RTCG REPORT No. 385

GSM / Anti-theft Equipment (888 - 889 MHz) Compatibility

2 April 1997

for

Janette Dobson, RA2/PNS

Project Engineer: John Mellish I.Eng, MIEIE

Project Manager: John Mellish I.Eng, MIEIE

Approved by *Bruce Ottaway*

Date *11th June 1997*

RADIOCOMMUNICATIONS AGENCY
Radio Technology & Compatibility Group,
Whyteleafe Hill,
WHYTELEAFE,
Surrey. CR3 OYY

Tel. Int. +44-(0)181-660-8456
Fax. Int. +44-(0)181-668-9856

Contents

1.0 Abstract

GSM services are planned to expand into the frequencies (888 - 889 MHz) that are currently used by some in store anti-theft equipments.

This report details the results of measurements conducted on a single in store anti-theft equipment to determine its e.r.p. and immunity from GSM transmissions, and a single GSM receiver to determine its co-channel rejection performance with respect to the type of signal radiated by the anti-theft equipment measured.

An assessment of the magnitude of the potential interference, based on the minimum coupling loss required between the two systems to avoid interference, and the application of an appropriate propagation model (Hata), is also included. This assessment predicts interference to GSM base stations from anti-theft equipments at distances of up to 8 kilometres, and interference to anti-theft equipments from GSM mobile stations at distances of up to 43 metres.

2.0 Introduction

2.1 GSM services are planned to expand into the frequencies (888 - 889 MHz) that are currently used by some in store anti-theft equipments. 888 - 889 MHz falls within the E-GSM (extended GSM) mobile transmit / base receive band which is 880 - 915 MHz. Interference mechanisms are therefore: Anti-theft equipment / GSM base station receiver and GSM mobile transmitter / anti-theft equipment.

2.2 The help assess the magnitude of the potential interference to GSM (base stations) from anti-theft equipments, measurements were conducted on a single in store anti-theft equipment to determine its UHF transmitters RF power, frequency, effective radiated power and modulation. Measurements were also conducted on a single GSM receiver, to assess the co-channel rejection performance of GSM equipment with respect to a signal carrying the same modulation as that of the anti-theft equipment measured.

The field strength (E & H) of the anti-theft equipments VLF transmitter was also measured as the manufacturer, who kindly loaned the Agency the equipment for this compatibility study, expressed an interest in these measurements.

2.3 To help assess the magnitude of the potential interference to anti-theft equipments from GSM (mobile stations), measurements were conducted on a single in store anti-theft equipment to determine its sensitivity, and also its spurious responses and blocking performance with respect to GSM signals.

3.0 Measurements on Anti Theft Equipment.

3.1 Equipment Measured.

3.1.1 Make.

The equipment measured was loaned to the RTCG specifically to assist with this GSM / Anti-theft equipment compatibility study. The manufacturers details are on file but have been withheld from this report for commercial reasons.

3.1.2 Type.

The equipment consisted of a main control unit (capable of driving up to three UHF/VLF antenna panels), two UHF/VLF antenna panels and an LED alarm indicator box. It is believed that the equipment was approved to MPT 1353 for operation within the 888 - 889 MHz band, and MPT 1337 for operation within the 0 - 185 kHz band but, because it was used by the manufacturer solely for demonstration purposes, it bore no specific identifying marks or serial numbers.

3.1.3 Operating Principle.

The equipment operated on the principle that a security tag containing a UHF antenna connected to schotty barrier diode will radiate a signal at f1±f2 when subjected to high field strengths at f1 and f2 (where f1 is the frequency of the UHF transmission and f2 is the frequency of the VLF transmission). Furthermore, the radiated signal will carry the same amplitude modulation as that applied to the VLF transmission. A receiver set to f1-f2 will therefore receive a UHF signal from a security tag, and the frequency of the modulation present can be compared with that transmitted by different VLF antennae to identify the security tags approximate location. Any signal received that is not modulated at one of modulating frequencies being transmitted (243 Hz or 333 Hz), or is also carrying modulation at a different frequency is ignored to avoid false alarms.

3.2 Transmitter Measurements.

3.2.1 RF Power (UHF).

The RF power delivered to the two UHF antennas was measured by disconnecting the antenna and connecting the antenna port to an RF power meter. See Table 1.

Table 1 RF Power Delivered to UHF Antennae

UHF Antenna Port 1	68.0 mW
UHF Antenna Port 2	77.3 mW

3.2.2 Effective Radiated Power (UHF).

The e.r.p. was measured in a partially lined chamber, using calibrated dipole antennas, a corner reflector, and a substitution method as described in MPT 1353 clause 3.5. The anti-theft equipment and the antenna being measured[1] were rotated to maximise the signal level received via a calibrated dipole in the corner reflector (the reference signal level). The anti-theft equipment was then replaced by a calibrated dipole (the substitution antenna) and an RF signal generator, and the generator level adjusted until the same reference signal level was achieved.

The RF power delivered to the substitution antenna was then measured with an RF power meter and recorded as the e.r.p. See Table 2.

Table 2	**Effective Radiated Power (UHF)**	
Horizontal Polarisation	UHF Antenna 1	145.2 mW
	UHF Antenna 2	74.4 mW
Vertical Polarisation	UHF Antenna 1	60.5 mW
	UHF Antenna 2	182.4 mW

[1] the antenna not being measured was left connected, but covered with radiation absorbent material.

3.2.3 Frequency of Operation (UHF).

The UHF operating frequency was not accurately measured but was confirmed to be within ±2.5 kHz of the nominal frequency (888.575 MHz) as displayed on a spectrum analyzer, when both the analyzer and anti-theft equipment were at ambient temperature following a 1 hour warm up period. The anti-theft equipment was capable of operating on other frequencies within the 888 - 889 MHz band, but the frequency setting (25 kHz steps) was not adjusted.

3.2.4 Signal Characteristics (UHF).

The AM and FM modulation present on the UHF signal appearing at antenna port 1 was measured with a modulation meter. See Table 3.

Table 3 **Modulation (UHF)**	
Amplitude Modulation	0.33% modulation depth
Frequency Modulation	2.1 kHz peak deviation

The phase noise of the UHF signal appearing at antenna port 1 was measured with a spectrum analyzer using a 1 kHz measurement bandwidth and the result normalised to dBc/Hz. Two discrete spurious visible above the phase noise were also measured. See Table 4.

Table 4 **Phase Noise (UHF)**	
Phase Noise	-88.6 dBc/Hz @ 20 kHz offset
Discrete spurious	-35 dBc @ 6.25 kHz offset

A detailed search to located and measure any low level spurious emissions that may have been present at other frequencies was not conducted, but none were evident.

3.2.5 Field Strength (VLF).

The electric and magnetic field strength of the 82 kHz VLF transmission was measured on an Open Area Test at a distance of 10 and 20 metres from the anti-theft equipment. The anti-theft equipment and the antenna being measured[2] were rotated through 360^0 and the maximum field strength occurring was measured with a short mono pole (E field) measuring antenna. The measurement was then repeated with a magnetic loop (H field) measuring antenna, which was also rotated during the measurement procedure to continually maximise the field. N.B. The VLF transmissions were amplitude modulated, the field strengths recorded refer to the carrier and not the peak signal levels. See Table 5.

Table 5	**Field Strength (VLF)**	
Electric	@ 10 metres distance	+93.0 dBµV/m
	@ 20 metres distance	+73.0 dBµV/m
Magnetic	@ 10 metres distance	+13.1 dBµA/m
	@20 metres distance	- 4.5 dBµA/m

[2] Field from antenna 1 only measured, antenna 2 was left connected, but covered with radiation absorbent material.

3.3 Receiver Measurements.

Immediately prior to the measurements, the internal sensitivity control of the anti-theft equipment was adjusted according to the manufacturers instructions.

3.3.1 Alarm Sensitivity and Spurious Responses. The sensitivity of the anti-theft equipments to a signal of the type radiated from a security tag was measured in a screened room using a horn antenna to radiate the tag type signal, and a calibrated dipole to measure the field strength of this signal at the anti-theft equipments antenna. Radiation absorbent material (RAM) was placed around the walls of the screened room to reduce reflections and produce a highly uniform field over the area occupied by the anti-theft equipments antenna being measured. The field uniformity, as measured by a calibrated dipole, proved to be better than ±2 dB over 100% of the desired area.

The tag type signal was simply a UHF signal containing the same amplitude modulation as VLF transmission i.e. AM modulation at 243 or 333 Hz depending on the anti-theft equipment antenna being measured (see 3.1.3 Operating Principle).

The frequency of a relatively high level (≈120 dBµV/m) tag type signal was increased from 863.575 MHz (-25 MHz) to 913.575 MHz (+25 MHz) and, at any frequency where a response was found (alarm triggered), the level of this signal was reduced (whilst fine tuning the frequency to maintain the optimum response) until the minimum level resulting in a response was found.

The field strength of the tag type signal was then measured and recorded together with the frequency of the response. See Table 6.

Table 6 **Alarm Sensitivity and Spurious Responses**		
Frequency Relative to 888.575 MHz	Response to Tag Type Signal with 243 Hz Modulation	Response to Tag Type Signal with 333 Hz Modulation
-21.483 MHz	+ 38.7 dBµV/m	+ 36.3 dBµV/m
-18.847 MHz	+ 97.2 dBµV/m	+ 95.1 dBµV/m
-16.131 MHz	+ 77.3 dBµV/m	+ 77.3 dBµV/m
-14.348 MHz	+ 88.9 dBµV/m	+ 89.6 dBµV/m
-12.565 MHz	+112.7 dBµV/m	+100.1 dBµV/m
-11.776 MHz	+115.9 dBµV/m	+120.5 dBµV/m
-10.863 MHz	+ 41.6 dBµV/m	+ 44.1 dBµV/m
- 9.788 MHz	+109.5 dBµV/m	+105.2 dBµV/m
- 8.065 MHz	+ 94.6 dBµV/m	+ 97.7 dBµV/m
- 5.349 MHz	+ 80.3 dBµV/m	+ 82.6 dBµV/m
- 0.081 MHz	+ 42.9 dBµV/m	+ 44.4 dBµV/m
+ 2.717 MHz	+ 96.9 dBµV/m	+ 98.4 dBµV/m
+ 5.374 MHz	+109.8 dBµV/m	+110.7 dBµV/m
+ 6.454 MHz	+ 98.9 dBµV/m	+ 98.6 dBµV/m
+ 7.162 MHz	+ 93.1 dBµV/m	+ 91.2 dBµV/m
+ 8.066 MHz	+102.1 dBµV/m	+100.7 dBµV/m
+ 8.308 MHz	+ 98.6 dBµV/m	+121.2 dBµV/m
+ 9.761 MHz	+106.2 dBµV/m	+106.2 dBµV/m
+10.701 MHz	+ 47.4 dBµV/m	+ 39.9 dBµV/m
+16.134 MHz	+ 87.6 dBµV/m	+ 80.9 dBµV/m
+17.999 MHz	Not measured	+ 93.4 dBµV/m
+18.891 MHz	Not measured	+ 97.5 dBµV/m
+19.422 MHz	Not measured	+115.7 dBµV/m
+20.574 MHz	Not measured	+116.8 dBµV/m
+21.485 MHz	Not measured	+ 38.2 dBµV/m
+21.649 MHz	Not measured	+ 98.8 dBµV/m
+23.738 MHz	Not measured	+102.1 dBµV/m

These results are also presented graphically in Figure 1.

3.3.2 Alarm Failure due to GSM or CW Signals. The field strength of a GSM and CW signal that stopped the anti-theft equipment from responding to a security tag within the normal detection area was measured in a screened room using the measurement configuration described in 3.3.1 Alarm Sensitivity and Spurious Responses. For these measurements however, a security tag was suspended 0.5 metres in front of the anti-theft equipments antenna being measured, to produce a continuous response (alarm). A GSM MS signal (a single burst of pseudo random data per frame) was then radiated from the horn antenna, at the frequencies at which responses had been measured in 3.3.1, and the level increased until the anti-theft equipment stopped responding to the security tag. The field strength of the GSM signal was then measured and recorded, and the measurement repeated with a CW signal. See Table 7 (on next page).

Measurements were also conducted at a number of frequencies between 863.575 MHz (-25 MHz) and 913.575 MHz (+25 MHz) at which no response had been found in 3.3.1. This was to determine the field strength required to cause an alarm failure due to blocking. See Table 8.

Table 8 **Alarm Failure due to Blocking**

Frequency Relative to 888.575 MHz	GSM MS Blocking Signal Level	CW Blocking Signal Level
±25 MHz	>118.0 dBµV/m	>121.5 dBµV/m

Table 7 Alarm Failure due to GSM or CW Signals

Frequency Relative to 888.575 MHz	GSM MS Signal Level Causing Alarm Failure	CW Signal Level Causing Alarm Failure
-21.483 MHz	+ 102 dBμV/m	+ 99.6 dBμV/m
-18.847 MHz	>118 dBμV/m	>121.5 dBμV/m
-16.131 MHz	>118 dBμV/m	>121.5 dBμV/m
-14.348 MHz	>118 dBμV/m	>121.5 dBμV/m
-12.565 MHz	>118 dBμV/m	>121.5 dBμV/m
-11.776 MHz	>118 dBμV/m	>121.5 dBμV/m
-10.863 MHz	+ 107 dBμV/m	+ 78.3 dBμV/m
- 9.788 MHz	>118 dBμV/m	>121.5 dBμV/m
- 8.065 MHz	>118 dBμV/m	>121.5 dBμV/m
- 5.349 MHz	>118 dBμV/m	>121.5 dBμV/m
- 0.081 MHz	+ 105 dBμV/m	+ 74.0 dBμV/m
+ 2.717 MHz	>118 dBμV/m	>121.5 dBμV/m
+ 5.374 MHz	>118 dBμV/m	>121.5 dBμV/m
+ 6.454 MHz	>118 dBμV/m	>121.5 dBμV/m
+ 7.162 MHz	>118 dBμV/m	>121.5 dBμV/m
+ 8.066 MHz	>118 dBμV/m	>121.5 dBμV/m
+ 8.308 MHz	>118 dBμV/m	>121.5 dBμV/m
+ 9.761 MHz	>118 dBμV/m	>121.5 dBμV/m
+10.701 MHz	+ 105 dBμV/m	+ 76.6 dBμV/m
+16.134 MHz	>118 dBμV/m	>121.5 dBμV/m
+17.999 MHz	>118 dBμV/m	>121.5 dBμV/m
+18.891 MHz	>118 dBμV/m	>121.5 dBμV/m
+19.422 MHz	>118 dBμV/m	>121.5 dBμV/m
+20.574 MHz	>118 dBμV/m	>121.5 dBμV/m
+21.485 MHz	+104 dBμV/m	+ 78.1 dBμV/m
+21.649 MHz	>118 dBμV/m	>121.5 dBμV/m
+23.738 MHz	>118 dBμV/m	>121.5 dBμV/m

These results are also presented graphically in Figures 2 and 3.

4.0 Measurements on GSM Equipment.

4.1 Equipment Measured.

4.1.1 Make.

Sharpe.

4.1.2 Type.

TQ - G400, power class 4 (2 W maximum), portable, plant number 1977.

4.2 Transmitter Measurements.

None conducted.

4.3 Receiver Measurements.

4.3.1 Co-channel Rejection. The SIM (subscriber identity module) of the GSM mobile was replaced with a test SIM that permitted communications to be established between the mobile and a Rohde & Schwarz digital radiocommunications tester (GSM test set). The GSM test set provided all of the wanted GSM signals (traffic and control channel), and BER and FER measurement facilities. The wanted traffic channel was adjusted to be at a level of -82 dBm at the receiver input, and the level of a co-channel unwanted signal (random, continuous, GSM-modulated) was increased until the Class II (RBER) reached approximately 1% under static conditions (no fading applied).

The ratio of the wanted to unwanted signals was then measured and recorded, and the measurement repeated with an unwanted signal carrying the same modulation as that of the anti-theft equipment measured in 3.2. See Table 9.

Table 9 GSM Mobile Receiver, Co-channel Rejection

Unwanted Signal, GSM (random, continuous)	+8.5 dB
Unwanted Signal, Anti-theft Equipment (CW)	+6.0 dB

5.0 Interference Assessment

5.1 Assessment Methods.

5.1.1 Minimum Coupling Loss. The commonest assessment method is based on the minimum coupling loss (MCL) required between the two systems to avoid interference. Generally the MCL is calculated and then converted to an interference distance using an appropriate propagation model. This method produces an accurate interference distance when the interference scenario is well defined (specific), but it is difficult to judge the overall magnitude of the problem from the study of a single interference scenario. Repeating the calculation for different scenarios is more informative but, without an agreed method of analysing the results, the magnitude of the problem is still open to interpretation - particularly if one or more 'worst' or 'best' case interference scenarios are included.

5.1.2 Monte Carlo. An alternative method, the Monte Carlo (MC) method, is gaining popularity but requires a complex simulation tool. The MC simulation is a statistical technique that works by considering many independent instants in time. For each instant, or simulation trial, an interference scenario is built up using a number of different random variables i.e. where the interferers are with respect to the victim, how strong the victims's wanted signal strength is, and which channels the victim and interferer are using etc. If a sufficient number of instants are considered then the probability of a certain event occurring (e.g. interference) can be calculated with a high level of accuracy.

5.1.3 Method Adopted. Unfortunately, the MC simulation tool is not readily available at present (it is still being developed). Interference to GSM has therefore been assessed using the MCL method and, although only one interference scenario has been considered, this has been selected to be 'typical' rather than a 'worst' or 'best' case. The results (interference distances) produced by this assessment method are open to interpretation, but they do provide a useful indication of the order of magnitude of the problem. Interference to anti-theft equipment has been assessed in a similar but simpler manner, since there are fewer variables and free space path loss is an appropriate propagation model for the short distances involved.

5.2 Potential Interference to GSM Base Stations (BTS).

5.2.1 E.r.p of the Interferer. The maximum e.r.p. of the anti-theft equipment measured was 182.4 mW (vertical polarisation) which, with a measured RF power of 77.3 mW, indicates that the antenna exhibited 3 to 4 dB gain. The maximum e.r.p. permitted in MPT 1353 is 500 mW. It is reasonable to assume that in most cases the maximum radiation would not be directed at a GSM BTS and, if 182 mW e.r.p. has proven adequate in practice, it seems unlikely that large numbers of anti-theft equipments would be radiating the maximum 500 mW e.r.p. A 'typical' e.r.p. of 100 mW (**+20 dBm**) toward the BTS has therefore been assumed.

5.2.2 GSM Wanted Signal Level. The reference sensitivity of a normal GSM BTS is -104 dBm. This is worst case but, although the wanted signal must be greater than this reference sensitivity, the output power of the MS is, in many cases, controlled to ensure that it is not significantly greater. A 'typical' wanted signal level of just 10 dB greater than the reference sensitivity has therefore been assumed i.e. **-94 dBm**.

5.2.3 GSM Base Station Antenna Gain. The gain of BTS antennas can be high, but **12 dBi** is considered ‘typical’.

5.2.4 GSM Co-channel Rejection of the Interferer. Although the co-channel protection required by a GSM BTS from the type of signal radiated by the anti-theft equipment examined was not measured, the co-channel protection required by a GSM MS from this type of signal (CW) was found to be **+6 dB**. As the minimum co-channel rejection performance specified for all GSM BTS and MS equipments is identical, this figure can be applied to a BTS with a fair degree of confidence.

5.2.5 The MCL required to avoid co-channel interference from an anti-theft device is given by:

$$\mathrm{MCL} = P_{\mathrm{Interferer}} - S_{\mathrm{Victim}} + G_{\mathrm{Victim}} + R_{\mathrm{Victim}} \quad \text{(dB)}$$

Where: $P_{\mathrm{Interferer}}$ = e.i.r.p. of the interferer (dBm)
S_{Victim} = wanted signal level at the victim (dBm)
G_{Victim} = antenna gain of the victim (dBi)
R_{Victim} = co-channel rejection of the interferer by the victim (dB)

Substituting the figures considered ‘typical’ (see 5.2.1 to 5.2.4) produces an MCL of 132 dB.

5.2.6 An appropriate propagation model for urban areas is the Hata model. This is given in CCIR Rep. 567-4 in terms of basic transmission loss (L_b) as:

$$L_b = 69.5 + 26.16\cdot\log_{10}(f) - 13.82\cdot\log_{10}(h_1) - a(h_2) + [44.9 - 6.55\cdot\log_{10}(h_1)]\cdot\log_{10}(R)$$

Where: L_b = transmission loss (dB)
f = frequency (150-1500 MHz)
h_1 = base station antenna height (30-200 m)
h_2 = vehicle antenna height (1-10 m)
R = distance (1-20 km)
and $a(h_2)$ = $[1.1\cdot\log_{10}(f) - 0.7]\cdot h_2 - [1.56\cdot\log_{10}(f) - 0.8]$

Transposing $R = 10^{[Lb - 69.5 - 26.16\cdot\log_{10}(f) + 13.82\cdot\log_{10}(h1) + a(h2)]/[44.9 - 6.55\cdot\log_{10}(h1)]}$

Substituting an MCL of 132 dB for L_b yields the interference distances for the ‘typical’ interference scenario considered. See Table 10.

Table 10 Interference to GSM (Interference Distances)

Height of Interferer (Anti-theft Equipment)	Height of GSM Base Station Antenna	
	25 metres	50 metres
1 metre	1.25 kilometres	1.68 kilometres
3 metres	1.73 kilometres	2.38 kilometres
10 metres	5.46 kilometres	8.1 kilometres

For information only, the free space path loss interference distance for the 'typical' scenario considered is ~100 km.

5.3 Potential Interference to Anti-theft Equipments.

5.3.1 E.r.p of the GSM MS. The maximum e.r.p. of a GSM MS is 8 W (Power Class 2), but a realistic power for the type of portable equipment that would used in close proximity to an anti-theft equipment is 2 W (Power class 4). The antenna gain for this type of equipment is small and is offset by body losses, an e.i.r.p. of 2 W (**+33 dBm**) has therefore been assumed.

5.3.2 Anti-theft Equipment Alarm Failure due to Presence of GSM Signals. A GSM transmission whose frequency fell on one of the anti-theft equipments four major spurious responses (or within the equipments wanted channel), was found to stop the equipment from responding to a security tag within the normal detection area, when the field strength of the transmission exceeded **105 dBµV/m** (typically). A 2W e.i.r.p. GSM MS would produce field strengths exceeding this figure at a distances of up to 43 metres (assuming free space path loss which is reasonably realistic for this distance). See Table 11.

On other frequencies (non-spurious response or non-wanted channel frequencies), the anti-theft equipment continued to function correctly even when subjected to the maximum field strength available (**118 dBµV/m**). It is impossible to determine from the measurements whether or not a GSM MS has the potential to produce a sufficiently high field to cause problems at these frequencies, even when in very close proximity to the anti-theft equipment. It is clear however, that a 2 W e.i.r.p. GSM MS could not cause a problem unless it were within 10 metres of the anti-theft equipment. See Table 11.

Table 11 Interference to Anti-Theft Equipment (Interference Distances)

Frequency of GSM MS Interferer	Interference Distance
Co-channel	43 metres
Spurious Response Frequency (~ ± 10.7 MHz & ± 21.4 MHz)	43 metres
Other Frequencies within ± 25 MHz	<10 metres (*probably very much less*)

6.0 Conclusions

6.1 GSM BTS.

6.1.1 The co-channel protection required by a GSM BTS from the type of signal radiated by the anti-theft equipment examined was established to be +6 dB (3 dB less than the reference co-channel rejection performance specified for a GSM transmission).

An anti-theft equipment radiating 100 mW e.r.p. toward a GSM BTS (wanted signal level of -94 dBm and antenna gain of 12 dBi), is predicted to cause interference at a distance of between 1.25 and 8 kilometres depending on the height of the anti-theft equipment and GSM BTS antenna.

6.1.2 Some interference to GSM BTS reception on channels also used by anti-theft equipment installed within the GSM cell coverage area should be expected.

6.2 Anti-theft Equipment.

6.2.1 The anti-theft equipment measured exhibited major spurious responses at approximately ±10.7 MHz and ±21.4 MHz relative to the UHF transmission (1st local oscillator) frequency. The equipments sensitivity to a tag type signal at these four major spurious response frequencies was similar to its sensitivity at its intended response frequency i.e. there appeared to be no front-end selectivity or image rejection present.

A 2 W e.i.r.p. GSM MS whose transmission frequency coincided with one of the anti-theft equipments spurious responses, or its wanted channel, is predicted to stop the equipment from responding to a security tag within the normal detection area at a distance of up to 43 metres.

6.2.2. Although the anti-theft equipment measured exhibited some major spurious responses, it did not respond with an alarm to the presence of GSM transmissions i.e. the equipments signal and logic processing, following demodulation, rendered it highly immune to false alarms.

6.2.3 As two of the major spurious responses exhibited by the anti-theft equipment measured fell within the current GSM and TACS bands, it must be assumed that alarm failures have already been occurring but have not been recognised. This is not surprising since it is only false triggering of the alarm that would be obvious. When GSM expands into the 888-889 MHz band the probability of alarm failure, due to the presence of GSM transmissions, will increase by approximately 50% i.e. the anti-theft equipment would then have three, rather than two major response frequencies falling within the frequency range of a GSM MS that could cause problems.

6.2.4 The appear to be no major technical reasons why the UHF frequency of the anti-theft equipment measured could not be adjusted to place it outside of the frequency bands that GSM is expanding into. If this were necessary, it would be in the anti-theft equipment manufacturers interest to consider suppressing the equipments spurious responses, especially as these may move into spectrum occupied by higher power transmissions e.g. broadcast television.

7.0 References

1. Reports of the CCIR, 1990. Annex to Volume V, Propagation in Non-ionized Media. Report 567-4, Propagation Data and Prediction Methods for the Terrestrial Land Mobile Service using the Frequency Range 30 MHz to 3 GHz.

2. CEPT WG-SE Paper, SE7(97)11. A Description of the Monte Carlo Simulation Tool used by Motorola in CEPT PT SE7.

8.0 Test Equipment Used

Signal Generator, Marconi 2052 (Digital/Vector), Plant Number 2421

Digital Radiocommunications Tester, Rohde & Schwarz CMD 50/53, Plant Number 2513

Spectrum Analyzer, Hewlett Packard 8591A, Plant Number 1826

Modulation Meter, Marconi 2305, Plant Number 1181

Pre-amplifier, Hewlett Packard 8447D, Plant Number 1298

Power Amplifier, Eaton 15100B, Plant Number 0575

Fixed Attenuator, Marconi 6530 (10 dB), Plant Number 1303

Power Meter, Hewlett Packard 436A, Plant Number 1625

Power Head, Hewlett Packard 8481A, Plant Number 0356

Horn Antenna, Antenna Research Associates DGR-2200/A, Plant Number 2417

Dipole Antenna (Reference), Anritsu 651A, Plant Number 1329

Dipole Antenna (Measurement & Substitution), Anritsu 651A, Plant Number 0160