståndet för strålat RÖS beräknas för fri rymd

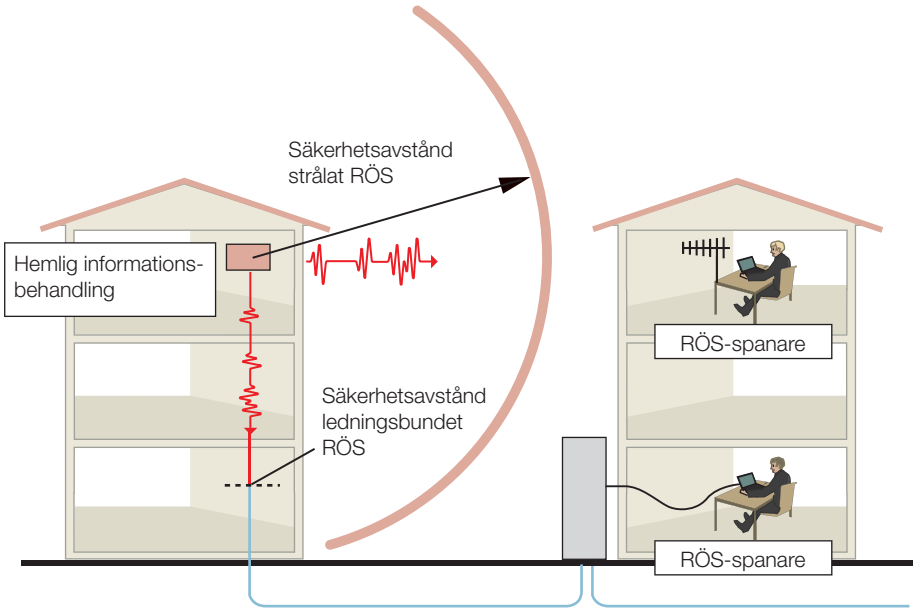
Anledningen till att definiera säkerhetsavståndet för strålat RÖS vid fri rymd är att säkerställa ett generellt skydd oberoende av var apparaten placeras. Ofta reducerar omgivningen de strålade röjande signalerna och ger då RÖS-säkerhetsavståndet för en apparat en extra säkerhetsmarginal, mer om detta i fördjupningsavsnittet ”Kvantifiering av naturliga skydd”, sidan 16.

6 Skyddsmetoder

RÖS-skydd kan erhållas på några principiellt olika sätt; RÖS-säkerhetsavstånd, RÖS-skyddade utrustningar, RÖS-skyddade rum och kabinett samt genom att utnyttja naturliga skydd i omgivningen.

6.1 Skydd genom RÖS-säkerhetsavstånd

Intensiteten hos radiofrekventa signaler avtar med avståndet från källan, vilket medför att både ledningsbundna och strålade signaler har begränsad räckvidd. Det är därför möjligt att skapa ett RÖS-skydd genom att kontrollera att ingen avlyssningsutrustning finns inom en sfär med en radie som är lika med utrustningens RÖS-säkerhetsavstånd, se figur 13.



Figur 13: Skydd genom RÖS-säkerhetsavstånd

6.2 RÖS-skyddade utrustningar

Utrustningar kan konstrueras så att emission av RÖS i princip elimineras, utrustningsklass 1 (U1), eller begränsas, utrustningsklass 2 (U2). Utrustningar som uppfyller kraven för U1 har ett mycket litet RÖS-säkerhetsavstånd medan U2-utrustningar har ett RÖS-säkerhetsavstånd som är större än för U1 men ändå begränsat. Utrustningar som inte kan kategoriseras i någon av klasserna U1 eller U2, men har ett uppmätt RÖS-säkerhetsavstånd större än för U2, klassas som utrustningsklass 3 (U3). Övrig utrustning har okänt säkerhetsavstånd.

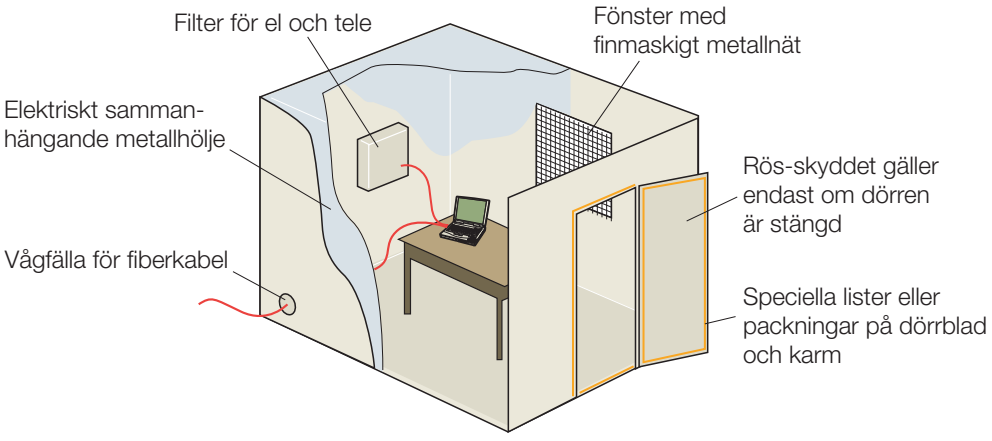
Att modifiera utrustning av typen COTS (Commercial Off The Shelf) i syfte att uppnå RÖS-skydd är förenat med höga kostnader och kräver specialistkompetens.

6.3 RÖS-skyddade rum och kabinett

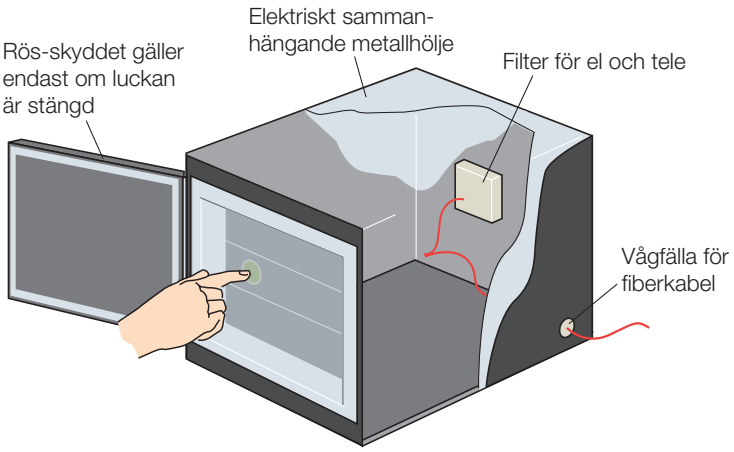
Apparater som inte har ett eget RÖS-skydd kan placeras i RÖS-skyddade rum eller RÖS-skyddade kabinett, se figurerna 14 och 15. RÖS-skyddet uppnås genom att det skyddade utrymmet utformas som en ”Faradays bur”, det vill säga utrymmet omges av en skärm i form av ett elektriskt sammanhängande metallhölje. För att förhindra att ledningsbundna röjande signaler kommer ut, måste alla el- och teleledningar med metalliska ledare förses med speciella filter.

Datakommunikation kan överföras genom att fiberoptiska kablar, utan metalliska mantlar, förs in i utrymmet genom särskilda öppningar i den metalliska skärmen. Öppningarna ska vara försedda med vågfällor dimensionerade för att uppfylla rummets eller kabinettets krav på dämpning. En vågfälla har formen av en metallisk stos kring en öppning och är i princip en vågledare med sådana mått i förhållande till våglängden att den i stället för att leda, dämpar strålade signaler.

I jämförelse med en tom vågfälla, kommer fiberoptiska kablar genom en vågfälla att medföra lägre dämpning för strålade signaler med frekvenser i GHz-området. Detta beror på att materialet i fiberkablarna har andra elektriska egenskaper än den luft som finns i en tom vågfälla.



Figur 14: RÖS-skyddat rum



Figur 15: RÖS-skyddat kabinett

RÖS-egenskaperna hos RÖS-skyddade rum och kabinett kvantifieras av en storhet som benämns skärmningseffektivitet. Skärmningseffektiviteten är ett mått på rummets eller kabinettets förmåga att reducera signalstyrkan från RÖS-källor i utrymmet.

RÖS-skyddade rum kan konstrueras så att emission av RÖS i princip elimineras, skalskyddsklass 1 (SS1), eller begränsas, skalskyddsklass 2 (SS2).

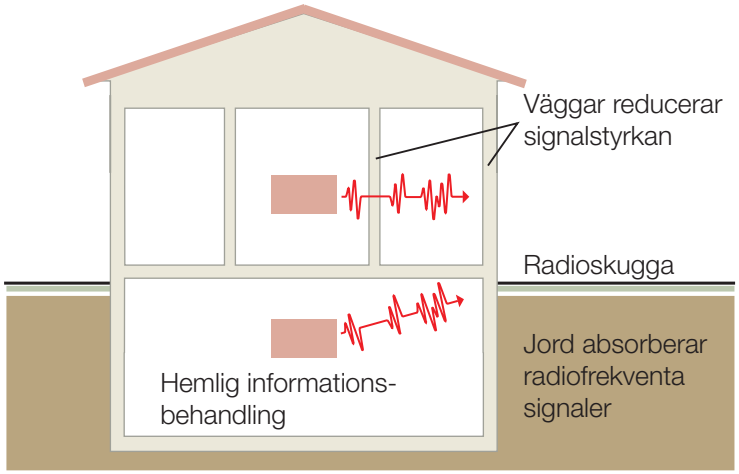
Vid upphandling av RÖS-skyddade rum är det viktigt att skyddet verifieras efter installation. Detta gäller också containrar som är kravsatta att utgöra RÖS-skyddade rum. Krav och verifieringsmetoder ges i referens [1]. Kontinuerliga kontroller bör också utföras för att säkerställa att inte RÖS-skyddet förändrats.

RÖS-skyddade kabinett ska konstrueras så att emission av RÖS i princip elimineras, skalskyddsklass 1 (SS1). Krav och verifieringsmetoder ges i referens [2] där också gränsdragningen mellan rum och kabinett finns definierad.

6.4 Allmänna åtgärder som försvårar avlyssning

Vid behandling av hemlig information i oskyddad utrustning kan möjligheten till avlyssning reduceras avsevärt genom att vidta några enkla försiktighetsåtgärder. Placera utrustningen i det inre av byggnaden och, för utrymmen ovan jord, så nära marknivå som möjligt. Omgivande väggar och närhet till mark reducerar räckvidden för strålat RÖS.

Bästa skyddet fås genom att placera utrustningen under marknivå. Jord- och byggnadsmaterial absorberar och sprider radiofrekventa signaler så att signalstyrkan reduceras kraftigt utanför byggnaden. Näst bäst är att placera utrustningen långt in i byggnaden, varje betongvägg mellan apparaten och avlyssnaren dämpar strålande signaler. Placera aldrig utrustningen direkt framför ett fönster som har fri sikt mot en tänkbar avlyssnare.

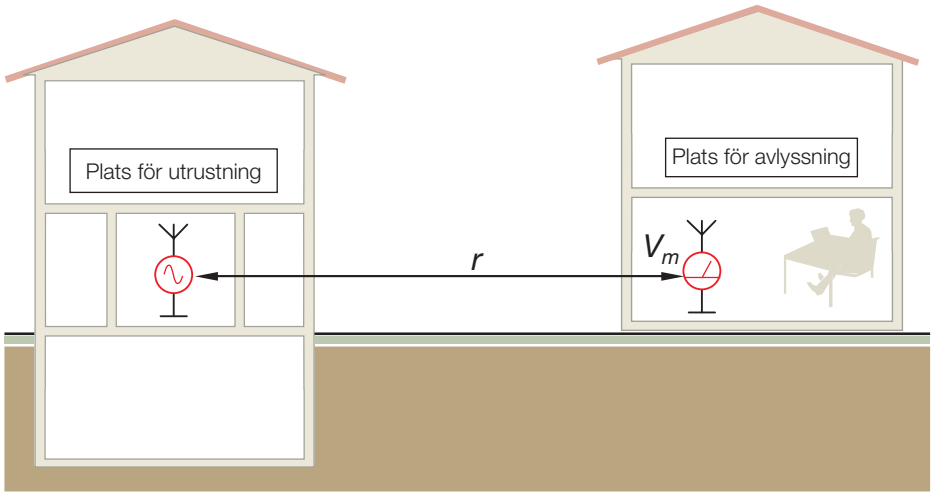


Figur 16: Rätt placering kan reducera strålat RÖS

Fördjupningsavsnitt: Kvantifiering av naturliga skydd

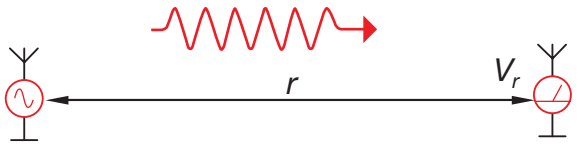
Det skydd mot strålat RÖS som man kan uppnå genom att placera utrustningen under mark (bergrum) eller långt in i en väl armerad byggnad, kan kvantifieras genom mätningar av en storhet som benämns utbredningsfaktor. Utbredningsfaktorn som här betecknas F_U, är ett mått på hur mycket den omgivande miljön reducerar signalstyrkan från en given radiokälla i förhållande till den signalstyrka som fås från källan på samma avstånd i fri rymd.

Källan placeras först på den plats där utrustningen (med känt säkerhetsavstånd R_s för strålat RÖS) kommer att vara placerad. Med mottagaren placerad på de platser där avlyssning kan tänkas ske, mäts nu signalstyrkan, här betecknad V_m, se figur 17.



Figur 17: Mätning av signalstyrkan vid platsen för tänkbar avlyssning

Med samma avstånd r mellan radiokälla och mätmottagare som vid mätningen enligt figur 17, genomförs sedan en frifältsmätning av signalstyrkan, här betecknad V_r, se figur 18.



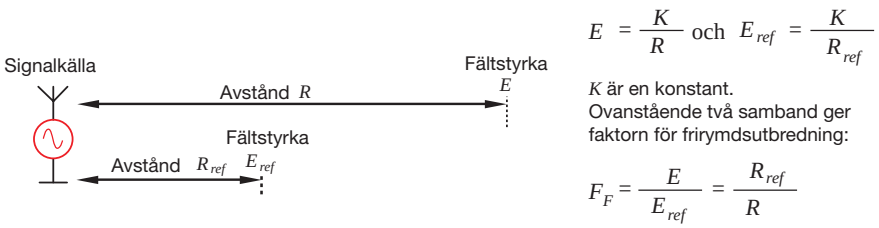
Figur 18: Mätning av signalstyrkan i fri rymd

Utbredningsfaktorn F_U beräknas från de uppmätta signalstyrkorna som kvoten mellan V_m i figur 17 och V_r i figur 18, $F_U = V_m / V_r$. Den uppmätta utbredningsfaktorn är ett mått på hur omgivningen reducerar fältet i RÖS frekvensområde och kommer således att reducera säkerhetsavståndet R_s för strålat RÖS. Med antagandet att RÖS-fältet hade ett avtagande som var omvänt proportionellt mot avståndet från källan då R_s bestämdes, kommer nu utbredningsfaktorn F_U att reducera utrustningens säkerhetsavstånd R_s för strålat RÖS till avståndet $F_U \cdot R_s$.

Anm. I den klassificerade handlingen "Beräkning av säkerhetsavstånd och korrektion för bärvågs-RÖS", ELEKTRO H10755:1165/98, visas att fler parametrar kan påverka det reducerade RÖS-säkerhetsavståndet. Sambandet $F_U \cdot R_s$ bör därför endast användas för överslagsberäkningar.

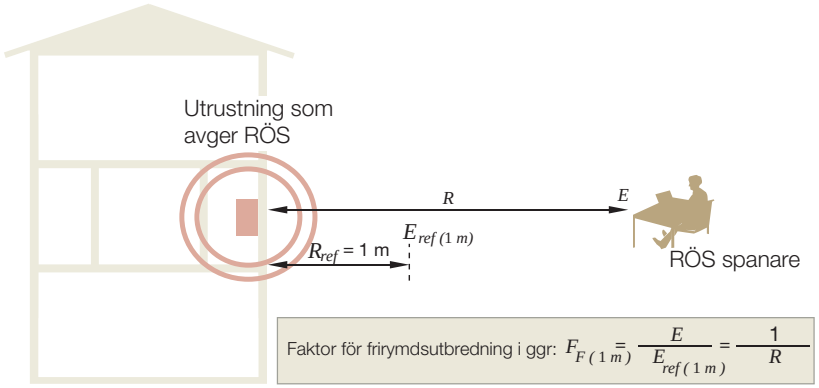
I en byggnad av armerad betong ger ytterväggarna ett bidrag till utbredningsfaktorn som i frekvensområdet för strålat RÖS brukar anta värden från 1/3 ner till 1/10. Detta betyder att byggnaden reducerar (dämpar) signalernas fältstyrka med en faktor 3 till 10 gånger (det vill säga med ca 10 dB till 20 dB). Om en apparat har säkerhetsavståndet 60 m för strålat RÖS, reducerar byggnaden detta säkerhetsavstånd till ca 20 respektive 6 m. Detta gäller under förutsättning att apparaten är placerad bakom en homogen betongvägg, det gäller inte då apparaten står placerad omedelbart innanför ett fönster.

För att få ett mått på hur mycket signalstyrkan från den strålande källan reduceras av såväl byggnad (och andra eventuella hinder) som avståndet till en plats för avlyssning, måste utbredningsfaktorn multipliceras med en faktor för frirymdsutbredningen. Denna faktor F_F anger hur signalens fältstyrka i fri rymd avtar med avståndet från källan. För fjärrfältsområdet är fältstyrkan omvänt proportionell mot avståndet från källan vilket ger sambanden i figur 19.



Figur 19: Fältstyrkeförhållanden i fjärrfältsområdet

Jämför nu signalkällan i figur 19 med en utrustning som avger RÖS och är placerad i en byggnad enligt figur 17 men där byggnaden och dess omgivning nu ska betraktas som helt elektromagnetiskt transparent eftersom en faktor för frirymdsutbredningen ska beräknas. För att inte behöva ta hänsyn till utrustningens placering inuti byggnaden, antas att utrustningen är placerad alldeles intill byggnadens yttervägg, vilket kan betraktas som ett värsta fall. Det avstånd R_{ref} från vilket frirymdsutbredningen för de röjande signalerna ska börja beaktas, sätts definitionsmässigt till 1 m från byggnaden. På detta avstånd antas fjärrfältsförhållanden råda för merparten av de röjande signalernas frekvenskomponenter. (I närfältsområdet avtar fältet snabbare än omvänt proportionellt mot avståndet vilket kan ses som en säkerhetsmarginal om fjärrfältsförhållanden inte uppnåtts vid 1 m.) $E_{ref\ (1\ m)}$ är således RÖS-fältets fältstyrka i fri rymd på avståndet R_{ref} = 1 m från byggnaden vilket, om byggnadsväggens tjocklek försummas, också är 1 m från utrustningen som avger RÖS, se figur 20.

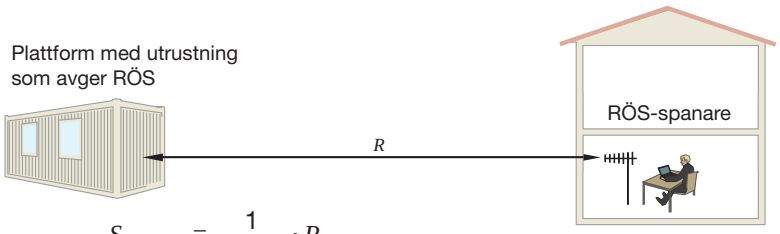


Figur 20: Approximativt uttryck för faktorn för frirymdsutbredningen då hänsyn till frifältsdämpningen börjar beaktas 1 m utanför byggnadsväggen.

Under givna förutsättningar blir faktorn för frirymdsutbredningen $F_{F\ (1\ m)} = 1/R$ vilket betyder att signalerna från den utrustning som avger RÖS dämpas $1/ F_{F\ (1\ m)} = R$ ggr eller $20 \cdot \log R$ dB enbart på grund av avståndet mellan utrustningen och RÖS-spanaren.

Den tidigare uppmätta utbredningsfaktorn F_U innebär en dämpning av signalerna med $1/F_U$ ggr eller $20 \cdot \log(1/F_U)$ dB, varför den totala RÖS-dämpningen blir $(1/F_U) \cdot R$ ggr eller $[20 \cdot \log(1/F_U) + 20 \cdot \log R]$ dB. Denna RÖS-dämpning är ett mått på den ekvivalenta skärmningseffektiviteten S_{ekv} som alltså kan innefatta både mellanliggande materia (till exempel väggar) och avstånd.

I figur 21 sammanfattas den här definierade ekvivalenta skärmningseffektiviteten (RÖS-dämpningen) mellan en plattform (byggnad, container, fordon, fartyg etc) med utrustning som avger RÖS och en RÖS-spanare.



$$S_{ekv\,(ggr)} = \frac{1}{F_U} \cdot R$$

$$S_{ekv\,(dB)} = 20 \cdot \log \frac{1}{F_U} + 20 \cdot \log R$$

där: S_{ekv} = *ekvivalent skärmningseffektivitet, RÖS-dämpning*

F_U = *uppmätt utbredningsfaktor*

R = *avstånd mellan plattform och RÖS-spanare*

Figur 21: Ekvivalent skärmningseffektivitet, RÖS-dämpning

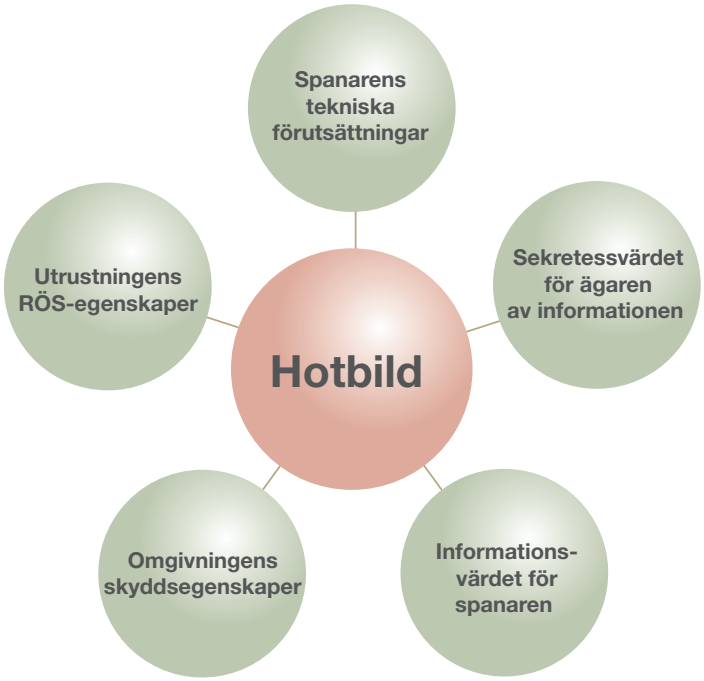
Exempel: Antag att CE-märkta civila produkter används i en välskärmad container och att en RÖS-spanare kan verka på ett avstånd 30 m utanför containern. Utbredningsfaktorn har i frekvensområdet för strålat RÖS mätts upp till ≤ 0,01 ggr, det vill säga containern och omgivande hinder (träd m m) dämpar signalen mer än 40 dB. Avståndet 30 m ger en faktor för frirymdsutbredning på 1/30 vilket innebär en dämpning på ca 30 dB. Sammanlagt kommer således signalerna från utrustningen som avger RÖS att ha dämpats med minst 70 dB på ett avstånd 30 m utanför containern, detta jämfört med odämpade signaler uppmätta 1 m från utrustningen. Den ekvivalenta skärmningseffektiviteten är minst 70 dB i frekvensområdet för strålat RÖS.

---

7 Hotbildens komponenter

Kännetecknande för RÖS-hotet är att en RÖS-spanare kan komma i besittning av hemlig information utan den avlyssnades vetskap. Detta är en konsekvens av att RÖS-spaning sker helt passivt, utan påverkan av den utrustning som avlyssnas.

Med hotbild avses en total bedömning av hotet från en tänkbar RÖS-spanare. I denna bedömning ska sekretessvärdet av informationen vägas mot såväl möjligheten för en RÖS-spanare att tekniskt genomföra en framgångsrik RÖS-spaning som informationsvärdet för spanaren, se figur 22.



Figur 22: Hotbildens komponenter

Mobila system är definitionsmässigt rörliga vilket gör det svårt för en spanare att sätta upp en avlyssningsutrustning, både med avseende på den ställtid som spanaren behöver och möjligheten att operera utan upptäckt.

8 Informationssäkerhetsklasser och signalskyddsgrader

För att kunna tolka kraven på skydd mot röjande signaler i efterföljande kapitel 9, ges i detta kapitel en beskrivning av vad olika informationssäkerhetsklasser och signalskyddsgrader innebär.

I Försvarsmaktens föreskrifter om säkerhetsskydd (FFS 2003:7) behandlas säkerhetsskyddet för hemlig information i form av hemliga uppgifter, hemliga handlingar och säkerhetskänslig verksamhet. Denna hemliga information, som kan behandlas i till exempel IT-system, jämför avsnitt 9.2, indelas i fyra informationssäkerhetsklasser med följande beteckningar och betydelser.

Informationssäkerhetsklass	Betydelse
HEMLIG/ TOP SECRET 	1. Hemliga uppgifter vars röjande kan medföra synnerligt men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet (kvalificerat hemliga uppgifter). 2. Hemlig handling som har åsatts beteckningen TOP SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.
HEMLIG/ SECRET 	1. Hemliga uppgifter vars röjande kan medföra betydande men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har åsatts beteckningen SECRET eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.
HEMLIG/ CONFIDENTIAL 	1. Hemliga uppgifter vars röjande kan medföra ett inte obetydligt men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har åsatts beteckningen CONFIDENTIAL eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.
HEMLIG/ RESTRICTED 	1. Hemliga uppgifter vars röjande kan medföra endast ringa men för totalförsvaret eller förhållandet till en annan stat eller en mellanfolklig organisation eller i annat fall för rikets säkerhet. 2. Hemlig handling som har åsatts beteckningen RESTRICTED eller motsvarande av en utländsk myndighet eller mellanfolklig organisation.

Med ett signalskyddssystem, som är en speciell typ av IT-system, menas

- system med kryptografiska funktioner som är godkänt av Försvarsmaktens högkvarter och
- system för skydd mot signalunderrättelsetjänst, störsändning eller falsk signalering som är godkända av Försvarsmaktens högkvarter.

Varje signalskyddssystem avsett för sekretesskydd är godkänt upp till och med en viss signalskyddsgrad (SG). Signalskyddsgrad är således ett mått på signalskyddssystemets maximala styrka.

Ett signalskyddssystem som är avsett för skydd av uppgifter som omfattas av sekretess enligt sekretesslagen (1980:100) skall i samband med Högkvarterets godkännande placeras i någon av nedan angivna signalskyddsgrader med följande beteckningar och betydelser.

Signalskyddsgrad	Betydelse
SG TS	Signalskyddsystemet är godkänt för att behandla information som är kvalificerat hemlig eller hänförs till informationssäkerhetsklassen HEMLIG/TOP SECRET.
SG S	Signalskyddsystemet är godkänt för att behandla information som är hemlig, men inte kvalificerat hemlig, eller hänförs till informationssäkerhetsklassen HEMLIG/SECRET.
SG C	Signalskyddsystemet är godkänt för att behandla information som hänförs till informationssäkerhetsklassen HEMLIG/CONFIDENTIAL.
SG R	Signalskyddsystemet är godkänt för att behandla information som hänförs till informationssäkerhetsklassen HEMLIG/RESTRICTED.

9 Krav på skydd mot röjande signaler

Försvarsmaktens krav på skydd mot avlyssning av RÖS styrs av FM:s dokument enligt referens [3]. Kraven i detta dokument från 2006-03-24 är omarbetade för att ta hänsyn till de i kapitel 8 definierade informationssäkerhetsklasserna som införts inom Försvarsmakten och som också är internationellt gångbara. De nya kraven som återges i detta kapitel, har även tagit hänsyn till att ett godkänt RÖS-skydd kan uppnås genom att väga samman RÖS-egenskaper hos en utrustning, känd RÖS-dämpning i lokal där uppgifter bearbetas samt avstånd till okontrollerat område.

9.1 Omfattning

Endast utrustningar eller lokaler, där uppgifter bearbetas som omfattas av sekretess enligt sekretesslagen (1980:100) och som rör rikets säkerhet, omfattas av krav på RÖS-skydd.

Av säkerhetsskyddsavtal med andra stater och mellanfolkliga organisationer följer att även utrustningar eller lokaler, där uppgifter som omfattas av sekretess enligt 2 kap. 1 § sekretesslagen (1980:100) och har klassificerats i någon av nivåerna TOP SECRET, SECRET, CONFIDENTIAL eller motsvarande men som inte rör rikets säkerhet, omfattas av krav på RÖS-skydd.

9.2 Generella krav

9.2.1 Signalskyddssystem

Signalskyddssystem och system för hantering av kryptonycklar skall uppfylla kraven för RÖS-skydd U1 för att kunna godkännas för SG C, SG S och SG TS.

9.2.2 Övriga IT-system

För bearbetning av uppgifter som har placerats i någon informationssäkerhetsklass gäller generellt att utrustning med känt RÖS-säkerhetsavstånd får användas om avståndet till okontrollerat område är större än RÖS-säkerhetsavståndet. (RÖS-säkerhetsavstånd är det avstånd inom vilket röjande signaler kan uppfångas)

9.3 Specifika krav

Bearbetning av uppgifter som har placerats i informationssäkerhetsklasserna HEMLIG/TOP SECRET eller HEMLIG/SECRET skall ske

- i RÖS-skyddad utrustning (U1) eller
- inom RÖS-skyddad lokal i skalskyddsklass 1 (SS1) eller
- genom placering så att ett sammanlagt skydd motsvarande SS1 uppnåtts genom någon kombination av RÖS-egenskaper hos utrustning, känd RÖS-dämpning i lokal där uppgifter bearbetas samt avstånd till okontrollerat område

i följande fall:

a. I IT-system som nyttjas utanför Sveriges gränser.
b. I IT-system som regelbundet bearbetar kvalificerat hemliga uppgifter.
c. När förutsägbara (regelbundna) bearbetningar av stora mängder sekretessbelagda uppgifter (H/S) genomförs på permanent eller förutsägbar plats.
d. I IT-system för överföring av identitets- och behörighetskoder och som omfattas av förutsättningar enligt punkt c.
e. I kommunikationssystem, till exempel lokalt nätverk, där någon del av nätet också omfattas av förutsättningar enligt punkt c.

Bearbetning av uppgifter som har placerats i informationssäkerhetsklassen HEMLIG/CONFIDENTIAL skall ske

- i RÖS-skyddad utrustning (U2) eller
- inom RÖS-skyddad lokal skalskyddsklass 2 (SS2) eller
- genom placering så att ett sammanlagt skydd motsvarande SS2 uppnåtts genom någon kombination av RÖS-egenskaper hos utrustning, känd RÖS-dämpning i lokal där uppgifter bearbetas samt avstånd till okontrollerat område

i följande fall:

a. I IT-system som på permanent eller förutsägbar plats nyttjas utanför Sveriges gränser.
b. När förutsägbara (regelbundna) bearbetningar av stora mängder sekretessbelagda uppgifter (H/C) genomförs på permanent eller förutsägbar plats.
c. I IT-system för överföring av identitets- och behörighetskoder och som omfattas av förutsättningar enligt punkt b.
d. I kommunikationssystem, till exempel lokalt nätverk, där någon del av nätet också omfattas av förutsättningar enligt punkt b.

Bearbetning av uppgifter som har placerats i informationssäkerhetsklassen HEMLIG/RESTRICTED behöver ej ske i RÖS-skyddad utrustning. För IT-system som är anslutet till radioutrustning eller placerad i radioutrustningens omedelbara närhet skall dock risk för RÖS beaktas.

9.4 Konsekvenser

Ovan beskrivna krav innebär bland annat att skyddet koncentreras till säkerhetskritiska system och funktioner samt regelbundna och större bearbetningar av sekretessbelagda uppgifter på permanent plats. Därmed krävs normalt inte RÖS-skydd för sporadiska och enstaka bearbetningar av sekretessbelagda uppgifter.

Vid ändring av eller i lokal där dämpningsmätning skett skall förnyad analys eller mätning ske för att säkerställa att ovanstående krav fortfarande är uppfyllda.

10 Sammanlagt skydd

I referens [3] liksom i föregående kapitel 9 nämns att ett sammanlagt skydd motsvarande SS1 respektive SS2 kan uppnås genom en kombination av RÖS-egenskaper hos utrustning, känd RÖS-dämpning i lokal där uppgifter bearbetas samt avstånd till okontrollerat område. Med RÖS-egenskaper hos utrustning avses då en apparats RÖS-säkerhetsavstånd och med känd RÖS-dämpning avses ekvivalent skärmningseffektivitet enligt fördjupningsavsnittet i 6.4.

Generellt gäller att en utrustning i klass U2 placerad i ett utrymme med skalskyddsklass SS2 ger ett sammanlagt skydd motsvarande SS1. U2- och U3-utrustning kan också ges ett sammanlagt skydd motsvarande SS1 genom att avståndet till okontrollerat område är större än RÖS-säkerhetsavståndet. Ett sammanlagt skydd motsvarande SS1 innebär att utrustningen får hantera information som är placerad i informationsäkerhetsklass HEMLIG/SECRET eller HEMLIG/TOP SECRET.

Utrustningsklassen för ett antal sammankopplade utrustningar utanför skalskyddsklassat utrymme, bestäms av utrustningsklassen hos den enskilda utrustning som har sämst RÖS-skydd. Är exempelvis en U1-utrustning sammankopplad med en U2-utrustning utanför skalskyddsklassat utrymme, ska de två utrustningarna tillsammans behandlas som en U2-utrustning.

11 Provningsmetoder

Att genomföra en RÖS-undersökning är en experimentell verksamhet. Omfattningen av mätningen går inte att bestämma på förhand, i själva verket är den viktigaste delen av arbetet att bestämma omfattningen. Detta görs genom en systemundersökning där man försöker hitta alla tänkbara RÖS-mekanismer och källor. Den därpå följande mätningen kräver mångårig dokumenterad erfarenhet, detta för att korrekt kunna värdera de uppmätta signalernas informationsinnehåll.

RÖS-mätningar utförs normalt på apparatnivå. Apparater som ingår i system och som inte går att mäta separat, mäts på systemnivå. Mätresultatet blir då giltigt endast för det unika systemet (konfiguration av apparater och kablage).

Normalt sker en RÖS-mätning i laboratoriemiljö. I de fall detta inte är möjligt, kan RÖS-mätningen ske på den plats där utrustningen är installerad. På grund av de mättekniska problem som är förknippade med mätningar i användarmiljö, tilldelas då objektet ett RÖS-säkerhetsavstånd motsvarande utrustningsklass 2 eller 3. Mätresultatet gäller endast för den aktuella installationen och den plats där utrustningen är installerad.

Utrustningar som har genomgått RÖS-mätning plomberas i normala fall. Vid leveranser sker också stickprovsundersökningar som verifierar kvalitén hos levererad utrustning.

Kravgränser och provningsmetoder för RÖS-skyddade rum och RÖS-skyddade kabinett finns i öppna handlingar, se referenserna [1] och [2].

12 Sekretess

Absolut säkerhet mot avlyssning av RÖS kan inte åstadkommas utan orimliga kostnader. Mätmetoder och gränsvärden för RÖS är valda för att ge tillräcklig säkerhet i förhållande till den hotbildsbedömning som är gällande. För att hålla presumtiva RÖS-spanare i osäkerhet om de metoder och resurser som krävs för att komma över hemlig information genom RÖS-spaning, är rapporter från RÖS-undersökningar hemliga enligt 2 kap 2§ sekretesslagen (1980:100). Vilka utrustningar som godkänts som U1-eller U2-utrustningar redovisas öppet.

13 Behov av RÖS-undersökning

Då Försvarsmaktens krav på RÖS-skydd kräver en RÖS-undersökning, ska behovet av en sådan anmälas till en av Försvarets materielverk godkänd RÖS-mätplats. Resultatet från RÖS-undersökningen sammanställs i en allmän och i en teknisk rapport. Normalt är det utrustningsleverantören som själv bekostar RÖS-undersökningen.

Följande uppgifter och dokument behövs för utförandet:

- Anmälande myndighet eller företag
- Handläggare
- Allmän beskrivning av mätobjektet
- Tillgängligt mätobjekt
- Mätobjektets tekniska relation till samverkande system
- Teknisk beskrivning, manual och kretsschema
- Kontaktperson för teknisk assistans (tillverkare eller leverantör)
- Kontaktperson för assistans med driftsättning.

14 M-nummersättning av RÖS-skyddad materiel

För att kunna vidmakthålla ett RÖS-skydd över tiden krävs periodvisa underhållsåtgärder enligt särskilda rutiner. Den erforderliga spårbarheten av RÖS-skyddad materiel uppnås genom M-nummersättning enligt följande regel:

RÖS-skyddade apparater, rum och kabinett avsedda att användas inom Försvarsmakten eller anslutas till av Försvarsmakten tillhandahållet nätverk skall förses med M-nummer.

15 FMV:s uppdrag inom RÖS-området

Det är FMV:s uppgift att

- utveckla mätmetodik och gränsvärden för att säkerställa skydd mot avlyssning av RÖS,
- säkerställa en resurs för undersökning och mätningar på RÖS-skyddad materiel,
- ge anvisningar för vidmakthållande av RÖS-skydd,
- följa den tekniska utvecklingen av RÖS-hotet,
- bistå med teknisk rådgivning vid behov av RÖS-skydd.

16 Nya EU-regler för TEMPEST

Inom Europeiska unionen (EU) har regler för TEMPEST[2] utarbetats som är lika de regler som används inom North Atlantic Treaty Organization (NATO). Ett mål är att på sikt också kunna erkänna varandras TEMPEST-godkända system. Dessa regler kommer att publiceras i form av fyra informationssäkerhetsklassade ”INFOSEC Technical Policy” dokument.

- TECH-P-04 TEMPEST Basic principles
  RESTREINT UE (EU RESTRICTED)
- TECH-P-04-01 Installation of sites and systems
  RESTREINT UE
- TECH-P-04-02 TEMPEST Zoning
  RESTREINT UE
- TECH-P-04-03 TEMPEST Evaluation and Testing
  CONFIDENTIEL UE

Allmänt går ”Basic principles” ut på att det ska vara en försumbar risk att kunna tolka signaler från informationsbearbetande utrustningar, detta i likhet med den svenska RÖS-policyn. Skillnaden är att reglerna ” Installation of sites and systems” i detalj reglerar hur system skall väljas och installeras.

”TEMPEST Zoning” går ut på att dela in områden i tre zoner (0, 1 och 2) beroende på avstånd till okontrollerat område och dämpning i till exempel väggar. Dessa så kallade ”FACILITY ZONES” skiljer sig från svenska skalskyddsklasser vad gäller säkerhetsavstånd.

”TEMPEST Evaluation and Testing” delar in utrustning i tre klasser beroende på säkerhetsavstånd. Dessa kallas level A, B och C. För att hantera EU-information klassad SECRET UE och högre i ZONE 0 skall utrustning som uppfyller level A användas.

De krav som skiljer sig mest från de svenska, är kraven på installation. Man använder ett så kallat ”RED/BLACK”-koncept som innebär att man noggrant skiljer på kretsar/utrustning som behandlar hemlig information (”RED signals”) och kretsar/utrustning som behandlar öppen eller krypterad information (”BLACK signals”). Vid installation skall bland annat minimiavstånd finnas mellan röd processor och svarta ledare samt mellan röd och svart ledare. Det ställs också hårdare TEMPEST-krav på utrustning som ska användas utanför EU jämfört med utrustning som används inom EU.

Om/när Sverige antar detta regelverk måste man räkna med ett ganska omfattande extra arbete med administration och uppföljning av lokaler och utrustning där hemlig information behandlas. Sverige har dock redan förbundit sig i avtal att följa dessa regler när klassad EU- eller NATO-information behandlas i svenska informationssystem.

---

2 TEMPEST är ett samlingsbegrepp för standarder, analyser, mätningar etc som rör röjande signaler, på engelska ”compromising emanation”.

17 Referenser

[1] Elektromagnetisk skärmning av RÖS-skyddade rum, Utgåva 3, FMV, M7780-251913, 2002-03-25.

[2] Anvisning för verifiering av skärmningseffektivitet för RÖS-skyddat kabinett, FMV, TO AF LEDN 800 015995, M7784-013769, 2008-10-17.

[3] Beslut om krav på skydd mot röjande signaler (RÖS), HKV 10 755:65114, 2006-03-24.

Projektledare FMV: Göran Undén
Illustrationer: Leif Sundberg, Sörman Information AB
Layout: Mats Lundgren, Sörman Information AB
Underlagsfoto för omslag: Mats Lundgren

FMV
TEKNIK FÖR SVERIGES SÄKERHET

FMV
Försvarets materielverk
115 88 Stockholm

Besöksadress: Banérgatan 62

Tel: 08-782 40 00
Fax: 08-667 57 99

registrator@fmv.se
www.fmv.se

M7773-001851 BROSCHYR RÖS