Electronic Communications Committee (ECC)
within the European Conference of Postal and Telecommunications Administrations (CEPT)

**COMPATIBILITY OF PLANNED SRD APPLICATIONS WITH
CURRENTLY EXISTING RADIOCOMMUNICATION APPLICATIONS
IN THE FREQUENCY BAND 863 – 870 MHz**

**Granada, February 2004,
Revised Nicosia, May 2008**

ECC Report 37 History

<u>**Revision Note – Nicosia May 2007**</u>

In Granada, February 2004, the ECC Report 37 "Compatibility of planned SRD applications with currently existing radiocommunications applications in the frequency band 863-870 MHz" was finally adopted by WGSE meeting after having completed public consultation.

Since this publication, there have been improvements to the method of operating RFID and it was considered necessary to revise this report. It was agreed to limit the modifications of the existing report (in particular to keep the material relating to "former" RFID equipments) as much as possible while inserting revision reflecting the new RFID operation. The wording "generic SRDs" has been removed and replaced by "Non specific SRD" for consistency with Annex 1 of ECC Recommendation 70-03.

The main changes are reflected in the Annex D.5 and D.6 and in all other respects the values assumed in the original report remain unchanged.

List of Abbreviations

AFA	Adaptive Frequency Agile
CDMA	Code Division Multiple Access
CEPT	European Conference of Postal and Telecommunications Administrations
CSMA	Collision Sensing Multiple Access
CT2	Cordless telephones
DSI	Detailed Spectrum Investigations
DSSS	Direct Sequence Spread Spectrum
DTOA	Differential TOA
DVB-T	Digital Video Broadcasting – Terrestrial
EICTA	European Information & Communications Technology Industry Association
ETSI	European Telecommunications Standards Institute
FHSS	Frequency Hopping Spread Spectrum
LBT	Listen Before Transmit
MCL	Minimum Coupling Loss
PR	Pseudo Random
RFID	Radio Frequency Identification systems
SEAMCAT	Spectrum Engineering Advanced Monte Carlo Analysis Tool
SRDs	Short Range Devices
UHF	Ultra High frequency

Foreword

This report analyses the compatibility between existing and proposed new systems in accordance with the Strategic Plan for 863 – 870 MHz. The principal method for determining compatibility in this report has been use of the "Spectrum Engineering Advanced Monte Carlo Analysis Tool" (SEAMCAT – [1] and [2]).

To simulate the worst case:
- the victim receiver was assumed to be used outdoor,
- the victim link's transmitter was assumed to be used indoor, and
- the interfering transmitter was assumed to be used outdoor.

For comparison purposes a parallel study was also undertaken using Minimum Coupling Loss (MCL) method [3].

0   EXECUTIVE SUMMARY

This report considers the potential to expand the use of SRDs within the band 863 – 870 MHz as originally proposed in the DSI Phase III Consultation and the CEPT Strategic Band Plan for this specific frequency band. Particular attention has been given to the use of new techniques, which could increase the number of users able simultaneously to operate within this band.

Since publication of the original version of this report, there have been improvements to the method of operating RFID. These changes have been considered in this revised version of the report (see Annex D.5 and D.6). In all other respects the values assumed in the original report remain unchanged.

SEAMCAT has been used as the primary simulation tool for the study. Additionally, the MCL method was used for comparative purposes as a parallel study. Receiver parameters from existing ETSI standards were used in this study.

The study examined the compatibility between existing and potential new users in four steps as follows:
1. Analysis of the compatibility between existing SRDs, including compatibility with other users in adjacent bands.
2. The effect of introducing spread spectrum techniques. For the purpose of this study spread spectrum techniques are DSSS (Direct Sequence Spread Spectrum) and FHSS (Frequency Hopping Spread Spectrum). The report considers the compatibility between different spread spectrum systems, including existing SRDs and other users in adjacent bands.

3. The impact on all above mentioned systems in point 1 and 2 by introducing new specific SRD applications using spread spectrum techniques as proposed by the following ETSI System Reference Documents (SRDocs):
    - ETSI Technical Report (TR 102 069) on the operation of DSSS transponders operating in the band 865-868 MHz. This system uses a polling frequency external to the band [4]
    - ETSI Technical Report (TR 102 134) for operation of Asset Tracking using FHSS in the band 865-868 MHz [5].
4. The impact on all of the above mentioned systems in point 1, 2 and 3 when operating generic Radio Frequency Identification systems (RFID) (TR 102 649 []) at power levels up to 2 W using firstly a frequency agile "listen before each transmit" technique and secondly in accordance with the proposed 4 channel plan for interrogators (see Annex D.5).

Although existing applications were taken as the basis for comparison, it should be noted that some existing applications already experience levels of interference that are not insignificant. This has been taken into account when considering planned new applications.

It should be noted that the SEAMCAT simulations were carried out by moving the wanted transmitter of the victim link randomly within the area that the application is designed to cover. By contrast, the MCL analysis is a worst-case calculation and assumes that a wanted transmitter is operating at its extreme range with respect to the victim. As anticipated the simulation figures for probability of interference generated by SEAMCAT are lower than for the MCL approach.

Special consideration was given to the needs of Social Alarms. The study shows that the probability of interference caused by existing systems is 4.5%, while for new systems it is less.

To improve compatibility with new and existing applications, spread spectrum techniques should use a frequency agile technique, e.g. known as "Listen Before (each) Transmit (LBT)". Currently only the Radio Service CT2 uses this mitigation technique within the analysed band. The effect of LBT was simulated by excluding a co-channel scenario.

For DSSS, which features a wide bandwidth, it was not possible to obtain sufficient receiver sensitivity to ensure an effective listen-function within the meaning of LBT. Additionally, if the victim operates within a sub-band, which is completely covered by a DSSS interferer, the victim is effectively jammed. Consequently, it is recommended that DSSS should be subject to transmit duty cycle limits as defined in Table 0.1 below.

It is also proposed to encourage the introduction of LBT within existing applications in ERC/REC 70-03 [7] in order to increase efficient usage of the spectrum.

It should be noted that for non specific SRDs either duty cycle or frequency agile LBT is a mandatory requirement, this offers the following options to industry:
- For equipment without frequency agile LBT, the duty cycle limit as defined in the table 0.1 shall not be exceeded;
- For equipment with frequency agile LBT, the traditional duty cycle restriction is not required. The net result in the event of high traffic is a dynamic duty cycle limitation that is dependent on the loading of the channel.

Where LBT is recommended, the necessary parameters shall be determined within ETSI standards. Special consideration should be given in the ETSI standards to the requirements of short "service" messages such as acknowledgements (ACK) etc.

The principle conclusion from this study is that the use of spread spectrum techniques and the special systems proposed by ETSI are considered compatible if the limits given in Table 0.1 below are met.

Application	Regulatory parameters	Comments
Non-specific SRD using DSSS	**sub band 865 – 868 MHz** - max radiated power = 25 mW e.r.p. - occupied bandwidth = 0.6 MHz - max power density = 6.2 dBm/100 kHz - max duty cycle = 1 % **sub band 865 – 870 MHz** - max radiated power = 25 mW e.r.p. - occupied bandwidth = 3 MHz - max power density = -0.8 dBm/100 kHz - max duty cycle = 0.1 % **sub band 863 – 870 MHz** - max radiated power = 25 mW e.r.p. - occupied bandwidth = 7 MHz - max power density = -4.5 dBm/100 kHz - max duty cycle = 0.1 %	Implementation of LBT is not considered possible for DSSS unless a narrow band receiver is used while in the listen mode. If LBT timing is used, the timing shall be determined within ETSI standards[1]: Examples for such values are: TX on-time= 500 ms TX off-time= 15 ms
Non-specific SRD using FHSS	**sub band 865 – 868 MHz** - max radiated power = 25 mW e.r.p. - channel bandwidth = 50 kHz - number of hop channels = 60 [2] - max duty cycle = 1 % or LBT [1] **sub band 865 – 870 MHz** - max radiated power = 25 mW e.r.p. - channel bandwidth = 100 kHz - number of hop channels = 50 [2] - max duty cycle = 0.1 % or LBT [1] **sub band 863 – 870 MHz** - max radiated power = 25 mW e.r.p. - channel bandwidth = 100 kHz - number of hop channels = 70 [2] - max duty cycle = 0.1 % or LBT [1]	If LBT timing is used, the timing shall be determined within ETSI standards[1]: Examples for such values are: TX on-time= 500 ms TX off-time= 15 ms
Non-specific SRD using other digital modulations [3]	**sub band 865 – 868 MHz** - max radiated power = 10 mW e.r.p. - 200 kHz < occupied bandwidth < 3 MHz - max duty cycle = 1 % or LBT [1] **sub band 865.5 – 867.5 MHz** - max radiated power 25 mW e.r.p. - 50 kHz < occupied bandwidth < 200 kHz - max duty cycle = 0.1% or LBT [1]	If LBT timing is used, the timing shall be determined within ETSI standards[1]: Examples for such values are: TX on-time= 500 ms TX off-time= 15 ms

System for stolen cars using DSSS [4]	**sub band 865.5 – 867.5 MHz** - max radiated power = 2 W e.r.p. - occupied bandwidth = 2 MHz - max power density = 20 dBm/100 kHz - max duty cycle = 0.03 %	Effective implementation of LBT is not considered possible for DSSS. If LBT timing is used, the timing shall be determined within ETSI standards[1]: Examples for such values are: TX on-time= 500 ms TX off-time= 15 ms
System for tracking containers using FHSS	**sub band 865 – 868 MHz** - max radiated power = 500 mW e.r.p. - channel bandwidth = 25 kHz - min number of hop channels = 7 [2] - max duty cycle = 0.03 % or LBT [1]	If LBT timing is used, the timing shall be determined within ETSI standards[1]: Examples for such values are: TX on-time= 500 ms TX off-time= 15 ms
Generic RFID [5]	**sub band 865 – 868 MHz** - max radiated power = 20 μW e.r.p. except at **center frequencies of 865.7, 866.3, 866.9 and 867.5 MHz where the following parameters shall apply**- max radiated power = 2 W e.r.p. - channel bandwidth = 200 kHz - maximum period of continuous transmit on a channel = 4 s	RFID tags may respond on any channel within the sub band. Interrogators shall not be required to use LBT in the four high power channels.

Table 0.1: Implementations considered feasible

Notes:
1) LBT = "Listen Before each Transmit" with defined maximum TX on-time and minimum TX off-time. It requires mandatory receiver parameters for sensitivity, adjacent channel selectivity and blocking response. Traditional Duty Cycle restrictions are unnecessary for equipment using LBT.
2) This number of hop channels has been used in combination with the channel bandwidth for the calculation of the probability of frequency collision. A minimum number of hop channels shall be implemented in an ETSI Standard. If the minimum number of hop channels is significantly less than the numbers used in this study the probability of interference shall be verified.
3) The outcome of ETSI studies on requirements for SRDs in the UHF band was that users wanted greater data rates and higher powers. To make greater data rates possible a larger bandwidth is proposed for digital modulations techniques. It should be noted that, due to the limited spreading range, none of the spread spectrum technique are able to achieve high data rates. To restrict the spectral density to an acceptable level the output power shall be limited to 10 mW.
4) For the purpose of this study the proposed ETSI transmitter spectrum mask has been changed (see the comment below the Figure 1-4-3-2).
5) As described in Annex D.5 generic RFIDs are simulated using that frequency for the victim, which is either the adjacent channel to a high power channel if applicable, or the closest channel of the adjacent sub-band.

For information, the SEAMCAT files used for the calculations in this study are available in a zip-file at the www.ero.dk (ERO Documentation Area) next to this Report.

Table of contents

1   INTRODUCTION

A Strategic Plan for future use by Short Range Devices in the Band 863 – 870 MHz was developed as part of DSI Phase III. The studies were conducted taking into account the requirements of the R&TTE Directive, which states that the most effective use of spectrum is a prime consideration. The Report presents results of these studies.

1.1   Situation at February 2004

The frequency band 863-870 MHz has for some time been considered for short range devices (SRD) as defined in ERC Report 25 [8].

The sub-band 862 – 863 MHz is not under current consideration.

The band 863 - 865 MHz is used for radio microphones and wireless audio applications in accordance with ERC/REC 70-03 [7] Annex 10 and Annex 13 respectively.

The band 868-870 MHz is designated for different types of SRD applications with defined duty cycle and power levels in order to allow a particular type of application to develop within a particular sub-band. Thus Annex 1 to ERC REC 70-03 [7] contains the regulations for NON-specific SRD applications within 868-870 MHz and Annex 7 contains sub bands with technical parameters specifically designated for alarm systems including Social alarms within the band 869.20 - 869.25 MHz (covered by ERC Decision (97)06 [9].

In order to promote further harmonisation and stronger commitment from European Administrations the European Communications Committee has adopted ERC Decisions ERC DEC (01)04 [10], (01)09 [11] and (01)18 [12] covering SRD applications within the frequency bands 868-870 MHz and 863-865 MHz .

Other services and applications use the band 863-868 MHz such as military tactical radio links and Cordless telephones (CT2) within the band 864.1-868.1 MHz. Furthermore the band 862-863 MHz is reserved for government use in some countries.

The DSI Phase III consultation process covering the frequency band 862-3400 MHz suggested that a strategic plan be developed for the use of SRD applications within the band 862-870 MHz and that spread spectrum systems be introduced across the band 863-870 MHz for non-specific SRD applications without specific regulation of power levels and duty cycle for each type of SRD-application. Other recommendations from the DSI resulted in Decision ECC/DEC (01)02 [13] stipulating the phasing out of CT2 equipment in Europe in order to allow expansion of SRD applications in the band in two steps:
- To withdraw the designation of the frequency band 864.1 - 868.1 MHz for CT2 applications as soon as possible, but at least before the year 2005;
- To reduce the use of CT2 equipment in the 900 MHz band to the necessary minimum before the end of 2008.

The compatibility study considers CT2 characteristics on an equal basis with other techniques in the band, existing and proposed, in the expectation that CT2 equipment will continue to be used well after the date for the anticipated launch of the Strategic Plan.

The strategic plan, which was published in 2004, was developed from the results of the DSI and contributions from the ETSI and EICTA organisations. These contributions were based on surveys and consultation with SRD representatives from industry within these organisations.

1.2   Further developments

Subsequently further developments have taken places that have significantly changed the way in which RFID can operate within its designated spectrum. A compatibility analysis of this improved method of operation is provided in Annex D.5 and D.6.

1.3   Future market and frequency requirements within the band 863-870 MHz

In general the information provided by industry indicates an expanded use of the frequency band 863-870 MHz for Short Range Devices. In particular traditional telemetry/telecontrol and building automation systems as well as some radio alarms seem to indicate expansion and will require in future additional spectrum within this band. Beyond the ETSI studies, no further detailed market information for each category of SRD application is available.

The industry requests are focused on the operation of SRDs:
- within wider bands to achieve higher data rates,
- with increased power levels and duty cycles,
- with use of different techniques e.g. Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) with low power density and low duty cycles and frequency agility with listen before each transmit.

Industry in general requests continuation of existing narrow band channels within the range 868-870 MHz and the audio applications within 863-865 MHz. If major changes are made in these sub-bands sufficient transition period should be agreed.

1.4   Proposed strategy for the future use of the 863 – 870 MHz band

The strategy adopted by the WGFM for the future development of SRD applications within the band should allow for continued use of the existing SRD applications. As an example a number of the sub-bands within the band 868-870 MHz as well as the wireless audio band 863-865 MHz has just been implemented and industry needs assurance that the existing services may continue for the lifetime of the equipment.

To meet the future requirements for more spectrum in particular for non specific SRD applications and in order to open the bands within the 863-870 MHz band for SRD applications this study has been carried out to introduce spread spectrum technology including both FHSS and DSSS technology. Frequency agile systems with "listen before each transmit" could also be introduced in parts of the band when allowing higher data rates.

Unless provision is made to limit the operation of wide area networks and third party traffic there is a risk that these systems will dominate this band. This would prevent the use of SRDs for simple applications. Networks should therefore be limited to single owned use within the premises of the owner/operator.

The SRD developments within the band 863-870 MHz should adhere to the following strategy:
- The band 863-865 MHz should continue to be available for wireless audio applications and wireless microphones as well as for narrow band analogue voice devices within the sub-band 864.8-865 MHz.
- The band 868-870 MHz should continue to be available for SRD applications within sub-bands as already introduced in ERC Recommendation 70-03 [7]. Following market developments and requirements from industry consideration should be given to the power levels and duty cycle restrictions for particular sub-bands. The ongoing update of the ERC Recommendation 70-03 [7] should consider such changes based on justified requirements from industrial organisations.
- The frequency band 863-870 MHz should be considered for NON specific spread spectrum SRD applications by using Direct Sequence Spread Spectrum (DSSS) and/or Frequency Hopping Spread Spectrum (FHSS) with a power level of 25 mW. The technical parameters for the power density for DSSS and the channel scheme/power level/hopping system should be defined based on detailed compatibility studies in order to provide sufficient protection to other services in the band and in particular safety services such as Social Alarms.
- The use of any technique such as adaptive frequency agility with listen before each transmit protocols etc. to ease spectrum sharing should be encouraged as much as possible and stipulated in the ERC/REC 70-03 [7] and relevant ERC Decisions.
- The frequency band 862-863 MHz is currently reserved for government use in a number of countries and should not be designated for other radio services.
- Any networking and use of repeaters within SRD bands 863-870 MHz should be limited to single owned use within the premises of the owner operator.

1.5   General assumptions for SEAMCAT simulations

For the purpose of this study the default values of SEAMCAT scenario set-up were used, except in those cases where other values are defined below or within the tables describing the input parameters and their respective values.

The terms used within this section are the terms defined in SEAMCAT.
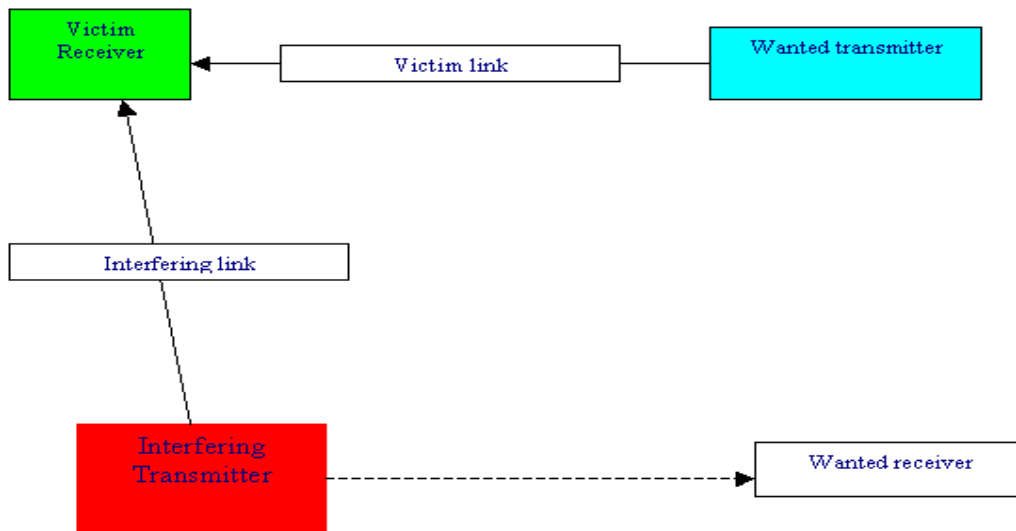
Figure 1.4: Principle of an interferer scenario and the used terms

1.5.1   Victim link

Within this study the "Wanted transmitter" (associated transmitter) is used for the victim link. The only exception is the application of Social Alarm Systems. For more details see Annexes D.1 to D.5.

1.5.1.1   Victim receiver

1.5.1.1.1   Antenna pointing

> **Antenna height**
> the antenna height was set to 1.5 m, otherwise it is noted within the tables
> **Antenna azimuth**
> the antenna azimuth was set to uniform 0° - 360°
> **Antenna elevation**
> the antenna elevation was set to constant = 0°

1.5.1.1.2   Reception characteristics

- **Noise floor**
  the noise floor is calculated from the formula
  N = kTB
  by adding 10 dB for the receiver noise figure and 5 dB for man made noise which leads to 15 dB above kTB

- **Blocking response**
  For the purposes of this study the Blocking attenuation mode was set to "Protection ratio" for relative values of the mask and to "Sensitivity" for absolute values, respectively. The values used were derived from the relevant standards. For more details see Annex D.3

- **Intermodulation rejection**
  for the purposes of this study this parameter was not used.

- **Power control**
  or the purposes of this study this parameter is not used. For more details, see under **Interfering link** below.

- **Sensitivity**
  the sensitivity used for the simulations was calculated by adding the C/(I+N) value to the calculated noise floor

- **Antenna**
  for the purposes of this study an omni-directional antenna type was defined with an antenna gain of 0 dB, if not otherwise noted within the tables.

1.5.1.1.3   Interference criteria

For the purpose of this study the criteria C/(I+N) = 8 dB was used (derived from the EN 300220-1 [14]), unless otherwise noted within the tables.

1.5.1.2   Wanted transmitter (associated transmitter)

- **Antenna** height, antenna azimuth, antenna elevation and antenna characteristics were the same as for the victim receiver described above. The power distribution was constant and equal to the value (e.r.p.) allowed for the application.

- **Wt -> Vr Path** (Wanted transmitter -> Victim receiver path) The "Coverage radius calculation mode" was set to "User defined" and the coverage radius is set to 100 m (0.1 km). Otherwise it is noted within the tables.

- **Propagation model** The Extended Hata model (SRD) was used. The general environment was set to "URBAN". To simulate a worst-case scenario, the local environment for the victim receiver was set to "OUTDOOR" and the wanted (associated) transmitter to "INDOOR".

1.5.2   Interfering link

For the purpose of this study no power control mechanism was used. Therefore, the definition of a wanted (associated) receiver was not necessary.

1.5.2.1   Interfering transmitter (It)

- **Antenna** height, antenna azimuth, antenna elevation and antenna characteristics are the same as for the victim receiver described above. The power distribution is constant and equal to the value (e.r.p.) allowed for the application.

- **Unwanted emission mask**
  Depending on the bandwidth of the wanted emission, the definition of the emission mask for unwanted emissions is based as far as applicable on the standard EN300 220-1 [14].

  Where other masks were used, this is noted in the table of input values. For details see Annex D.3.

  For special assumptions, e.g. for DSSS, see sub clause 2.4.3

- **Unwanted emission floor**: not used within this study

- **Power control:**
  not applicable for the applications being studied;
  since the "Wanted receiver (Wr)" (associated receiver) is only needed if power control is implemented, the definition of Wr and Wr -> It path was not necessary.

1.5.2.2 *It -> Vr path (interfering transmitter -> victim receiver path)*

- **Relative location**
  For the purpose of this study it was assumed that all devices will use simplex operation. It therefore follows that the maximum proportion of devices in a given population that can transmit at any instant is 50%. This figure has been used in both the SEAMCAT and MCL simulations.

  The only exceptions to this rule were DVB-T and RFID.

  For the DVB-T transmitter as interferer the relative location was set to "NONE", the number of active transmitters was set to 1 and the simulations radius, which is otherwise calculated by SEAMCAT depending on the relative location (see Annex D.4), was set to 25 km.

  Since an RFID interrogator transmits only in one direction the number of active transmitters was set equal to the density of interrogators.

- **Probability of transmissions**
  This value was set to the duty cycle defined by the application.

  In the case of frequency hoping, the duty cycle is multiplied by other factors, derived from the number of hopping frequencies and the dwell time. For details see sub clause 2.4.4.

- **Activity**
  This value was set to a constant of 1.

- *Note:*
  This feature can be used (user defined) where different kinds of interferers are active within different time periods.
  For example:
  The interferer "1" is active from 2 to 5 a.m. (with its own duty cycle), interferer "2" from 3 and 7 a.m. (with its own duty cycle, too) and so on;

  For the purpose of this study this mitigation factor was not used.

- **Time (hour)**
  As the definition of duty cycle provided by various ETSI standards and ERC/REC 70-03 [7] is based on one hour, this value was set to 1. An exception was made for DVB-T, which transmits all the time. For DVB-T as an interferer the value was set to 24.

- **Protection distance**
  This parameter gives the opportunity to define a distance from the victim beyond which any interferer is not allowed to interfere.
  For the purpose of this study this parameter was not used and therefore set to 0.

- **Propagation model**
  For the purpose of this study the Extended Hata (SRD) model was used. This propagation model takes into account the lower antenna heights usually used for SRDs.

> To simulate a "worst case", the victim and the interferer were set to "OUTDOOR". All the other values, e.g. wall losses, were therefore not relevant.

1.5.3   Assumptions made for applications using DSSS (as interferer)

To explain how within SEAMCAT the applications using DSSS are simulated, the following example, based on the SRDoc DSSS [4], may help:

- The SRDoc defines the power density mask as shown below.
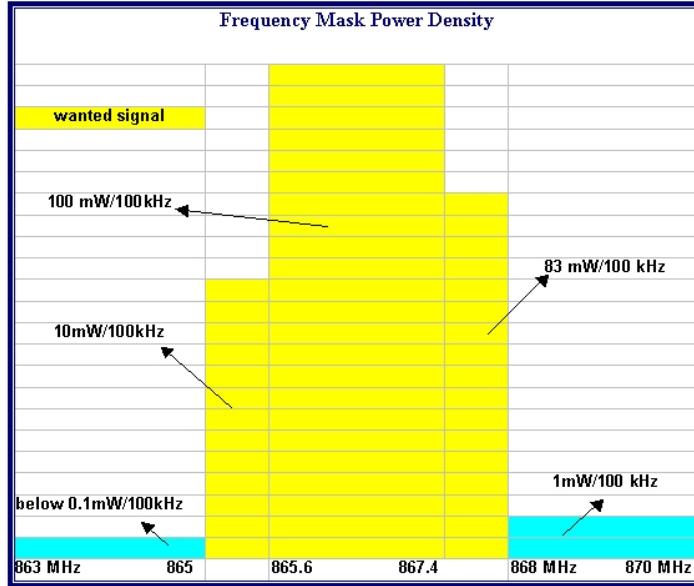
Figure 1-4-3-1: Power density mask (defined by the SRDoc DSSS, see Annex G.2)

The transmitter mask used for the SEAMCAT simulation is derived from the above mask but includes also frequencies below 863 MHz and above 870 MHz. This is illustrated in Fig 1-4-3-2 below.
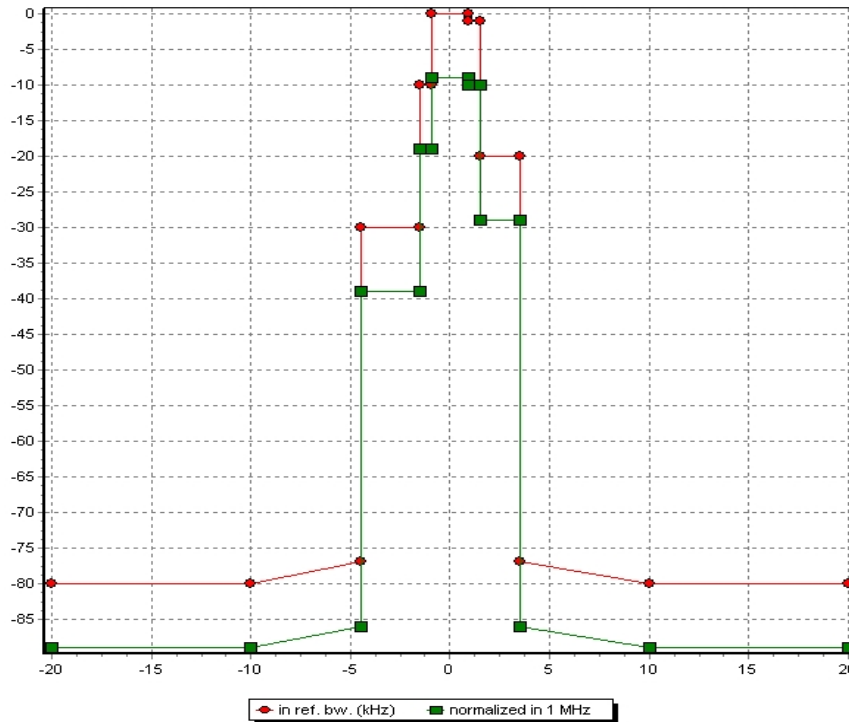
Figure 1-4-3-2: Example of a transmitter mask for a SEAMCAT simulation

Note: *This mask was not used for the simulation of DSSS. The reason is that this mask is not in line with the EN 300 220-1 [14], which defines a maximum limit of –36 dBm for spurious emissions (all emissions outside the defined sub band).*

The way to simulate this mask is as follows:
- define the complete frequency range (in this case the frequency range from 862 – 870 MHz)
  <u>*Note:*</u>
  the frequency ranges below 862 MHz and above 870 MHz are needed to cover the frequency bands for DVB-T and the TETRA/TAPS applications

- the un-attenuated power density (i.e. in this example 100 mW/100 kHz) is multiplied by the frequency range over which the power should be spread (i.e. 8 MHz)

- this gives a total power of 8 W

- enter this total power as input data into SEAMCAT as Interfering transmitter; power

- the normalized bandwidth ("Interfering transmitter -> Unwanted emission mask) within SEAMCAT is defined as the frequency range over which the total power is to be spread (i.e. 8000 kHz). SEAMCAT automatically spreads the total power over the defined normalized bandwidth

- SEAMCAT then simulates "transmission" of the spread power using the defined transmitter mask

1.5.4   Assumptions made for applications using FHSS

1.5.4.1   The interferer

The behaviour of an SRD using FHSS as an interferer can be described by the following parameters:
- output power
- bandwidth of the transmission
- duty cycle
- number of possible hops (sub-band within which it is allowed to hop)

1.5.4.2   The victim

The victim can be defined by:
- its sensitivity
- its bandwidth
- its selectivity
- its blocking response

For the purposes of simulation all of the possible mitigation factors of an FHSS scheme are transferred to the interferer.

1.5.4.3   Calculation of the probability of a frequency collision (co-channel scenario)
(see also section E.4.2.4.3.3. in Annex E)

$$P_{FREQ\_COLL} = \frac{SPAN_{OVERLAP} \cdot Max\left(BW_{INT}, BW_{VIC}\right)}{SPAN_{VIC} \cdot SPAN_{INT}}$$

where:

$SPAN_{OVERLAP}$:   is the frequency overlap range for the interferer and the victim;

$SPAN_{VIC}$:   is the allocated frequency range for the victim;

$SPAN_{INT}$:   is the allocated frequency range for the interferer;

BW_{VIC} :   is the receiver bandwidth of the victim;

BW_{INT} :   is the transmit bandwidth of the interferer.

Notes:

1. This formula is used for those scenarios where a planned system is either the interferer or the victim or both of them.

2. The probability of transmission is then calculated by P_{FREQ_COLL} * duty cycle

2   CHARACTERISTICS AND INTERFERENCE RESULTS FOR EXISTING APPLICATIONS

This section lists input data and interference results for existing applications using SEAMCAT simulations within the frequency range 863 – 870 MHz.

2.1   Short Range Devices

2.1.1   Introduction

A number of applications already exists within the frequency range 863 to 870 MHz.

The technical parameters of the equipment used in these applications are defined within the following annexes of CEPT/ERC/REC 70-03 [7]:

Annex 1   Non-specific Short Range Devices
Annex 7   Alarms
Annex 10   Radio microphones
Annex 13   Wireless Audio Applications.

2.1.2   Technical parameters of existing Short Range Devices

Values used in the simulations for existing applications are listed in the table below.

Application Category	sub-band	freq low	freq high	power	BW	duty cycle
		(MHz)	(MHz)	(mW)	(kHz)	(%)
Non-specific Short Range Devices						
Annex 1	f	868	868.6	25	na	1
	g	868.7	869.2	25	na	0.1
	h	869.3	869.4	10	25	100
	i	869.4	869.65	500	25	10
	k	869.7	870	5	na	100

Alarms

Annex 7	a	868.6	868.7	10	100	0.1
	b	869.25	869.3	10	25	0.1
	c	869.65	869.7	25	25	10
	d [1]	869.2	869.25	10	25	0.1

Radio microphones

Annex 10	c	863	865	10	200	100

Wireless Audio Applications

Annex 13	a	863	865	10	300 or 600	100
	b	864.8	865	10	50	100

Table 2.1.2: Technical parameters and values of existing short range devices

where:

freq low	lower frequency of the frequency sub-band
freq high	upper frequency of the frequency sub-band
power	output power e.r.p.
BW	bandwidth

1) This sub-band is reserved for Social Alarm Systems. For more details see Annex F.

2.1.3 *Parameters of victims*

The table below lists the values used in the simulations of existing SRDs as victims

Victim	BW (kHz)	Sensitivity (dBm)[1]	C / I (dB)	Selectivity
Annex 1 sub f	600	-93	8	EN 300 220-1 clause 9
Annex 1 sub g	500	-94	8	EN 300 220-1 clause 9
Annex 1 sub h	25	-107	8	EN 300 220-1 clause 9
Annex 1 sub i	25	-107	8	EN 300 220-1 clause 9
Annex 1 sub k	300	-96	8	EN 300 220-1 clause 9
Annex 7 sub a	100	-101	8	EN 300 220-1 clause 9
Annex 7 sub b	25	-107	8	EN 300 220-1 clause 9
Annex 7 sub c	25	-107	8	EN 300 220-1 clause 9
Annex 7 sub d	25	-107	8	EN 300 220-1 clause 9
Annex 10 sub c	200	-98	52	EN 301 357 Annex C [22]
				EN 301 357 Annex C
Annex 13 sub a	300	-96	52	EN 301 357 Annex C
Annex 13 sub a	600	-93	52	EN 301 357 Annex C
Annex 13 sub b	50	-104	8	EN 300 220-1 clause 9

Table 2.1.3: Parameters of victims and their values used for simulation

Notes:
 Calculated from the formula: $-107 + 10\log(BW/25)$. The figure of -107 dBm is derived from EN 300 220-2 referenced to a 25 kHz bandwidth [15].

The values of receiver parameters used in the study were taken from existing ETSI standards.

2.1.4   *Parameters of interferers*

The table below lists the values used in the simulations where existing SRDs are interferers

Interferer	Power (dBm) e.r.p.	BW (kHz)	Duty cycle (%)	Units per km^2
Annex 1 sub f	14	600	1	100
Annex 1 sub g	14	500	0.1	100
Annex 1 sub h	10	25	100	20
Annex 1 sub i	27	25	10	20
Annex 1 sub k	7	300	100	100
Annex 7 sub a	10	100	0.1	20
Annex 7 sub b	10	25	0.1	20
Annex 7 sub c	14	25	10	20
Annex 7 sub d	0	25	0.1	20
Annex 10 sub c	10	200	100	20
Annex 13 sub a	10	300	100	100
Annex 13 sub a	10	600	100	100
Annex 13 sub b	10	50	100	100

Table 2.1.4: Parameters of interferers and their values used for simulation

The following points should be considered when using the values in the above table.

a. **Bandwidth**
Where bandwidth is defined for an existing SRD sub-band, it is used for both the receiver and the transmitter. In all other cases the bandwidth is set to the range of the applicable sub-band.

b. **Density**
This is defined in terms of units per km^2

c. **Propagation model**
For the SEAMCAT simulation the Extended Hata SRD model has been used.

d. **Frequencies**
For the purposes of this simulation the frequencies of the different applications are set to the centre of the applicable sub-band.

e. **Exceptions:**
If the application in annex 10 sub-band c is the victim and an application in annex 13 is the interferer the frequency of the victim is set to 863.4 MHz.
If the application in annex 13 sub-band a is the victim and the application in annex 10 sub-band c is the interferer, the frequency of the victim is set to 864.3 MHz with a bandwidth of 300 kHz and the frequency of the interferer is set to 864.6 MHz with a bandwidth of 600 kHz.

These exceptions have been introduced to avoid simulation of co-channel situations.

2.1.5   *Results of SEAMCAT simulation for existing Short Range Devices*

In the following tables where the figure "<0.1" is shown, this indicates that the level of interference is insignificant.

Victim		Interferers Probability of interference in %		
Non-specific Short Range Devices	**Sub band**	**Alarms**	**Radio microphones**	**Wireless Audio Applications**
Annex 1	f	<0.1	0.1	1
	g	0.3	<0.1	0.7
	h	<0.1	0.1	0.2
	i 25 kHz	0	0	0
	i 250 kHz	0.3	0	<0.1
	k a)	0.3	0	0
Alarms		**Non-specific Short Range Devices**	**Radio microphones**	**Wireless Audio Applications**
Annex 7	a	0.4	<0.1	0.4
	b	0.22	0	0.2
	c	0.5	0	<0.1
	d b)	4.5	<0.1	5.2
Radio microphones		**Non-specific Short Range Devices**	**Alarms**	**Wireless Audio Applications**
Annex 10	c	0.1	<0.1	11
Wireless Audio Applications		**Non-specific Short Range Devices**	**Alarms**	**Radio microphones**
Annex 13	a (300 kHz)	0.2	<0.1	7
	a (600 kHz)	0.4	<0.1	6.8
	b	<0.1	0	<0.1

Table 2.1.5: Probability of interference

a)   for an output power of 5 mW (7 dBm e.r.p.) the operational radius is set to 50 m.

b)   for the purposes of this study the input value of the received signal (desired Received Signal Strength, dRSS) for the Social Alarm System as a victim is set to a constant value of −104 dBm. This is 3 dB above the level of the sensitivity as defined in EN 300 220, clause 9.1. Thus the received signal is independent of any scenario. For more details see Annex F.

The results from the SEAMCAT simulation in the table above for existing Short Range Devices show that most of the probabilities of interference are well below 1 %, with the exception of Social Alarms (4.5 %), Wireless Audio Applications (1 %, 5.2 % and 11 % depending on sub-band) and Radio Microphones (6.8 % and 7 % depending on sub-band).

2.2 Cordless Telephony (CT2) applications

2.2.1 Introduction

2.2.1.1 Market Status

The market for CT2 products is almost exclusively (>95%) based upon Cordless PABX usage. With this in mind it is worth remembering that an office PABX system has a much longer service life and represents a greater investment for the end user than that of domestic cordless telephones.

2.2.1.2 Technical description

A Cordless PABX system operates in a similar manner to a cellular network albeit on a much smaller scale and geographically confined to one building or campus. Like a cellular network the coverage of a Cordless PABX system is split up into cells, with users being able to move between these cells both during and in between calls. Location information of each subscriber is retained within the host PABX along with control of the polling of individual handsets, used to determine the nearest base station for placing a call to that user.

Base Stations in the context of a Cordless PABX system are the RF transceivers that are used to terminate/originate the RF part of the call and are controlled by the host PABX. These Base Stations are located in the office work environment, usually above head height on the interior walls. The host PABX is usually located in the central switch room with other central communications resources.

One or more Base Stations may serve an individual cell. The decision on how many Base Stations are required is based upon traffic patterns for that location. Although the CT2 allocation is 40 channels a practical limit of 8 usable channels in one particular cell is the usual maximum. However over an entire site all 40 channels may be used and in large building or campus site individual channels may be re-used.

All CT2 systems operate on a listen before transmit basis. This operates quite simply upon the receiver listening on the chosen channel prior to transmitting to check whether the level of received RF energy is below a given threshold. If it is then the channel is deemed to be free and transmission will take place, it not then another channel is selected and the process repeated.

The power output of a CT2 product (either handset or base station) is 10mW e.r.p. This gives an effective indoor range of around 50m and an outdoor range of ~200m. These distances are dependant upon the nature of the building construction, furniture etc. However when a call is placed between a handset and base station that are physically very close, the transmit power of both products may be reduced to 1mW e.r.p.

All of the above considerations are taken into account when "sizing" a customer installation to ensure that the customer will have sufficient infrastructure to meet his traffic demands.

Since the surrounding area is mainly sub urban the simulated results are likely to be worst case.

2.2.2 Technical parameters for CT2

Values used in the simulations for CT2 are listed in the table below.

Interferer	Frequency MHz	Power (dBm) e.r.p.	BW (kHz)	Duty cycle (%)
CT2	864.1 – 868.1	10	100	50

Table 2.2.2: Technical parameters of CT2

2.2.3 Parameters of CT2 as a victim

The table below lists the values used in the simulation of CT2 as a victim.

Victim	BW (kHz)	Sensitivity (dBm)	C / I (dB)	Selectivity (dB)
CT2	100	-100	15	ETS 300 131 [16]

Table 2.2.3: Parameters of CT2 as victim and its values used for simulation

2.2.4   *Parameters of CT2 as an interferer*

Values used in the simulations for CT2 as an interferer are listed in the table below

Interferer	Power (dBm) e.r.p.	BW (kHz)	Duty cycle (%)	Units per km^2
CT2	10	100	50	40

Table 2.2.4: Technical parameters of CT2

Note: All applications within an Annex are considered simultaneously as interferers

2.2.5   *Results of simulations for CT2*

2.2.5.1   *Probability of interference with CT2 as a victim*

Values used in the simulations for CT2as a victim are listed in the table below

Victim	Interferer Probability in %			
	Non-specific Short Range Devices Rec 70-03 Annex 1	Alarms Rec 70-03 Annex 7	Radio microphones Rec 70-03 Annex 10	Wireless Audio Applications Rec 70-03 Annex 13
CT2	30.2	0.2	22.1	3.2

Table 2.2.5.1: Probability of interference with CT2 as a victim

Notes: All applications within an Annex are considered simultaneously as interferers.

2.2.5.2   *Probability of interference caused by CT2*

The probability of interference caused by CT2 is listed in the table below:

Interferer	Victim Probability in %			
	Non-specific Short Range Devices Rec 70-03 Annex 1 Sub-band k	Alarms Rec 70-03 Annex 7 Sub-band d	Radio microphones Rec 70-03 Annex 10	Wireless Audio Applications Rec 70-03 Annex 13 Sub-band a (BW 600 kHz)
CT2	0.6	3.6[1]	1.0	1.2

Table 2.2.5.2: Probability of interference caused by CT2

Note: only the worst case within each Annex is listed above

1   For the purposes of this study the input value of the received signal (desired Received Signal Strength, dRSS) for the Social Alarm System as a victim is set to a constant value of –104 dBm, This is 3 dB above the level of the sensitivity as defined in EN 300 220-1, clause 9.1[13], Thus the received signal is independent of any scenario. For more details see Annex F.

3   EXISTING APPLICATIONS WITHIN ADJACENT FREQUENCY RANGES

The following section details specific applications in adjacent frequency bands. ECC WG FM requested that DVB-T and TETRA TAPS were analyzed for compatibility as part of this study.

3.1 DVB-T

3.1.1 Introduction

For details see ERC/REP 88 [17] "Compatibility and sharing analysis between DVB–T and radio microphones in bands IV and V"

3.1.2 Technical parameters

For the purposes of this study the following assumptions have been made:
- a study has been performed to show the probability of interference from DVB-T on channel 69 (centre frequency 858 MHz)
- the output power of a DVB-T transmitter is 10 kW (70 dBm) e.r.p. or 100 kW (80 dBm) e.r.p. , according to scenario
- the transmitter mask is the so-called "Chester-filter", described in sub-clause 2.1.1 Table 1 of the ERC/REP 88 [17]
- the vertical polar diagram of the antenna of the transmitter gives 3 dB-points at ±30°, 16 dB-points at ±60° and an antenna gain of 14.5 dBi
- the height of the antenna for the DVB-T transmitter has been set to 200 m (relative to the victim)
- DVB-T receiver protection ratio is based on ITU-R Recommendation BT.1368-3 (Table 22 on Page 23 therein) [18]
- for the purposes of this study calculation of the probability of interference caused by spurious emissions from a DVB-T receiver against SRD applications has not been carried out
- the antenna height of a DVB-T receiver has been set to 10 metres

3.1.3 Parameters of DVB-T receiver as victim and its values used for simulation

The table below lists the values used in the simulation of a DVB-T receiver as a victim

Victim	BW (kHz)	Sensitivity (dBm)	C / I (dB)	Receiver noise (dBm)
DVB-T receiver	7600[a]	-79.5 [b]	According Table 22 of ITU-R BT.1368-3	-98.2[c]

Table 3.1.3: Parameters of DVB-T receiver as victim and its values used for simulation

Notes:
- [a] This value is derived from ERC report 88 [17]
- [b] This value is applicable to 64-QAM (2k/8k, 2/3)
- [c] This value is valid with a 7 dB noise figure.

3.1.4 Parameters of DVB-T transmitter as interferer and its values used for simulation

Values used in the simulations for a DVB-T transmitter as an interferer are listed in the table below.

Interferer	Power e.r.p. (dBm)	BW (kHz)	Duty cycle (%)	Simulation radius
DVB-T 10 kW	70	7600	100	[a]
DVB-T 100 kW[b]	80	7600	100	[a]

Table 3.1.4: Parameters of DVB-T transmitter as interferer and its values used for simulation

[a] the simulation radius was not calculated, but set to 25 km (assumed coverage radius of DVB-T).

[b] to date no DVB-T transmitters above 10 kW are in operation although there are some test transmitters on trial at up to 100 kW.

3.1.5   *Results of SEAMCAT simulation for DVB-T systems*

3.1.5.1   *Probability of interference to DVB-T receiver*

Victim	Interferer Probability in %			
	Non-specific Short Range Devices	Alarms	Radio microphones	Wireless Audio Applications
DVB-T receiver	0	0	0	0

Table 3.1.5.1 Probability of interference to DVB-T receiver

Notes:

All applications within an Annex are considered simultaneously as interferers.
To simulate the worst case the output power of the wanted transmitter (DVB-T) is set to 10 kW e.r.p.

3.1.5.2   *Probability of interference caused by DVB-T transmitter*

The probability of interference caused by a DVB-T transmitter is listed in the table below.

Interferer	Victim Probability of %				
	Non-specific Short Range Devices Rec 70-03 Annex 1 sub band f	Alarms Rec 70-03 Annex 7 sub band d	Radio microphones Rec 70-03 Annex 10	Wireless Audio Applications Rec 70-03 Annex 13	CT2
				600 kHz	
DVB-T 10 kW	< 0.1	0.9	7.8	6.7	1.6
DVB-T 100 kW	0.4	7.1	25.9	29.3	7.2

Table 3.1.5.2: Probability of interference caused by DVB-T transmitter

Notes:

- Only the worst case within each sub-band is shown in the above table
- SRDs operate on a non-protected basis.

4   CHARACTERISTICS AND INTERFERENCE RESULTS FOR PLANNED TECHNIQUES

This section lists input data and interference results for planned techniques using SEAMCAT simulations within the frequency ranger 863-870 MHz.

4.1   Introduction

The study was specifically mandated to consider the introduction of generic spread spectrum techniques at 25 mW. It was also encouraged to consider the use of any techniques that resulted in more efficient spectrum sharing. Section 4.1 describes the techniques considered and section 4.2 contains the results of compatibility studies of these techniques.

4.1.1   *Generic Spread Spectrum*

The accepted definition of a spread spectrum system is one in which the transmitted radio signal is spread over a much larger bandwidth than would be required for sending the data stream by conventional techniques. One result of spreading the signal is that the average spectral power density is correspondingly reduced.

There are two main types of Spread Spectrum in general use: Direct Sequence and Frequency Hopping.

4.1.1.1   Generic DSSS (Direct Sequence Spread Spectrum)

DSSS is a technique in which the spread signal is generated by multiplying a narrow band signal by a high speed pseudo random code sequence. The receiver multiplies the spread spectrum signal by the same code to convert it back to a narrow band signal.

Isolation between different users in the same frequency band is achieved by selection of different codes, so called Code Division Multiple Access (CDMA). In any given implementation, the number of suitable codes is finite, in the same way that frequency channels or time slots are finite in a conventional arrangement.

The characteristics of a generic DSSS system are:
1. The transmitted energy is spread over a wide frequency range by the spreading ratio. The spreading ratio determines the amount by which the spectral power density can be reduced.
2. The transmission appears similar to wideband noise to all listeners except the intended recipient.
3. The intended receiver is able to recover the wanted data stream by de-spreading the noise like signal. This process also converts other signals into wideband noise.

The properties of DSSS are discussed in more detail in Annex G.

4.1.1.2   Generic FHSS (Frequency Hopping Spread Spectrum)

In a FHSS system the transmitter and the receiver hop in synchronised manner from one frequency to another. The hop pattern will be a pseudo random sequence covering a large number of discrete frequency channels. The transmitted energy is thus shared out over a large bandwidth, but the transmitter to receiver link still appears as a narrow band link at a given time instance.

The characteristics of a FHSS system depend on the rate of hopping, which can be classified as Fast, Slow or Very Slow.

In Fast Frequency Hopping, the dwell time on each channel is very short, for instance sufficient for only one bit of data. To a conventional receiver the resulting spectrum appears noise like. Fast Frequency Hopping is not considered further in this study as it is not commonly used. It has similar compatibility characteristics to DSSS and the results for DSSS may be taken as indicative of Fast FHSS.

In Very Slow Frequency Hopping the dwell time on each channel is very long. These systems are discussed below.

The majority of FHSS systems are Slow Hopping. The dwell time on each channel is sufficient to send a short burst of data and a transmission consists of a number of hops. In this study, generic FHSS is understood to refer to this type of system.

To another user of the band, the FHSS transmission will appear as a time divided bursts of interference. To the FHSS system, a conventional transmission will also appear as a time divided burst of interference. FHSS systems are discussed in Annex H.

4.1.1.3   Very Slow Frequency Hopping

If the dwelling time on an individual channel is long, e.g., more than 100 ms, it may be sufficient to send a complete message. In this case, a device would not change frequency during a transmission, but would make a transmission and then, at a later time, make a transmission on a new frequency.

4.1.2   Other techniques considered

4.1.2.1   Listen Before Transmit

Listen before Transmit, or Collision Sensing Multiple Access (CSMA) is commonly employed in wired or single channel systems. Each device checks whether a channel is free before transmitting; if it is not free, to avoid a collision it backs off for a given time before trying again. Listen before Transmit systems work best if all devices are able to hear all other devices. In a wired system this is the case and a simple protocol may be sufficient. In wireless systems a more elaborate protocol and/or methods of detecting collisions may be necessary.

4.1.2.2   *Frequency Selection*

If multiple frequencies are available, a frequency may be allocated to each device at the time of use. This can allow more devices to use the band than if each one operated on a pre-determined frequency. The allocations may be made by a central controller or by peer-to-peer negotiations among the devices. Only peer-to-peer negotiations are considered possible in an SRD band.

4.1.2.3   *Adaptive Frequency Agile*

Adaptive Frequency Agile (AFA) is a form of Frequency Selection, which operates on a peer-to-peer basis. Devices using the band are capable of frequency agility and select a frequency and/or timeslot in response to the environment prevailing at the time of use.

An example of a non specific AFA system is described in Annex J.

4.2   Technical parameters of planned techniques

The table below provides generic data for SRDs using DSSS technology.

DSSS System	Total RMS Power (dBm)	Power Density (dBm/100 kHz)	Occupied Bandwidth [a] (MHz)	Frequency range of operation (MHz)	Duty Cycle (%)
DSSS 0.6	14.0	6.2	0.6	865 to 868[b]	1
DSSS 3.0	14.0	-0.8	3.0	865 to 868	0.1
DSSS 7.0	14.0	-4.5	7.0	863 to 870	0.1
DSSS 2.0	33.0	20.0	2.0	865.5-867.5	0.03

Table 4.2-1: Technical parameters for DSSS as an interferer

Notes:

[a] For the purposes of this report occupied bandwidth is defined as the range within which the emission at any frequency is greater than or equal to –36 dBm.

[b] Preliminary work showed that DSSS 0.6 was incompatible with existing SRDs operating in the bands 863-865 MHz and 868-870 MHz. The study of DSSS 0.6 was therefore confined to the band 865-868 MHz.

The table below provides generic data for FHSS technology.

FHSS System	Output Power (dBm)	Frequency range (MHz)	Channel Bandwidth (kHz)	Number of Channels	Duty Cycle (%)
FHSS 3	14.0	865 to 868	50	60	1
FHSS 5	14.0	865 to 870	100	50	0.1
FHSS 7	14.0	863 to 870	100	70	0.1
FHSS 2	27.0	865 - 868	25	7	0.03

Table 4.2-2: Technical parameters for FHSS

4.3 Parameters of planned techniques as victims and their values used for simulation

The table below lists the values used in the simulation of DSSS as a victim.

Victim	Occupied Bandwidth [1] (MHz)	Blocking [2] (dBm)	Receiver Processing Gain [3] (dB)	Frequency range of operation (MHz)
DSSS 0.6	0.6	-35.0	17.0	865 to 868
DSSS 3.0	3.0	-35.0	17.0	865 to 868
DSSS 7.0	7.0	-35.0	17.0	863 to 870
DSSS 2.0	2.0	-35.0	17.0	865.5 to 867.5

Table 4.3-1: Technical parameters for DSSS as a victim

Notes:

1   For the purpose of this report occupied bandwidth is defined as the range within which the emission at any frequency is greater than or equal to –36 dBm.

2   For the purposes of this study blocking occurs at least 1 MHz outside the range of operation

3   Co-channel rejection is achieved by means of the processing gain of the receiver.

4.3.1.1   *The table below lists the values used in the simulation of FHSS as a victim*

Victim	Frequency range (MHz)	Channel Bandwidth (kHz)	Number of Channels	Receiver Sensitivity (dBm)	Blocking [1]
FHSS 3	865 to 868	50	60	-109	-35 dBm
FHSS 5	865 to 870	100	50	-106	-35 dBm
FHSS 7	863 to 870	100	70	-106	-35 dBm
FHSS 2	865 to 868	25	7	-107	84 dBc

Table 4.3-2: Technical parameters of FHSS as a victim

1   Measured at 1MHz from the centre frequency of the receiver.

4.4 Parameters of planned techniques as an interferer

The table below lists the values used in the simulation of DSSS as an interferer.

Interferer	Power Density (dBm/100 kHz)	Occupied Bandwidth [1] (MHz)	Duty cycle (%)	Units per km^2
DSSS 0.6	6.2	0.6	1	100
DSSS 3.0	-0.8	3.0	0.1	100
DSSS 7.0	-4.5	7.0	0.1	100
DSSS 2.0	20.0	2.0	0.03	100

Table 4.4.1-1: Parameters of DSSS as interferer and values used for the SEAMCAT simulation

1   For the purpose of this report occupied bandwidth is defined as the range within which the emission at any frequency is greater than or equal to -36dBm.

4.4.1.1 **The table below lists the values used in the simulation of FHSS as an interferer**

Interferer	Output Power (dBm)	Channel Bandwidth (kHz)	Duty cycle (%)	Units per km²
FHSS 3	14.0	50	1	100
FHSS 5	14.0	100	0.1	100
FHSS 7	14.0	100	0.1	100
FHSS 2	27	25	0.03	1000

Table 4.4.1-2: Parameters of FHSS as interferer and values used for the SEAMCAT simulation

4.5 Results of simulations for planned techniques

4.5.1 Probability of interference with planned techniques as a victim

The probability of interference to planned techniques from existing systems and from planned new systems is listed separately in the following two tables. For completeness the tables included the effect of DVB-T as an interferer at power levels of both 10 kW e.r.p. and 100 kW e.r.p.

4.5.1.1 Probability of interference to planned techniques from existing systems

The probability of interference to DSSS from existing systems is listed in the following table.

The simulation for FHSS was conducted using 70 channels.

Victim	Interferer Probability of interference (%)						
	Non-specific SRD Rec 70-03 Ann. 1 (h)	Alarms Rec 70-03 Annex 7 sub band c	Radio microphones Rec 70-03 Annex 10	Wireless Audio Applications Rec 70-03 Ann. 13 sub band (a) BW=600 kHz	CT2	DVB-T 100 kW e.r.p.	DVB-T 10 kW e.r.p.
DSSS 0.6	0.9	0.2	0.2	0.3	0	8.6	1.9
DSSS 3.0	3.3	0.2	0.6	1.4	0.7	11.2	2.7
DSSS 7.0	5.3	1.5	29.3	89.7	14.5	13.3	3.4
DSSS 2.0	0.1	0	0	0.1	0	2.9	0.6

Table 4.5.1.1-1: Probability of interference to DSSS by existing systems

Notes:
- All applications within an Annex are considered simultaneously as interferers.
- The probability of interference to FHSS from existing systems is listed in the following table.
- SRDs operate on a non protected basis.

Victim	Interferer Probability of interference (%)						
	Non-specific SRD Rec 70-03 Ann. 1 (h)	Alarms Rec 70-03 Annex 7 sub band c	Radio microphones Rec 70-03 Annex 10	Wireless Audio Applications Rec 70-03 Ann. 13 sub band a BW=600kHz	CT2	DVB-T 100 kW e.r.p.	DVB-T 10 kW e.r.p.
FHSS 3	-	-	-	-	12.3	0.5	0.1
FHSS 5	41.5	45.9	13.1	52.1	11.5	0.5	ns
FHSS 7	ns	ns	ns	ns	ns	ns	ns
FHSS 2	9.0	7.6	24.9	29.2	7.1	5.3	1.2

Table 4.5.1.1-2: Probability of interference to FHSS by existing systems

Notes:
a All applications within an Annex are considered simultaneously as interferers.
ns = not simulated since in all cases the probability of interference is less than the results for FHSS 5

4.5.1.2 Probability of interference to planned techniques from planned systems

The probability of interference to DSSS from existing systems is listed in the following table.

Victim	Interferer			
	Probability of interference (%)			
	DSSS 0.6	DSSS 3.0	DSSS 7.0	DSSS 2.0
DSSS 0.6	< 0.1	0.1	0.1	0.1
DSSS 3.0	1.2	0.2	0.1	0.3
DSSS 7.0	0.9	0.2	0.1	0.3
DSSS 2.0	0.4	0.1	0.1	0.1
FHSS 3	5.3	2.0	1.8	4.2
FHSS 5	3.7	2.0	1.7	1.1
FHSS 7	ns	ns	ns	ns
FHSS 2	18.4	8.2	7.9	17.8

Table 4.5.1.2-1: Probability of interference to FHSS and DSSS by DSSS

Victim	Interferer			
	Probability of interference (%)			
	FHSS 3	FHSS 5	FHSS 7	FHSS 2
DSSS 0.6	0.4	0.1	0.1	0.7
DSSS 3.0	1.0	0.1	0.1	1.1
DSSS 7.0	0.8	0.1	0.1	0.9
DSSS 2.0	0.2	0.1	0.1	0.4
FHSS 3	1.2	0.1	0.1	0.1
FHSS 5	1.1	0.1	0.1	0.1
FHSS 7	ns	ns	ns	ns
FHSS 2	4.4	0.5	0.3	0.6

Table 4.5.1.2-2: Probability of interference to DSSS and FHSS by FHSS.

4.5.1.2 *Probability of interference caused by planned techniques to existing systems*

The probability of interference to existing systems from DSSS is listed in the table below.

Interferer	Victim					
	Probability of interference (%)					
	Non-specific SRD Rec 70-03 Ann. 1 (f)	Alarms Rec 70-03 Ann. 7 (d) input level of −104 dBm	Radio microphones Rec 70-03 Annex 10 sub-band c	Wireless Audio Applications Rec 70-03 Ann. 13 sub- band a BW=600kHz	CT2	DVB-T receivers at sensitivity −79.5 dBm
DSSS 0.6	0.1	0.2	0	1.2	13.5	1.2
DSSS 3.0	< 0.1	< 0.1	< 0.1	< 0.1	< 0.1	0.1
DSSS 7.0	1.1	3.6	5.0	5.1	1.4	0.1
DSSS 2.0 [1]	< 0.1	< 0.1	< 0.1	< 0.1	0.1	0.4

Table 4.5.1.3-1: Probability of interference caused by DSSS to existing systems

Notes:
- Only the worst case within each sub-band is listed above
- A specific example of an application of DSSS technology is given in Annex G.

The probability of interference to existing systems from FHSS is listed in the table below.

Interferer	Victim					
	Probability of interference (%)					
	Non-specific SRD Rec 70-03 Ann. 1 (f)	Alarms Rec 70-03 Annex 7 sub band d	Radio microphones Rec 70-03 Annex 10	Wireless Audio Applications Rec 70-03 Annex 13 (a) BW=600kHz	CT2	DVB-T receivers at sensitivity −79.5 dBm
FHSS 3	< 0.1	< 0.1	< 0.1	< 0.1	< 0.1	1.1
FHSS 5	0.5	1.1	< 0.1	< 0.1	< 0.1	0.1
FHSS 7	< 0.1	< 0.1	1.6	1.9	1.4	0.1
FHSS 2	< 0.1	0.3	< 0.1	0.6	< 0.1	1.8

Table 4.5.1.3-2: Probability of interference caused by FHSS to existing systems

4.5.2 Other mitigation techniques

The above results show the effects of introducing generic spread spectrum in the band 863 to 870 MHz. An analysis of the techniques in para 4.1.2 appears in Section 7 of this report.

5 RFIDS USING UP TO 2 W E.R.P.

5.1 Introduction

RFID systems are used for the identification of persons, animals and objects. Radio transponders (tags) are attached to the things that are to be identified. The tags are normally in a quiescent state. However when they are brought within range of the interrogation field generated by an interrogator, the tags are activated and transmit a response. This response may comprise either identity or data, or a mixture of both.

To ensure that only the required tags send a response, the interrogator prefixes its transmission with a short identification message. This is followed by a period of continuous un-modulated carrier, which in most cases provides the energy for activation of the tags. In many situations once all the tags have been identified the interrogator will cease transmission. However there will be some situations where it may be necessary either to modify the data or to write new data to a tag. This is achieved through a short dialogue between the interrogator and tag, which ensures that the data is entered correctly. Typically both the interrogator and tag will use pulse amplitude modulation.

Reading of multiple tags within the same interrogation field is performed by means of a sophisticated anti-collision algorithm.

Users of RFID systems have increasingly requested operating ranges of at least 2 meters combined with high rates of data transfer. A study by the RFID industry has shown that the most suitable frequency range to meet this requirement is at UHF. Also calculations have shown that to achieve the necessary operating ranges, a transmit level from the interrogator of at least 2 W e.r.p. is necessary.

In the original report a compatibility analysis was performed in which RFID made use of adaptive frequency agility and listen before talk techniques as a means to avoid harmful interference to other users in the band

Subsequently chip manufacturers started to produce low cost devices with much improved input circuits. This has enabled SRD manufacturers to build products that operate at lower input sensitivities. Many of these products are battery powered with typical transmission levels of 5 mW. As a consequence the basis for the assumptions upon which RFID with LBT protected SRDs ceased to be valid. This led to the consideration of an alternative scheme in which RFID interrogators restricted their transmissions to a small number of designated channels.

The compatibility study for RFID using this alternative scheme was based on four typical scenarios. The densities of interrogators assumed for both the store and the "other" scenarios were derived from data contained in the European passive RFID marketing study [19]. This gave a figure of 12 interrogators per km^2 for both scenarios. Full details on the SEAMCAT analysis are provided at Annexes D.5 and D.6

5.2   Technical Parameters for RFID

Values used in the simulation assuming "listen before talk in RFID are listed in the table below.

RFID System	Frequency range (MHz)	Output Power (e.r.p) (dBm)	Antenna Gain (dB)	Antenna Beam Width (degrees)	Channel Band Width (kHz)	Duty Cycle (%)	Maximum operational range (m)	Maximum continuous transmitter on time(s)[a]
RFID 20	865 to 868	20.0	4	87	200	0.1	2	10
RFID 33	865.6 to 867.6	33.0	6	69	200	0.1	10	10
RFID 27	865.6 to 868	27.0	4	87	200	0.1	5	10

Table 5.2.1: Technical parameters of RFID systems as an interferer

> **[a]**   **For systems not using "listen before each transmit"** the sum of the individual "transmit on" periods shall not exceed the permitted duty cycle on any one sub-band.

In addition, when reviewing this report in 2008, the characteristics for a 4 channels RFID plan were considered as described in Annex D.5.

5.3   Parameters of RFID as a victim

The table below lists the values used in the simulation for RFID as a victim

Victim	Frequency range (MHz)	Channel Bandwidth (kHz)	Receiver Sensitivity (LBT) [1] (dBm)	Receiver Sensitivity (during operation) [2] (dBm)	Blocking [3] (dBm)
RFID 20	865 to 868	200	-83	-75	-30
RFID 33	865.6 to 867.6	200	-96	-75	-30
RFID 27	865.6 to 868	200	-90	-75	-30

Table 5.3.1: Technical parameters of RFID as a victim

Notes:
1) The Receiver sensitivity in the listen mode prior to transmission.
2) The receiver sensitivity during normal operation of the RFID system. For the purposes of the SEAMCAT study the input value of the wanted signal (tag signal) is set to –72dBm.
3) Measured at 1MHz from the center frequency of the receiver.

5.4   Parameters of RFID as an interferer

5.4.1.1   *The table below lists the values used in the simulation of RFID as an interferer*

Interferer	Output Power (dBm)	Channel Bandwidth (kHz)	Duty cycle (%)	Units per km[2] [1]
RFID 20	20.0	200	0.1	90
RFID 27	27.0	200	0.1	60
RFID 33	33.0	200	0.1	20

Table 5.4.1: Parameters of RFID as interferer and the values used for the SEAMCAT simulation

Notes:
1 These values refer only to the interrogator.
2 In order to simulate a worst case within the SEAMCAT simulation, the density of interrogators is set to 90 units/km^2 for all categories of RFID.

5.5 Results of simulations for RFID (as described in Table 5.2.1)

This section provides results for RFID using the characteristics given in Table 5.3.1 and 5.4.1.

5.5.1 Probability of interference with RFID as a victim

The probability of interference to RFID from existing systems and planned new systems is listed separately in the following two tables.

5.5.1.1 Probability of interference to RFID from existing systems

The probability of interference to RFID from existing systems is provided in the table below.

Victim	Interferer						
	Probability of interference (%)						
	Non-specific SRD Rec 70-03 Annex 1 (h)	Alarms Rec 70-03 Annex 7 sub band c	Radio microphones Rec 70-03 Annex 10	Wireless Audio Applications Rec 70-03 Annex 13 sub band a BW=600 kHz	CT2	DVB-T 100 kW e.r.p.	DVB-T 10 kW e.r.p.
RFID 20,27,33[a]	0.3	< 0.1	0	0.8	0.6	20.7	4.1

Table 5.5.1.1: Probability of interference to RFID from existing systems

[a] The sensitivity of RFID interrogators in the operational mode is the same irrespective of their transmit power. See Table 5.3.1

Note: All applications within an Annex are considered simultaneously as interferers

5.5.1.2 Probability of interference to RFID by planned new systems

The probability of interference to RFID from planned new systems is listed in the table below.

Interferer	Victim [a]
	Probability of interference (%)
	RFID 20,27,33
DSSS 0.6	6.7
DSSS 3.0	0.3
DSSS 7.0	0.3
DSSS 2.0	1.0
FHSS 3	0.7
FHSS 5	0.1
FHSS 7	0.1
FHSS 2	0.1
RFID 20	0.3
RFID 27	1.1
RFID 33	2.0

Table 5.5.1.2.1: Probability of interference to RFID as a victim from new systems

[a] The sensitivity of RFID interrogators in the operational mode is the same irrespective of their transmit power. See Table 5.3.1

5.5.2   *Probability of interference by RFID*

The probability of interference from RFID to both existing systems and planned new systems is listed separately in the following two tables.

5.5.2.1   *Probability of interference from RFID to existing systems*

The probability of interference to existing systems from RFID is listed in the table below.

Interferer	Non-specific SRD Rec 70-03 Ann. 1 (f)	Alarms Rec 70-03 sub band d	Radio microphones Rec 70-03 Annex 10	Wireless Audio Applications Rec 70-03 Annex 13 sub band a BW=600 kHz	CT2	DVB-T receivers at sensitivity −79.5 dBm
RFID 20	< 0.1	< 0.1	< 0.1	< 0.1	< 0.1	0.2
RFID 27	< 0.1	< 0.1	< 0.1	< 0.1	< 0.1	0.6
RFID 33	< 0.1	< 0.1	< 0.1	< 0.1	< 0.1	1.1

Table 5.5.2.1.1: Probability of interference from RFID to existing systems

Notes:
> - only the worst case within each sub-band is listed above
> - co-channel interference is mitigated by the LBT function – see section 7

5.5.3   *Interference between new applications within the band 863 - 870 MHz.*

As derived from SEAMCAT simulations, the results in the tables below are shown for victims with different receiver bandwidths.

5.5.3.1   *Probability of interference to new systems from RFID*

The probability of interference to planned new systems from RFID is listed in the table below

Interferer	**Victim** Probability of interference (%)							
	DSSS 0.6	DSSS 3.0	DSSS 7.0	DSSS2.0	FHSS 3	FHSS 5	FHSS 7	FHSS 2
RFID 20	< 0.1	< 0.1	0.1	0.1	0.1	0.2	ns	0.3
RFID 27	< 0.1	0.2	0.1	0.1	0.2	0.1	ns	0.6
RFID 33	< 0.1	0.3	0.1	0.1	5.7	5.0	3.8	1.1

Table 5.5.3.1.1: Probability of interference to new systems by RFID

6.5.4   **Results for RFID 4 channel plan**

Results for these systems are given in Annexes D.5 and D.6.

6   RESULTS

Examination of the results of the planned new techniques contained in sections 4 and 5 shows that not all scenarios are acceptable. Section 6.1 includes information only on those new applications that are considered feasible. This information is presented in a graphical form for ease of interpretation.

For the purpose of this study each application using a proposed new technique is considered feasible, provided that the probability of interference against the existing applications caused by this application is less than that probability of interference caused by the existing applications themselves.

The results from SEAMCAT simulations for existing Short Range Devices show that most of the probabilities of interference are well below 1%, with the exception of Social Alarms (4.5 %), Wireless Audio Applications (1 %, 5.2 % and 11 % depending on sub-band) and Radio Microphones (6.8 % and 7 % depending on sub-band).

It should be noted that the possible impact of aggravation effects by transmitter switching transients has been taken into account. In order to avoid harmful interference a rise-time and fall-ime of approximately 100 μs has been assumed. Appropriate values shall be implemented within ETSI standards.

The new application described "other digital modulations" is not shown in the figures below because the probability of interference caused by this is always less than that caused by DSSS 0.6.

6.1   SEAMCAT simulations

For all scenarios both the victim and the interferer are simulated outdoors. If a wanted transmitter (this is the transmitter of the victim link) is relevant to a simulation, it is assumed to be indoors to simulate worst case. Otherwise the level of constant receiver input power is set to 3 dB above its sensitivity (this is used, for example, to prevent the need for a more complex indoor propagation model).

The figures for the probability of interference are illustrated below: The results shown for RFID apply only for the compatibility analysis performed assuming the "listen before talk" technique.
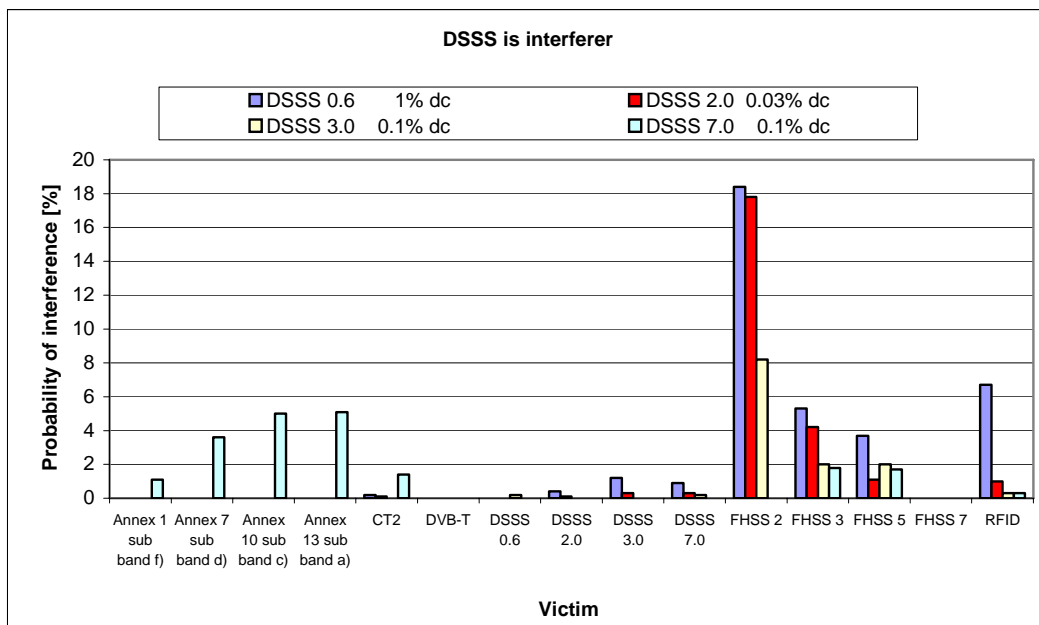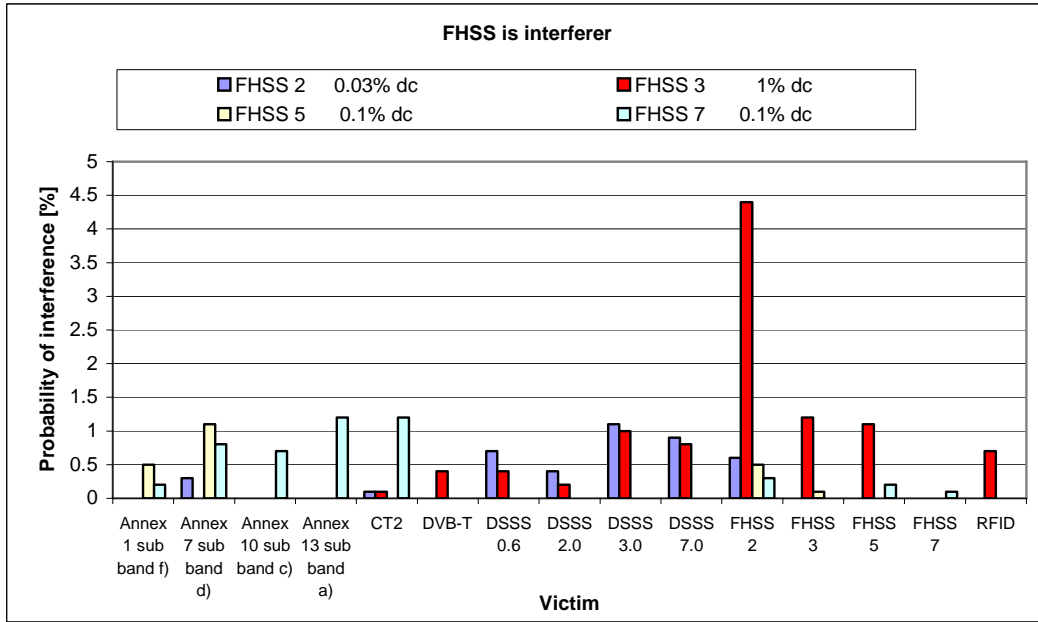
Figure 6.1.1: Probability of interference caused by DSSS
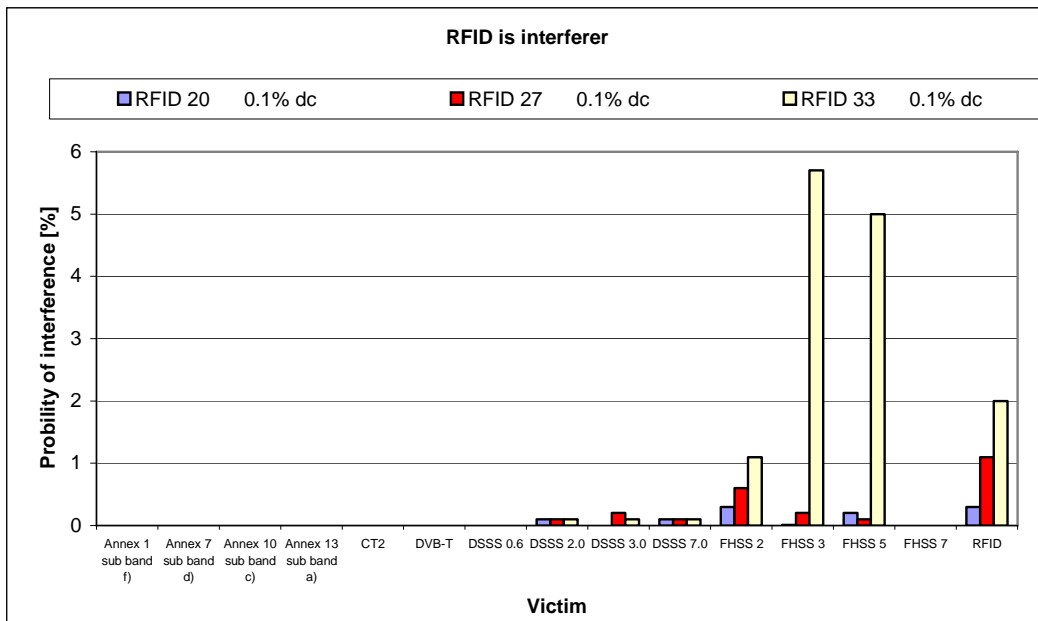
Figure 6.1.2: Probability of interference caused by FHSS

Figure 6.1.3: Probability of interference caused by RFID (co-channel)
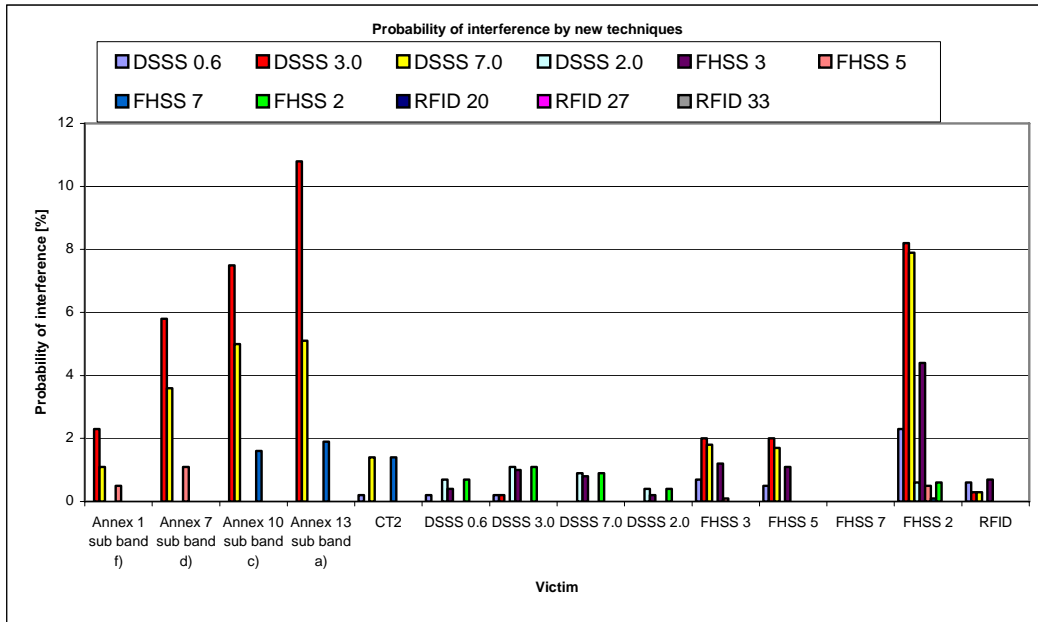
Figure 6.1.4: Probability of interference caused by the new techniques

6.2   MCL calculations

The definition of types of application and their names as used in the MCL calculations are shown in Table 7.2.1 below:

Designations for MCL in Annex E	SEAMCAT Designations	Power (mW) e.r.p.	BW (kHz)	DC (%)
DSSS 1/DSSS600kHz	DSSS 0.6	25	600	1
DSSS 2	Analysed but not proposed	25	600	10
DSSS 3	Analysed but not proposed	25	600	100
DSSS 4/DSSS2 MHz	DSSS 2.0	2000	1800	0.03
FHSS 1/FSSS25	FHSS 5 & 7	25	100	1
FHSS 2	Analysed but not proposed	25	100	10
FHSS 3	Analysed but not proposed	25	100	100
FHSS 4/FHSS 25	FSSS 2	500	25	0.03
RFID 1	RFID 20	100	200	30
RFID 2	RFID 27	500	200	30
RFID 3	RFID 33	2000	200	30
SRD 1	Rec 70-03 Annex 1 & 7	10	15	100
SRD 2	Rec 70-03 Annex 1 & 7	25	100	1
SRD 3	Rec 70-03 Annex 1 & 7	500	250	10
Microphones	Rec 70-03 Annex 10 & 13	10	200	100
Wireless audio	Rec 70-03 Annex 10 & 13	10	300	100
Consumer audio	Rec 70-03 Annex 10 & 13	10	50	100
CT 2	CT2	10	100	LBT

Table 6.2.1: Definition of types of applications and their names for MCL
Note: *For details see Annex E sub clause E.3.1*

It should be noted that the applications of SRD1, SRD2 and SRD3 are allocated within different sub bands, so the probability of frequency collision is also different, i.e. the probability of interference is not only correlated to the receiver bandwidth of the victim.

It should also be noted that the DSSS1, DSSS2 and DSSS3 are assumed as co-channel interferers over the complete frequency range 863 – 870 MHz . Since this gives an unacceptable probability of interference, the SEAMCAT simulation was redefined to give a satisfactory result by adjusting the values for sub bands, max bandwidths, max power density and lower duty cycles.

It is important to note that the use of an I/N of 0 dB for the MCL calculation represents the worst case since it assumes a receiver sensitivity equal to the receiver noise level. The measurement procedures in ETSI standards define a wanted input power of 3 dB above the sensitivity. Therefore a "SEAMCAT correction factor" of 3 dB has been used within the MCL calculation.

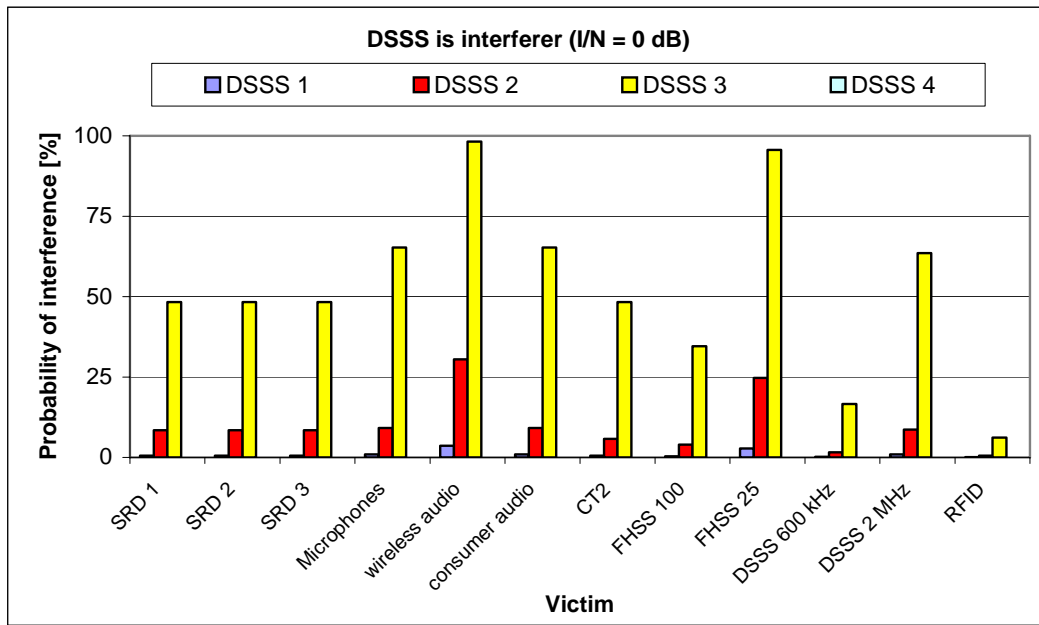The figures below show the scenarios "Urban, outdoor to outdoor, max units".

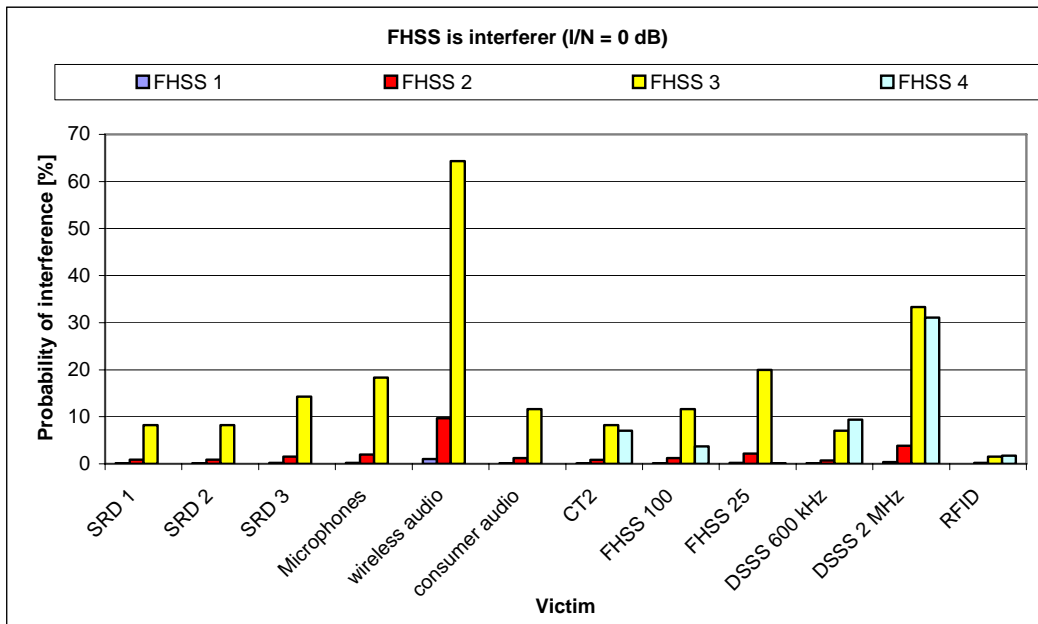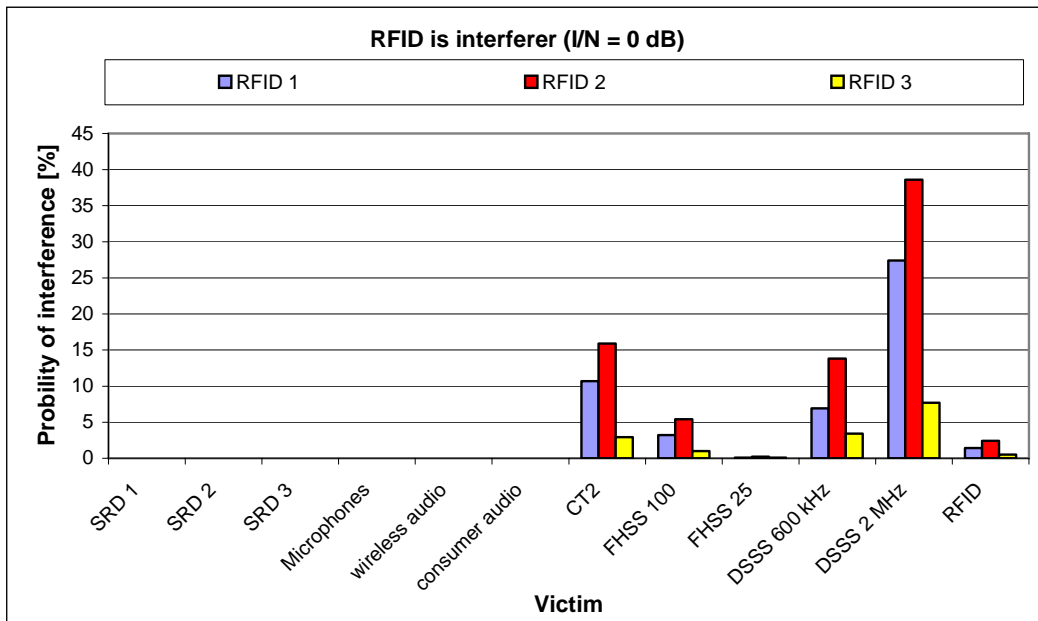**Figure 6.2.2: Probability of interference caused by DSSS (I/N = 0 dB)**

FHSS is interferer (I/N = 0 dB)

Figure 6.2.3: Probability of interference caused by FHSS (I/N = 0 dB)

RFID is interferer (I/N = 0 dB)

Note: *The probability of interference caused by RFID3 (2 W) is less than the RFID2 (500 mW) because of the use of a 6 dB gain antenna with a beam width of 69° instead of a 4 dB antenna with 87° beam width*
**Figure 6.2.4: Probability of interference caused by RFID (I/N = 0 dB)**

6.3 Comparison of the minimum protection distances between SEAMCAT and MCL

The figure 6.3.1 below shows a comparison of the minimum protection distances calculated using MCL and SEAMCAT based data.

The corresponding types of application and their names are shown in Table 6.3.1 below:

MCL	SEAMCAT
DSSS 600 kHz	**DSSS 0.6**
DSSS 2 MHz	**DSSS 2.0**
RFID1	**RFID 20**
RFID2	**RFID 27**
RFID3	**RFID 33**

Table 6.3.1: Types of applications and their names used for MCL and SEAMCAT, respectively
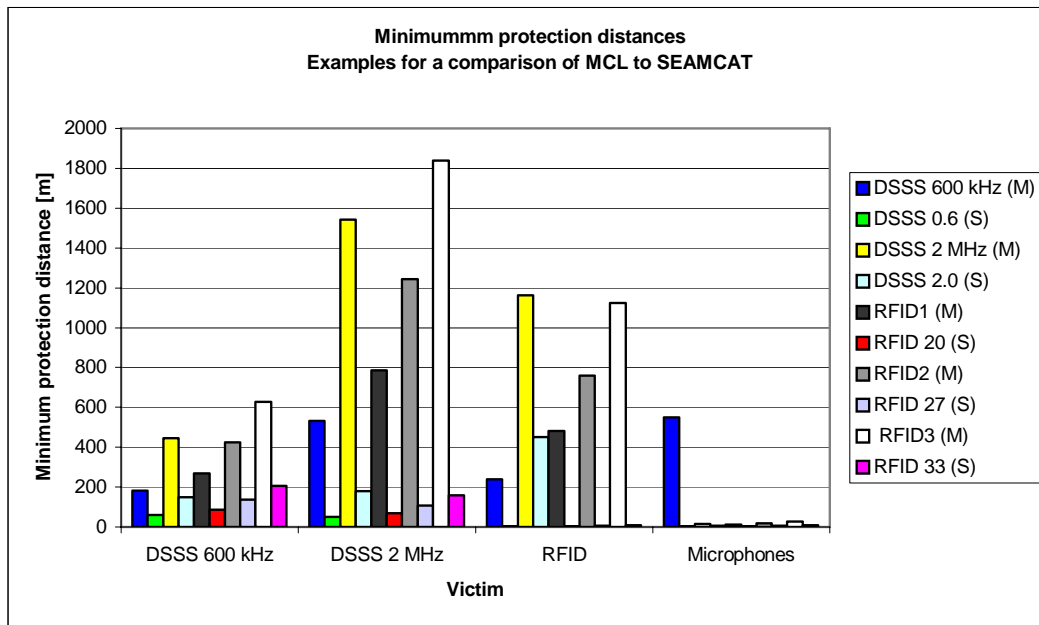
Notes: 1)   *(M) stands for MCL, (S) stands for SEAMCAT*
          2)   *For the purpose of this study a processing gain of 17 dB (for DSSS) is also used for the calculation of the minimum protection distances*

Figure 6.3.1: Examples for a comparison of the minimum protection distances MCL to SEAMCAT

Although the same formula for propagation loss (Modified Hata (SRD)) has been used for both the calculation based on the input values for MCL and the data for SEAMCAT, comparison of the minimum protection distances shows significant differences.

Reasons are:
- The MCL calculation is based on I/N = 0 dB.
- In accordance with the standards SEAMCAT uses C/(I+N) e.g. 8 dB. In cases where I=N, (ie I/N=0 dB) the minimum usable sensitivity within the SEAMCAT simulations is 11 dB above the receiver noise value used in the MCL calculations.
- MCL does not take into account the minimum usable sensitivity of an RFID receiver during its operational mode, which is defined by the needs of its application. Therefore, for the SEAMCAT simulation the sensitivity is set to –75 dBm instead of -105.8 dBm as calculated by MCL.
- MCL assumes that both DSSS 600 kHz and FHSS 100 kHz are allocated over the complete frequency range 863 – 870 MHz (see also sub clause 7.2 above). Therefore, these are always considered to be co-channel interferers. For the SEAMMCAT simulation DSSS 0.6 is assumed to operate only within the sub band 865 – 868 MHz.

6.4 Protection Distances derived from the MCL calculation

(based on the input parameters used for SEAMCAT simulations)

The figures below show the minimum protection distances calculated using the same input parameters as defined for SEAMCAT simulations. The propagation model used is also "Modified Hata (SRD) outdoor - outdoor".

The use of the LBT feature prevents co-channel interference. Results incorporating LBT have been shown in the figures under "off-channel" scenarios. The victim used for this comparison is the most critical application which is Social Alarms.
It should be noted that the same results will be obtained for any other victim that has a bandwidth of 25 kHz.
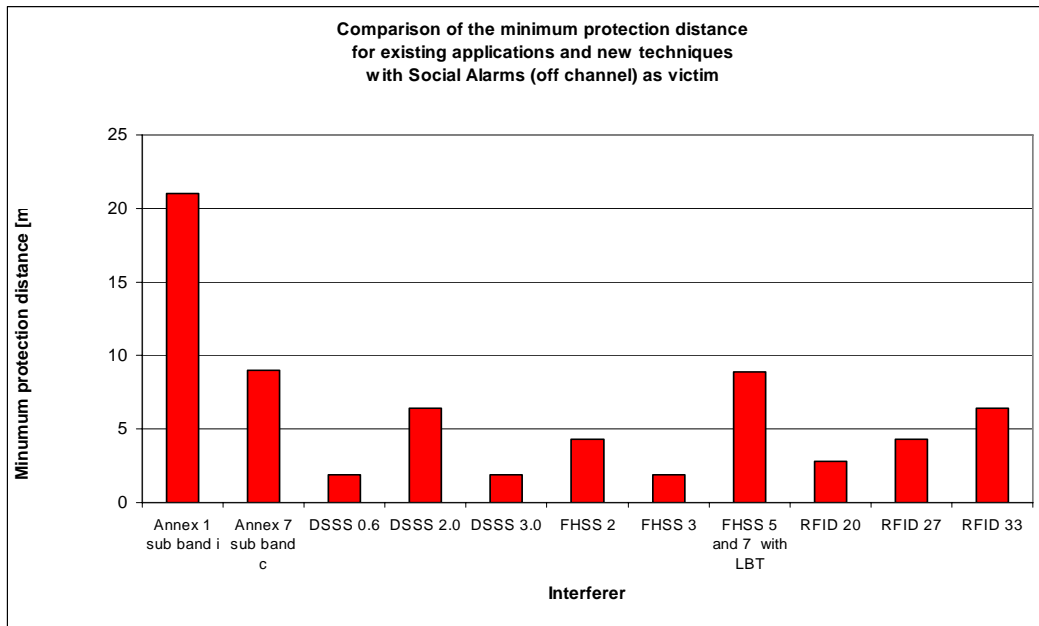
Note: *The minimum protection distance for FHSS not using LBT would be 589 m (see Figure 6..4.3 below)*
Figure 6.4.1: Minimum protection distances for existing applications and new techniques with Social Alarms as victim. The FHSS 5 and FHSS 7 are assumed to use LBT

The figure above shows that the minimum protection distance needed for interferers using new techniques is always less than that distance necessary for an existing Non-specific SRD according to ERC/REC 70-03 [9] Annex 1 sub band (i)as interferer.

In accordance with EN 300 220 [14] [15] for frequency separations of less than 1 MHz an "off channel" attenuation of 60 dB (adjacent channel selectivity) is used. For frequency separations of more than 1 MHz a blocking response of 84 dB (for class 1 receivers) is used.
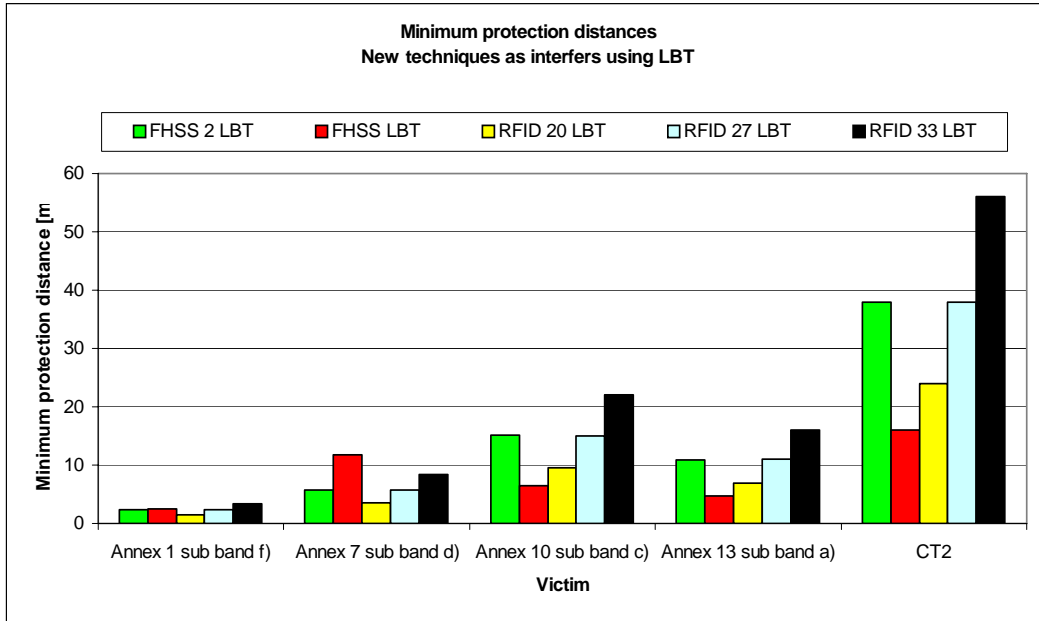
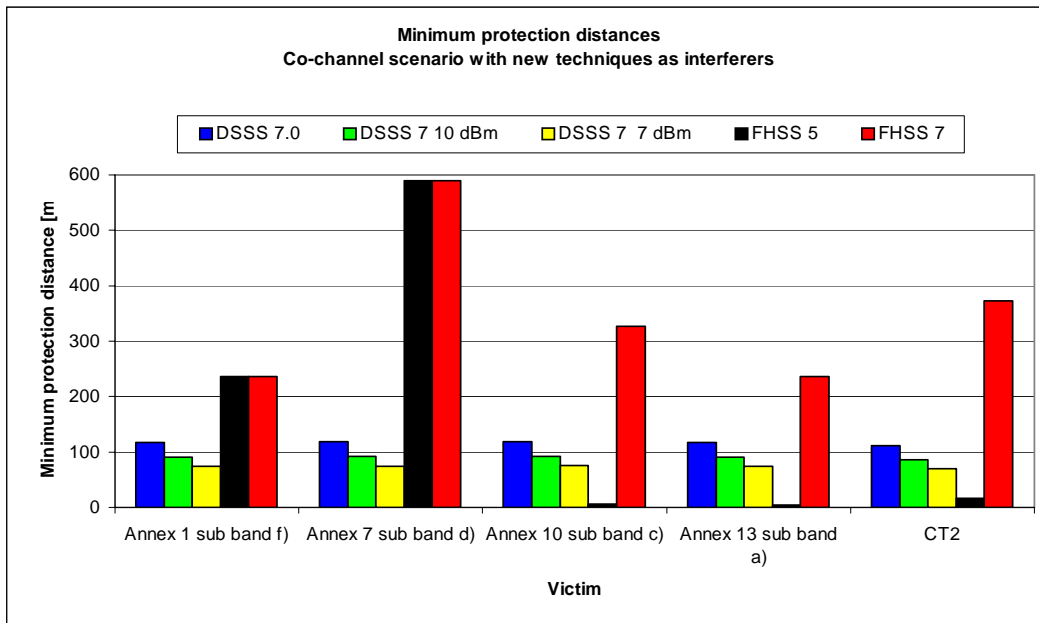**Figure 6.4.2: Minimum protection distances for existing applications (off channel)**

Figure 6.4.3: Minimum protection distances for existing applications (co-channel scenario)
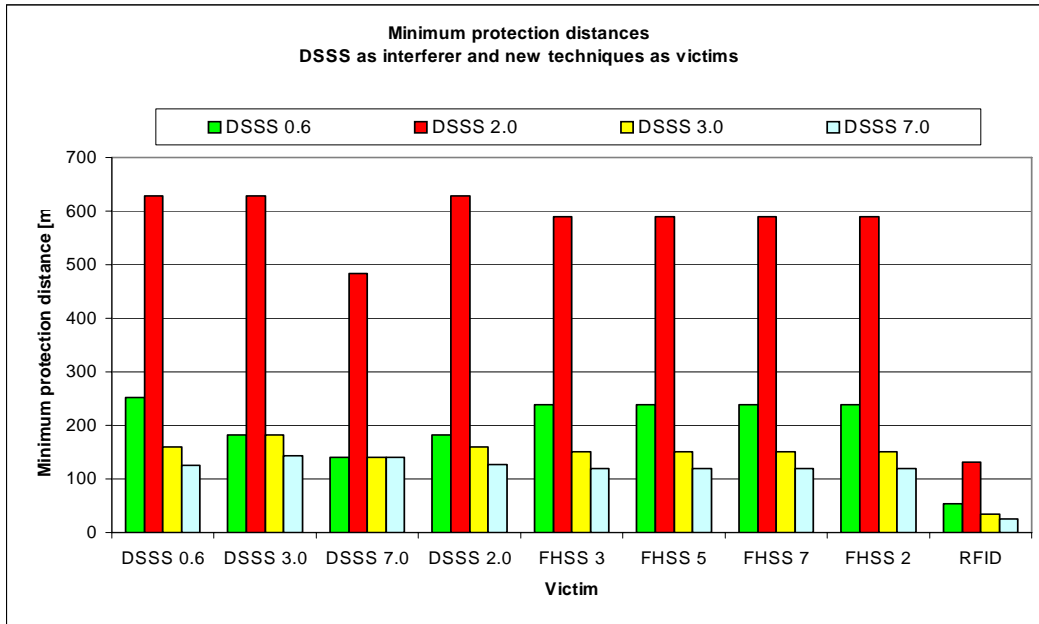
Figure 6.4.4: Minimum protection distance DSSS as interferer and new techniques as victims
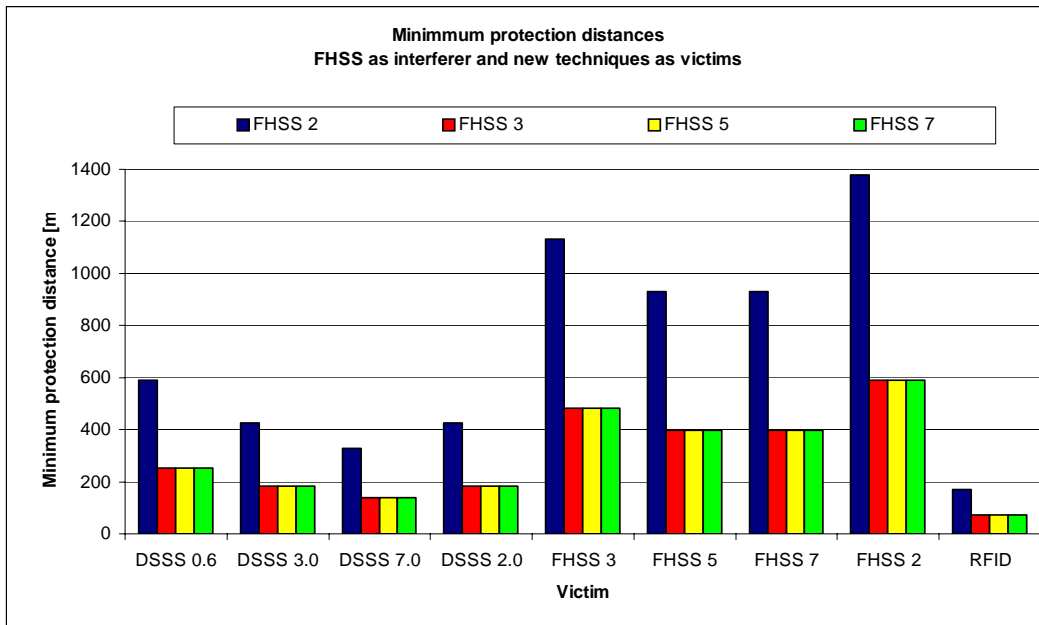
Figure 6.4.5: Minimum protection distances FHSS as interferer and new techniques as victims
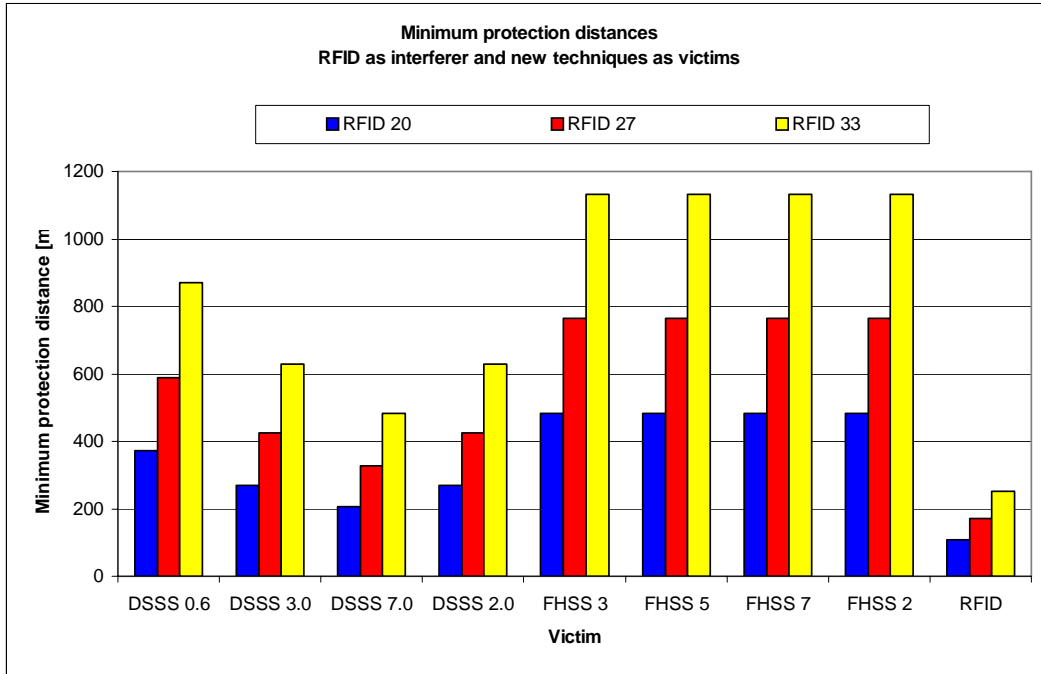
Figure 6.4.6: Minimum protection distance RFID as interferer and new techniques as victims
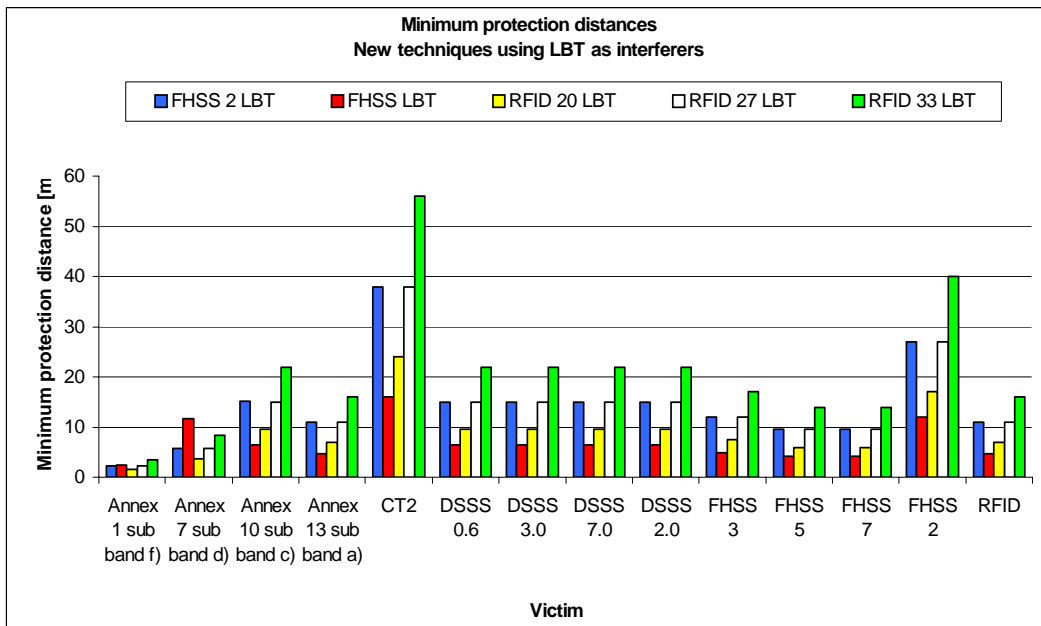
Figure 6.4.7: Minimum protection distances New techniques using LBT (where possible) as interferers

7   FREQUENCY AND TIME TECHNIQUES TO ASSIST SPECTRUM SHARING

7.1   Introduction

The SEAMCAT and the MCL studies model the interference levels to be expected between different equipments in randomized circumstances.   The underlying assumption is that both interferer and victim are operating independently. Neither study has the mechanism to take proper account of the effect of systems that actively

attempt to avoid each other. For instance, FHSS is modelled on the basis of the probability that a given unit will be using a given frequency at a particular time. Similarly, the effect of a low duty cycle is modelled as a probability that the transmitter is on at a given time.

In practice, it is quite possible that users could arrange the frequency and/or the time of their operation in order to minimize interference to and from other users. The techniques of Listen Before Talk (LBT) and Adaptive Frequency Agility (AFA) are introduced in Section 4 above and discussed further in Annex J. It should be stressed that these techniques are neither particularly new nor difficult to implement.

This section discusses the effect that the use of these techniques will have in an SRD band with a number of simultaneous users. In order to optimize access to the spectrum, each user operates a strategy that consists of one or more techniques such as DSSS, FHSS, AFA, LBT, etc.

7.2   Effect of the different Strategies

A spreadsheet was used to calculate the effects on communication reliability for the various strategies against the number of users. Rather than a probability of interference, the results are expressed as a throughput. Throughput can be viewed either as the probability of successful transmission of a short packet or as the normalized data rate that can be achieved. Throughput is therefore a measure of how efficiently the spectrum is being used.

Figure 7.1 shows the calculated throughput versus number of users for each strategy examined.

The following general assumptions are made:
- The users are clustered at a hotspot and all in range of each other. Wanted and unwanted signals at each receiver do not differ greatly in magnitude.
- Each user wishes to send data in a nominal 100 kHz sub-band at 100% duty cycle.
- The frequency band available is 7 MHz wide.
- All users operate the same strategy.
- Some strategies result in unequal throughputs for different users. The throughput plotted is the result for the Nth user. Ie., if N-1 users are already present, this is the expected throughput experienced by a new arrival.
- Small overhead allowances have been made for the time spent changing frequency or listening before transmitting.
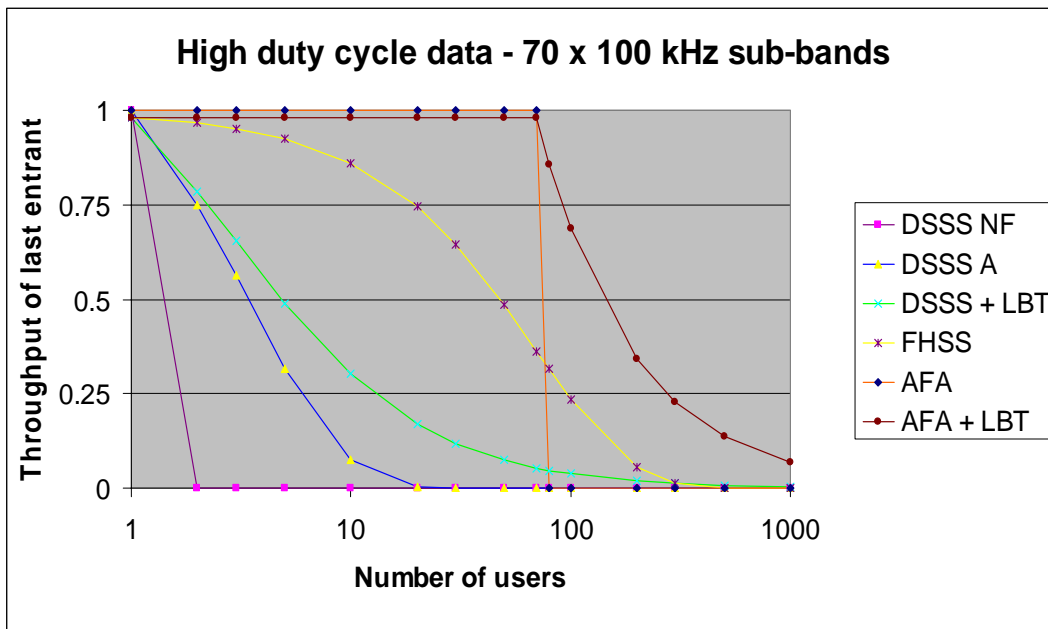

Figure 7.1: Effect of different sharing systems against number of users

7.2.1 Description of the Strategies

Three DSSS strategies are shown in Fig 7.1. With a spread to un-spread ratio of 70, the processing gain in a DSSS receiver is limited to approx. 17 dB. Therefore it can only cope with an unwanted signal that is less than approx 9 dB stronger than the wanted signal.

DSSS NF shows the use of DSSS where the near-far problem is significant - for instance if the positioning is such that the processing gain is never sufficient to separate the wanted and unwanted signals. This is a possibility with duplex systems. In this case, while one user may experience full throughput, the second experiences none.

DSSS A assumes a spread of incoming signal levels and that the processing gain is sufficient to reject the unwanted signal except in a proportion (in this example 25%) of cases.

DSSS + LBT is similar to DSSS A except that a level of adaptability is assumed. Where clashes occur between two or more users, they either use LBT to share access or reduce their data rate in order to increase the processing gain.

FHSS shows a frequency hopping system that hops over 70 frequencies in a pseudo random sequence.

AFA is an Adaptive Frequency Agile system capable of seeking out a clear sub-band. When such a sub-band is found the system occupies it until no longer needed. In this case, 70 users can be accommodated without problem, but the 71st receives no service.

AFA + LBT is similar to F Agile but with a further level of adaptability. Where there is potential contention over a sub-band, LBT is used to time divide access. Up to 70 users, there is full throughput apart from a small overhead. Where there are more than 70 users, each receives a proportionate reduction in throughput.

7.2.2 Spreadsheet calculations

The formulae used in calculating the curves in Figure 7.1 are:

DSSS-NF and DSSS-A

Throughput T is calculated as the probability of receiving a signal without interference.

$$T = (1 - P_{SI})^{N-1}$$

Where P_{SI} = Probability that a given interfering signal is too strong to be removed by the processing gain. N is the number of users.

For DSSS-NF $P_{SI} = 1$, For DSSS-A $P_{SI} = 0.25$

DSSS-LBT

The available capacity is shared evenly between the subset of users who are interfering with each other.

$$T = \frac{OHF}{(N-1)P_{SI} + 1}$$

Where OHF is the overhead factor for operating a LBT protocol. In this case $P_{SI} = 0.25$ and $OHF = 0.98$.

FHSS

The proportion of the time available to each user depends on the number of other users.

$$T = FH(1 - 1/70)^{N-1}$$

Where FH is the overhead factor associated with changing frequency. In this case $FH = 0.98$.

AFA

For the first 70 users, $T = 1$, otherwise $T = 0$

AFA + LBT

For the first 70 users, $T = OHF$,

For $N > 70$ the time and frequency resources are shared evenly among the users

$$T = OHF\left(\frac{70}{N}\right)$$

In this example, $OHF = 0.98$.

7.3 Discussion

Not shown in Figure 7.1 is the random access case, in which each user selects a frequency and time without reference to any other users. On average this would have the same effect as being on a fixed frequency and transmitting when required, similar to the operation of many existing SRDs. A plot of the average throughput for this strategy would follow the same curve as for FHSS. This is the average, or expected, throughput and hides the fact that different users will experience very different levels of service. FHSS, however, serves to randomize time and frequency access further; the average throughput is much the same, but the difference is that each user receives the average service rather than some receiving all and some none.

The FHSS curve therefore represents a benchmark. It is the average level of throughput that would be achieved if no coherent strategy were adopted.

One conceivable strategy that is not shown is that of adaptive FHSS. In this a frequency hopping system would omit frequencies on which it detected interference. At first glance this appears an attractive addition to FHSS. In the case of one FHSS system in a population of fixed frequency users it yields obvious advantages. If, however, there are multiple FHSS users each trying to adapt to the others then each will gradually reduce its hopping to its own set of exclusive sub-bands. In the limiting case, there would be 70 users, none of which were hopping. An interesting result then is that there is no service available for the 71st user; for him adaptive FHSS is worse than non adaptive. Adaptive FHSS therefore is virtually the same as Adaptive Frequency Agile, both in how it behaves and in the results achieved.

The relatively poor showing of DSSS is due to the limited processing gain that is available compared to the dynamic range of unwanted signals. In this study it performs significantly worse than the FHSS benchmark curve. In other circumstances, where the variation in incoming signal strengths can be controlled, DSSS can perform better than this benchmark. Such circumstances, however, do not pertain in an SRD band.

7.4 Mixed Equipment

An attempt has not been made to calculate the effect of different users pursuing different strategies. The assumption made is that all users would adopt the same strategy, either because they each independently decided it was the best or because regulations forced them to. The effect of some users operating a strategy and some not (e.g., on fixed frequencies) should, however, be considered as this may arise during the introduction of a new technique. In the SEAMCAT and MCL studies the probability of interference caused by DSSS and FHSS has been analyzed.

AFA devices will seek to avoid frequencies used by conventional fixed frequency devices and LBT devices will time their transmissions to avoid them. In general therefore, AFA and LBT are friendly towards conventional users, up to and even beyond the point of complete band congestion.

7.5 LBT and Duty Cycle Limits

Where there is contention between users in a given sub-band, sharing must occur by dividing access in the time domain. A simple way of doing this is to impose duty cycle limits on each user. With very low limits (e.g., 0.1%) there is little probability of clashes between users and this is a useful technique for one way links. At higher limits, however, duty cycle limits alone do not provide an efficient means of sharing. For instance, consider two users each limited to 10% duty cycle. If they both operate one way links they will experience an unacceptable level of mutual interference. They cannot usefully share the frequency unless one or both change to half duplex and use LBT. But if both use LBT, then the duty cycle limit is not necessary. In this example, the effect of the 10% duty cycle limit is

to reduce the potential throughput of each user by a factor of ten while adding little benefit in the form of sharing. A more efficient use of the air time is obtained if each user operates LBT and the duty cycle limit is replaced with a maximum transmission time limit. An example of how this might operate in practice is given in Annex J.

Similarly, it can be shown that a 1% duty cycle limit does not allow useful sharing between three or more users unless LBT is used and therefore does not result in efficient use of the air time.

The 0.1% duty cycle limit, while not resulting in efficient use of air time, does, however, permit access by low cost one way equipment and its use could be justified on these grounds.

One particular effect of imposing low duty cycle limits in specific sub-bands should be noted. Manufacturers will, as intended, design equipment to exploit the allocation. The result is a body of installed equipment that is reliant on very low levels of co-channel interference.

7.6   Summary of frequency and time techniques to assist spectrum sharing

With the scenarios under consideration in this section the best results are obtained with a combination of Listen Before Talk and Adaptive Frequency Agility. For any number of users in the band, this strategy results in the best average throughput. It also acts to share the resources equitably between the competing users; as the band gets more congested, each user experiences gradual degradation rather than sudden loss of service.

Another feature of this strategy is that it is not harmful to other systems not using a similar strategy.

7.7   Operation by RFID in the band 865 – 868 MHz

The characteristics of RFID make them unsuited to the above spectrum sharing techniques. This is because of the wide difference in power levels between SRDs and RFID. Consequently SRDs transmitting at low power levels, which are within the protection distance of an interrogator, cannot be detected by the LBT receiver in the interrogator. Instead spectrum sharing is achieved by operating RFID in the dense interrogator mode with high power transmissions restricted to four of the 15 available channels. The remaining eleven channels are reserved for the low level responses from the tags. This is further described in Annex D.5, Section D.5.1.

This approach is highly spectrum efficient since it enables multiple interrogators to operate on the same channel in the same geographic space.

8   CONCLUSIONS

This report considers the impact of introducing new techniques in the band 863 to 870 MHz in accordance with the CEPT Strategic Plan 862 – 870 MHz. The results show that the probability of interference caused by the new techniques against existing applications is no greater than between existing applications. Receiver parameters of existing ETSI standards were used in this study.

The results from SEAMCAT simulations for existing Short Range Devices show that most of the probabilities of interference are well below 1%, with the exception of Social Alarms (4.5 %), Wireless Audio Applications (1 %, 5.2 % and 11 % depending on sub-band) and Radio Microphones (6.8 % and 7 % depending on sub-band).

The new techniques include DSSS and FHSS. This report also considers the "listen before each transmit" feature. The probability of interference caused by these new techniques has been analysed using SEAMCAT simulations and MCL calculations.

Based on the results presented in section 6, the following conclusions were reached:

1.   New applications for non specific SRDs within this band shall use "listen before each transmit" if their Duty Cycles are higher than the limits shown in table 8.1 below. The values of all other parameters shall not exceed the limits in table 8.1.

Traditional Duty Cycle restrictions are unnecessary for equipment using "listen before each transmit", provided the minimum transmit-off time and maximum transmit-on time are defined. This needs to be implemented within ETSI standards as a mandatory requirement.

2.   Based on the advantages demonstrated in the analysis of LBT in section 7, it is recommended that administrations should encourage a migration by non specific SRDs towards its use. The "listen before each transmit" feature can be applied to most existing SRDs as covered by ERC/REC 70-03. However "Listen before each transmit" may be inappropriate for one-way systems, e.g. social alarms

3.   It should be noted that either duty cycle or LBT with AFA is a mandatory requirement for non specific SRDs. This offers the following options to industry:
- For SRDs without LBT or those with LBT but without AFA the duty cycle limit as defined in the table 8.1 shall not be exceeded.
- For equipment with LBT and AFA, the traditional duty cycle restriction is not required. The net result in the event of high traffic, is a dynamic duty cycle limitation which is dependent on the loading of the channel.

4.   The probability of interference caused by the new techniques to existing short range devices is considered acceptable. However, it should be noted that the results for the new techniques in Section 6 were simulated/calculated without taking into account the "listen before each transmit" feature.

5.   Special consideration was given to the needs of Social Alarms. The study shows that the probability of interference caused by existing systems is 4.5% while for new systems it is less. Nevertheless, one manufacturer of these systems has declared that the only acceptable figure is one where the probability of interference is effectively zero.

6.   Operation of RFID in accordance with the four channel plan described in Annex D.5 provides significant benefits to end-users and improves co-existence with SRDs using LBT and AFA. For the nearby SRDs without LBT and AFA that are co-channel with an RFID interrogator, the probability of interference will be increased. The probability will exceed the figures in Table A.1.2 for RFID 33 @ D.C. of 30%. (See also ETSI TR 102 649-1 [29]). This may make the operation of such SRDs impracticable in the four high power channels.

A summary of the recommended limits for satisfactory operation of the different technologies within the band is provided in Table 8.1 below.

Application	Regulatory parameters	Comments
Non-specific SRD using DSSS	**sub band 865 – 868 MHz** - max radiated power = 25 mW e.r.p. - occupied bandwidth = 0.6 MHz - max power density = 6.2 dBm/100 kHz - max duty cycle = 1 % **sub band 865 – 870 MHz** - max radiated power = 25 mW e.r.p. - occupied bandwidth = 3 MHz - max power density = -0.8 dBm/100 kHz - max duty cycle = 0.1 % **sub band 863 – 870 MHz** - max radiated power = 25 mW e.r.p. - occupied bandwidth = 7 MHz - max power density = -4.5 dBm/100 kHz - max duty cycle = 0.1 %	Implementation of LBT is not considered possible for DSSS unless a narrow band receiver is used while in the listen mode. If LBT timing is used, the timing shall be determined within ETSI standards[1]: Examples for such values are: TX on-time= 500 ms TX off-time= 15 ms
Non-specific SRD using FHSS	**sub band 865 – 868 MHz** - max radiated power = 25 mW e.r.p. - channel bandwidth = 50 kHz - number of hop channels = 60 [2] - max duty cycle = 1 % or LBT [1] **sub band 865 – 870 MHz** - max radiated power = 25 mW e.r.p. - channel bandwidth = 100 kHz - number of hop channels = 50 [2]	If LBT timing is used, the timing shall be determined within ETSI standards[1]: Examples for such values are: TX on-time= 500 ms TX off-time= 15 ms

	- max duty cycle = 0.1 % or LBT [1] **sub band 863 – 870 MHz** - max radiated power = 25 mW e.r.p. - channel bandwidth = 100 kHz - number of hop channels = 70 [2] - max duty cycle = 0.1 % or LBT [1]	
Non-specific SRD using other digital modulations [3]	**sub band 865 – 868 MHz** - max radiated power = 10 mW e.r.p. -200 kHz < occupied bandwidth < 3 MHz - max duty cycle = 1 % or LBT [1] **sub band 865.5 – 867.5 MHz** - max radiated power 25 mW e.r.p. - 50 kHz < occupied bandwidth < 200 kHz - max duty cycle = 0.1% or LBT [1]	If LBT timing is used, the timing shall be determined within ETSI standards[1]: Examples for such values are: TX on-time= 500 ms TX off-time= 15 ms
System for stolen cars using DSSS 4)	**sub band 865.5 – 867.5 MHz** - max radiated power = 2 W e.r.p. - occupied bandwidth = 2 MHz - max power density = 20 dBm/100 kHz - max duty cycle = 0.03 %	Effective implementation of LBT is not considered possible for DSSS. If LBT timing is used, the timing shall be determined within ETSI standards[1]: Examples for such values are: TX on-time= 500 ms TX off-time= 15 ms
System for tracking containers using FHSS	**sub band 865 – 868 MHz** - max radiated power = 500 mW e.r.p. - channel bandwidth = 25 kHz - min number of hop channels = 7 [2] - max duty cycle = 0.03 % or LBT [1]	If LBT timing is used, the timing shall be determined within ETSI standards[1]: Examples for such values are: TX on-time= 500 ms TX off-time= 15 ms
Generic RFID 5)	**sub band 865 – 868 MHz** - max radiated power = 20 μW e.r.p. except at **center frequencies of 865.7, 866.3, 866.9 and 867.5 MHz where the following parameters shall apply:** - max radiated power = 2 W e.r.p. - channel bandwidth = 200 kHz - maximum period of continuous transmit on a channel = 4 s	RFID tags may respond on any channel within the sub band. Interrogators shall not be required to use LBT in the four high power channels.

Table 8.1: Implementations considered feasible

Notes:
1) LBT = "Listen Before each Transmit" with defined max. TX on-time and min. TX off-time.
   It requires mandatory receiver parameters for sensitivity, adjacent channel selectivity and blocking response.
   Traditional Duty Cycle restrictions are unnecessary for equipment using LBT.

2) This number of hop channels has been used in combination with the channel bandwidth for the calculation of the probability of frequency collision. A minimum number of hop channels shall be implemented in an ETSI Standard. If the minimum number of hop channels is significantly less than the numbers used in this study the probability of interference shall be verified.

3) The outcome of ETSI studies on requirements for SRDs in the UHF band was that users wanted greater data rates and higher powers. To make greater data rates possible a larger bandwidth is proposed for digital modulations techniques. It should be noted that, due to the limited spreading range, none of the spread spectrum technique are able to achieve high data rates . To restrict the spectral density to an acceptable level the output power shall be limited to 10 mW.

4) For the purpose of this study the proposed ETSI transmitter spectrum mask has been changed (see the comment below the Figure 1-4-3-2)

5) As described in Annex D.5 generic RFIDs are simulated using that frequency for the victim, which is either the adjacent channel to a high power channel if applicable, or the closest channel of the adjacent sub-band.

9   REFERENCES

[1]   **ERC/REP 68**
Monte Carlo Simulation Methodology for use in sharing and compatibility studies between

[2]   **SEAMCAT user manual** (www.seamcat.org)

[3]   **ERC/REP 101**
Minimum coupling loss method, enhanced minimum coupling loss method, and the Monte-Carlo simulation.

[4]   **ETSI TR 102 069**
Electromagnetic compatibility and Radio Spectrum Matters (ERM);
Technical Report on the operation of DSSS transponders in the band 865-868 MHz, with polling frequency external to the band

[5]   **ETSI TR 102 134**
Electromagnetic compatibility and Radio Spectrum Matters (ERM);
SRD equipment operating below 1 GHz; Systems Reference Document for introduction of systems for Asset Tracking using Frequency Hopping Spread Spectrum FHSS in the band 865-868 MHz

[6]   **ETSI TR 102 649-1**
Electromagnetic and radio spectrum matters; Technical characteristics for RFID in the UHF band; System Reference Document for Radio Frequency Identification (RFID) equipment Part 1: RFID equipment operating in the range from 865 MHz to 868 MHz

[7]   **ERC/REC 70-03**
ERC Recommendation 70-03 relating to the use of short range devices (SRD)

[8]   **ERC Report 25**
The European Table of Frequency Allocations and Utilisations covering the Frequency Range 9 kHz to 275 GHz.

[9]   **ERC/DEC(97)06**
ERC Decision of 30 June 1997 on the harmonized frequency band to be designated for Social Alarm Systems

[10]   **ERC/DEC(01)04**
ERC Decision of 12 March 2001 on harmonized frequencies, technical characteristics and exemption from individual licensing of Non-specific Short Range Devices operating in the frequency bands 868.0 - 868.6 MHz, 868.7 - 869.2 MHz, 869.4 - 869.65 MHz, 869.7 - 870.0 MHz

[11]   **ERC/DEC(01)09**
ERC Decision of 12 March 2001 on harmonized frequencies, technical characteristics and exemption from individual licensing of Short Range Devices used for Alarms operating in the frequency bands 868.60 - 868.7 MHz, 869.25 - 869.3 MHz, 869.65 - 869.7 MHz.

[12]   **ERC/DEC(01)18**
ERC Decision of 12 March 2001 on harmonized frequencies, technical characteristics and exemption from individual licensing of Short Range Devices used for Wireless Audio Applications operating in the frequency band 863 - 865 MHz.

[13]   **ECC/DEC (01)02**
         ECC Decision of 15 November 2001 on phasing out digital CT2 applications in the 900 MHz band.

[14]   **EN 300 220-1**
         Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW; Part 1: Technical characteristics and test methods.

[15]   **EN 300 220-2**
         Electromagnetic compatibility and Radio spectrum Matters (ERM);
         Short range devices; Technical characteristics and test methods for radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW;
         Part 2: Supplementary parameters not intended for regulatory purposes.

[16]   **i-ETS 300 131**
         Radio Equipment and Systems (RES);
         Common air interface specification to be used for the inter-working between cordless telephone apparatus in the frequency band 864.1 MHz to 868.1 MHz, including public access services.

[17]   **ERC/REP 88**
         Compatibility and sharing analysis between DVB-T–t and radio microphones in bands IV and V Naples, February 2000.

[18]   **ITU-R Recommendation BT.1368-3**
         Planning criteria for digital terrestrial television services in the VHF/UHF bands

[19]   European Passive RFID Market Sizing 2007 – 2022 February 2007 by LogicaCMG and GS1

[20]   **ECC Report 34**
         Compatibility between Narrowband digital PMR/PAMR and tactical radio relay in the 900 MHz band

[21]   **ITU-R P.1238-3**
         Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 900 MHz to 100 GHz.[22]**EN 301 357**
         Cordless audio devices in the range 25 MHz to 2 000 MHz; Consumer radio microphones and in-ear monitoring systems operating in the CEPT harmonized band 863 MHz to 865 MHz;
         Part 1: Technical characteristics and test methods.

[23]   **TR 100 220**
         Radio Equipment to be used in UHF-range System reference document for UHF RFID systems.

[24]   **ECC Report 109**
         Compatibility of Bluetooth with other existing and proposed radiocommunication systems in the 2.45 GHz frequency band

[25]   "Wireless Communications" by T. S. Rappaport, ISBN 0-13-375536-3, chapter 3.

[26]   **EN 302 208-1**
         Electromagnetic compatibility and Radio spectrum Matters (ERM);
         Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W;Part 1: Technical requirements and methods of measurement

ANNEX A   COMPLETE SEAMCAT SIMULATION RESULTS

Only relevant sections of the SEAMCAT results have been included within the main body of the report. However for completeness it was decided to include in this Annex the results of all SEAMCAT simulations performed as part of this study.

A.1   Interference between existing systems and planned systems

A.1.1   Probability of interference from existing systems to planned systems

Victim	Interferer Probability in %						
	Non-specific SRD Rec 70-03 Annex 1 sub band h	Alarms Rec 70-03 Annex 7 sub band c	Radio microphones Rec 70-03 Annex 10	Wireless Audio Applications Rec 70-03 Annex 13 sub band aBW=600 kHz	CT2	DVB-T 100 kW e.r.p.	DVB-T 10 kW e.r.p.
DSSS 0.6	0.9	0.2	0.2	0.3	0	8.6	1.9
DSSS 3.0	3.3	0.2	0.6	1.4	0.7 [a)]	11.2	2.7
DSSS 3.0 co-channel	55.6	4.7	19.3	45.6	58.5 [b)]	-	
DSSS 7.0	5.3	1.5	29.3	89.7	14.5	13.3	3.4
DSSS 2.0 [c]	0.1	-	0	0.1	0	2.9	0.6
FHSS 3	-	-	-	-	12.3	0.5	< 0.1
FHSS 3 non overlapped	0.2				0.1	-	-
FHSS 5	41.5	45.9	-	-	11.5	0.5	-
FHSS 5 non overlapped	-	-	13.1	52.1	-	-	-
FHSS 7 [d]						-	-
FHSS 2 [e]	9.0	7.6	24.9	29.2	7.1	5.3	1.2
RFID 20,27,33 [f]	0.3	<0.1	0	0.8	0.6	20.7	4.1

Table A.1.1: Probability of interference from existing systems to planned systems

Notes:
- simulation not performed

a   an adjacent band scenario is simulated by setting the interferer frequency to 866.1 MHz and the victim frequency to 867.5 MHz

b   the victim frequency has been set to 866.5 MHz

c   Special application according to ETSI TR 102 069 [4] for car anti-theft. For the purpose of the SEAMCAT simulations a transmitter mask according to the definition within section 4.4 is used instead of the filter mask described in the called reference

d   since the probability of interference for FHSS 7 is less than for FHSS 5 (the same receiver bandwidth) these scenarios are not simulated

e   Special application according to ETSI TR 102 134 [5] for tracking of containers

f   Since the receiver characteristics of the different RFIDs are the same and the input power of the wanted signal is set to a constant value of −72 dBm, the simulated results are valid for all types of RFID. To simulate the blocking response of −30 dBm SEAMCAT has to use the "sensitivity mode" as "Blocking attenuation mode". In order to simulate the worst case, an omni directional antenna of 0 dB gain is assumed.

Additional information:

1 For the purpose of this study the blocking response of the DSSS receiver is set to constant –35 dBm., The interference criterion is C / (N+ I) = -17 dB equal to the processing gain. To simulate the blocking response of –35 dBm, SEAMCAT has to use the "sensitivity mode" as the "Blocking attenuation mode".

2 Three scenarios are considered in order to simulate fully the operation of DSSS 3.0. These are:-
   a) Centre frequency of 866.5 MHz to cover the centre of the range
   b) Centre frequency of 864.5 MHz to cover the lower part of the band.
   c) Centre frequency of 868.5 MHz to cover the upper part of the band.

3 The term co-channel shown in the table refers to scenarios b and c.

4 For the purpose of this study the existing applications in all annexes of the ERC/REC 70-03 [9] are simulated simultaneously, except where FHSS is the victim. In that case each application is simulated separately and the worst case is noted.

A.1.2   Probability of interference from planned systems to existing systems

Interferer /Duty Cycle	Victim Probability in %					
	Non-specific SRD Rec 70-03 Annex 1 sub band f	Alarms Rec 70-03 Annex 7 sub band d	Radio microphones Rec 70-03 Annex 10 sub band c	Wireless Audio Applications Rec 70-03 Annex 13 sub band a BW=600 kHz	CT2[d]	DVB-T receivers at sensitivity −79.5 dBm
DSSS 0.6 100%	0.1	0.2	0	1.2	13.5	-
10%	-	-	-	-	1.9	-
1%	-	-	-	-	0.2	1.2
DSSS 3.0 cc 10% [a]	-	-		-	-	
1% [a]	-	-	-	-	-	-
0.1%	2.3	5.8	7.5	10.8	-	0.1
DSSS 3.0 ac	1.9	10.4	2.2	4.3	14.3	-
10%	-	0.8	-	-	2.1	-
1%	0.1	0.2	-	-	0.2	-
0.1%	-	-	-	-	-	0.1
DSSS 7.0 10%	43.9	100	-	95.9	-	-
1%	8.5	36.4	42.4	43.2	10.4	-
0.1%	1.1	3.6	5.0	5.1	1.4	0.1
DSSS 7.0 10 dBm 0.1%	0.8	2.3	3.0	3.2	1.3	-
DSSS 2.0 100%	0.8	8.0	2.2	7.7	56.9	-
10%	0.1	0.7	0.1	0.5	13.3	-
1%	-	-	-	-	1.6	-
0.03%	0	0	-	-	0.1	0.4
FHSS 3 100%	1.3	6.5	9.7	8.8	14.3	
FHSS 3 10%	-	0.6	0.4	1.3	2.1	
1%	-	-	-	-	-	1.1
0.1%	-	-	-	-	-	-
FHSS 5 10%	27.2	92.9	0.5	1.9	1.9	-
FHSS 5 1%	4.6	12.1	-	-	-	-
0.1%	0.5	1.1	-	-	-	0.1

FHSS 7 10%	-	-	76.3	87.7	50.2	-
FHSS 7 1%	-	-	18.1	26.4	11.5	-
0.1%	-	-	1.6	1.9	1.4	0.1
FHSS 2 [b] 10%	12.7	64.6	59,9	58.0	45.3	-
1%	1.7	7.6	8.2	9.1	9.5	-
0.1%	0.2	0.8	0.7	1.2	1.2	-
0.03%	0	0.3	-	0.6	0.01	1.8

Interferer /Duty cycle	Victim Probability in %					
	Non-specific Short Range Devices Rec 70-03 Annex 1 sub band f	Alarms Rec 70-03 Annex 7 sub band d	Radio microphones Rec 70-03 Annex 10 sub band c	Wireless Audio Applications Rec 70-03 Annex 13 sub band a BW=600 kHz	CT2[d]	DVB-T receivers at sensitivity -79.5 dBm
RFID 20 100%	1.3	1.4	9.6	18.5	8.6	-
30%	0.5	0.5	3.1	7.7	2.9	-
10%	0.1	0.1	1.2	2.8	0.9	-
1%	-	-	-	-	-	-
0.1%	-	-	-	-	-	0.2
RFID 27 100%	3.0	6.8	18.6	31.	16.3	-
30%	1.0	1.8	7.1	14.7	5.8	-
10%	0.4	0.6	2.7	6.0	2.4	-
1%	<0.1	<0.1	-	0.7	0.2	-
0.1%	-	-	0	-	-	0.6
RFID 33 [c,)e] 100%	5.3	15.6	14.2	14.2	24.9	-
30%	2.0	4.7	5.5	6.3	9.6	-
10%	0.7	1.4	1.9	2.1	3.6	-
1%	<0.1	0.1	0.2	0.3	0.5	-
0.1%	-	-	-	-	-	1.1

Table A.1.2 : Probability of interference from planned systems to existing systems

Notes:

- not simulated

a Since the probability of interference is unacceptably high, the scenarios using more than 1 % duty cycle were not simulated

b For the purpose of the SEAMCAT simulations the unit density of interferer = 1000/sqkm with100 transmitters active was used.

c RFID 20 and RFID 27 were assumed to have an antenna gain of 4 dB whereas RFID 33 had an antenna gain of 6 dB. This leads to a situation where RFID 33 causes a lower probability of interference than RFID 27.

d Since CT2 uses listen before each transmit co-channel interference is not simulated except for DSSS 7.0 and FHSS 7.1

e) These probabilities of interference were achieved with unit densities three times higher than those predicted by industry.

f) aa is adjacent channel
cc is co-channel

A.2   Interference between planned systems

A.2.1   Interference from DSSS to planned systems

Victim	Interferer (f = 866.5 MHz) Probability in %											
	DSSS 0.6			DSSS 3.0			DSSS 7.0			DSSS 2.0		
	10	1	0.1	10	1	0.1	10	1	0.1	1	0.1	0.03
DSSS 0.6 ac	< 0.1	-	-	na	na	na	na	na	na	2.9	0.4	-
cc				6.6	0.8	-	4.7	0.6	-	6.0	0.8	-
DSSS 3.0 ac f = 864.5 MHz	< 0.1	-	-	6.2	0.8	-	7.1	0.9	-	4.4	0.5	-
	-	-	-	-	-	-	-	-	-	-	-	-
cc f = 866.5 MHz	9.9	1.2	0.2	9.9	1.2	0.2	7.1	0.8	-	7.4	0.9	0.3
DSSS 7.0	7.8	0.9	-	7.8	1.0	-	7.6	1.0	-	5.6	0.7	0.3
DSSS 2.0 cc	3.3	0.4	-	2.6	0.3	-	1.6	0.2	-	2.6	0.3	0.1
FHSS 3	29.1	5.3	0.7	55.9	14.7	2.0	53.4	13.6	1.8	44.7	11.7	4.2
FHSS 5	23.0	3.7	0.5	57.6	15.6	2.0	54.2	13.9	1.7	37.4	8.4	1.1
FHSS 7	ns	ns	ns	ns	ns	ns	54.2	13.9	1.7	ns	ns	ns
FHSS 2 ac	< 0.1	-	-	na	na	na	na	na	na	< 0.1	-	-
cc	68.1	18.4	2.3	88.2	46.6	8.2	86.9	44.4	7.9	86.1	41.4	17.8
RFID 20,27,33 [a] ac	< 0.1	-	-	na	na	na	na	na	na	22.4	2.1	0.7
cc	59.6	6.7	0.6	33.8	3.6	0.3	24.1	2.5	0.3	32.5	3.3	1.0

Table A.3.2 : Probability of interference from DSSS to planned systems

Notes:

-    not simulated

ns   since the probability of interference for FHSS 7 is less than for FHSS 5 (the same receiver bandwidth) these scenarios are not simulated

a   Since the receiver characteristics of the different RFIDs are the same and the input power of the wanted signal is set to a constant value of –72 dBm, the simulated results are valid for all types of RFID. To simulate the blocking response of –30 dBm SEAMCAT has to use the "sensitivity mode" as "Blocking attenuation mode". In order to simulate the worst case, an omni directional antenna of 0 dB gain is assumed.

A.2.2   Interference from FHSS to planned systems

Victim	Interferer Probability in %												
	FHSS 3			FHSS 5			FHSS 7			FHSS 2			
	10	1	0.1	10	1	0.1	10	1	0.1	10	1	0.1	0.03
DSSS 0.6	2.5	0.4	-	4.4	0.7	-	1.2	-	-	66.6	16.5	1.9	0.7
DSSS 3.0	8.4	1.0	-	5.4	0.6	-	6.4	0.8	-	82.9	29.3	3.7	1.1
DSSS 7.0	6.7	0.8	-	6.5	0.9	-	6.5	0.8	-	-	23.7	2.9	0.9
DSSS 2.0	1.8	0.2	-	1.1	-	-	0.9	-	-	45.4	10.4	1.2	0.4
FHSS 3	8.4	1.2	-	8.8	1.3	0.1	6.5	0.9	-	24.9	4.8	0.6	-
FHSS 5	9.0	1.1	-	9.3	1.1	-	7.1	0.9	-	27.0	5.1	0.7	-
FHSS 7	ns	ns	ns	ns	ns	ns	7.1	0.9	-	ns	ns	ns	ns
FHSS 2	29.7	4.4	0.6	28.4	4.1	0.5	22.6	3.0	0.3	63.6	17.1	1.7	0.6
RFID 20,27,33 [a]	6.2	0.7	-	3.7	0.4	-	2.7	0.3	-	28.2	2.6	0.3	-

Table A.2.2: Probability of interference from FHSS to planned systems

Notes:

- not simulated

ns since the probability of interference for FHSS 7 is less than for FHSS 5 (the same receiver bandwidth) these scenarios are not simulated

a   Since the receiver characteristics of the different RFIDs are the same and the input power of the wanted signal is set to a constant value of –72 dBm, the simulated results are valid for all types of RFID. To simulate the blocking response of –30 dBm SEAMCAT has to use the "sensitivity mode" as "Blocking attenuation mode". In order to simulate the worst case, an omni directional antenna of 0 dB gain is assumed.

A.2.3   Interference from RFID to planned systems

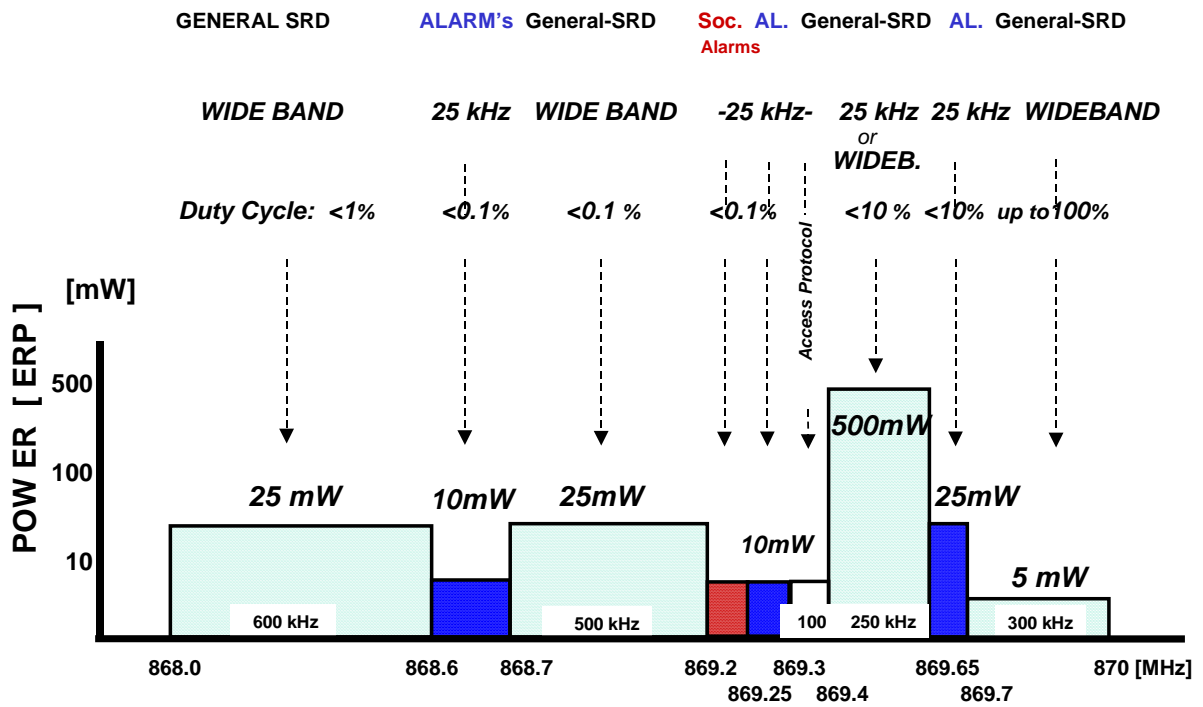| Victim	Interferer Probability in %								
	RFID 20			RFID 27			RFID 33		
	30	1	0.1	30	10	0.1	30	10	0.1
DSSS 0.6 [a]	0.1	-		-	-	-	-	-	-
DSSS 3.0 [b]	11.0	1.3	0	-	10.6	0.2	-	24.7	0.1
DSSS 7.0	8.6	1.3	0.1	-	10.2	0.1	-	26.0	0.1
DSSS 2.0 [b, c]	3.8	-	0.1		3.4	0.1	-	5.3	0.1
FHSS 3	22.5	1.5	0.01	-	19.8	0.2	-	27.3	5.7
FHSS 5	18.3	1.2	0.2	-	16.6	0.1	-	24.0	5.0
FHSS 7	14.9	1.1	ns	-	12.6	ns	-	19.4	3.8
FHSS 2 [d]	-	-	0.3	-		0.6	-	-	1.1
RFID 20,27,33 [e, b]	-	-	0.3	-		1.1	-	-	2.0

Table A.2.3: Probability of interference from RFID to planned systems

Notes:

- not simulated
   a   An adjacent channel scenario is simulated
   b   In order to simulate the worst case a co-channel scenario is assumed
   c   Special application according to ETSI TR 102 069 for car anti-theft [4].
      For the purposes of this study a transmitter mask according to the definition in section 5.4. is simulated
   d   Special application according to ETSI TR 102 134 for tracking of containers [5]
   e   Since the receiver characteristics of the different RFIDs are the same and the input power of the wanted signal is set to a constant value of –72 dBm, the simulated results are valid for all types of RFID. To simulate the blocking response of –30 dBm SEAMCAT has to use the "sensitivity mode" as "Blocking attenuation mode". In order to simulate the worst case, an omni directional antenna of 0 dB gain is assumed.
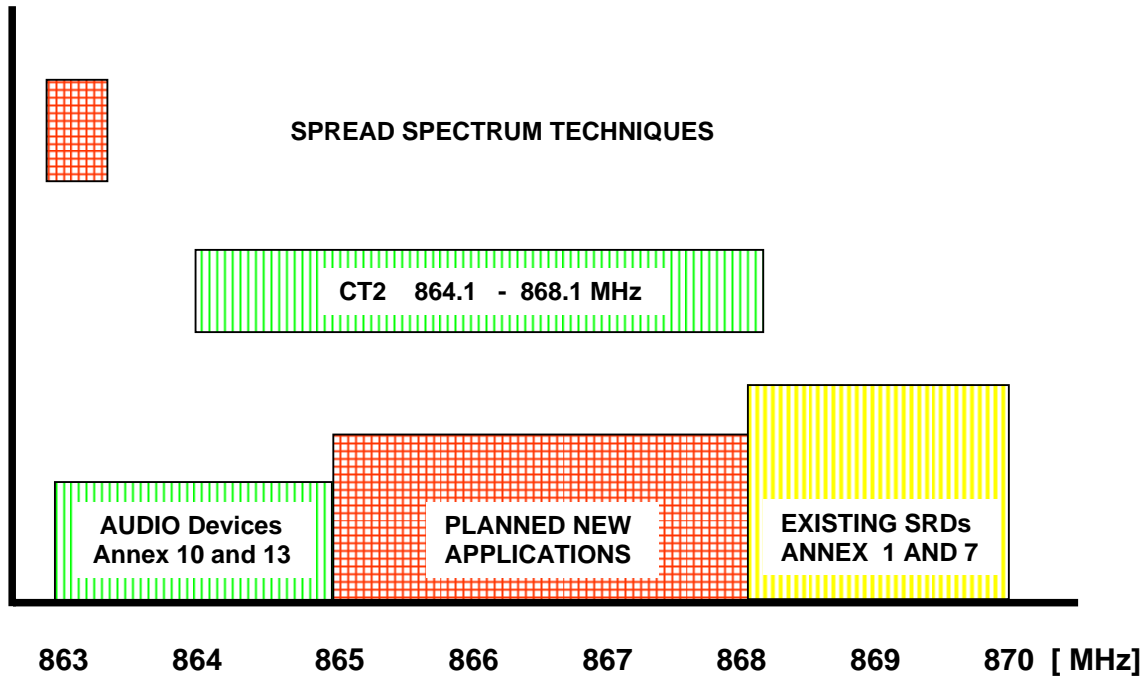
ANNEX B   EXISTING USE OF THE SUB BAND 868 – 870 MHZ

Existing use of the band 868-870 MHz (ERC REC 70-03)

| GENERAL SRD | | ALARM's | General-SRD | | Soc. AL. | AL. | General-SRD | | AL. | General-SRD |

GENERAL SRD   ALARM's General-SRD   Soc. AL. General-SRD AL. General-SRD
                                                          Alarms

WIDE BAND   25 kHz WIDE BAND   -25 kHz- 25 kHz 25 kHz WIDEBAND
                                                   or
                                                  WIDEB.

Duty Cycle: <1%   <0.1%   <0.1 %   <0.1%   <10 % <10% up to 100%

[mW]

POWER [ERP]

Access Protocol

500

100

10

25 mW   10mW   25mW   10mW   500mW   25mW

                                                                5 mW

600 kHz   500 kHz   100   250 kHz   300 kHz

868.0   868.6 868.7   869.2 869.3   869.65   870 [MHz]
                                 869.25 869.4   869.7

ANNEX C   STRATEGIC PLAN 863 – 870 MHZ

Strategic Plan   863 - 870 MHz   (ERC/REC 70-03)

SPREAD SPECTRUM TECHNIQUES

CT2   864.1 - 868.1 MHz

AUDIO Devices
Annex 10 and 13

PLANNED NEW
APPLICATIONS

EXISTING SRDs
ANNEX 1 AND 7

863   864   865   866   867   868   869   870 [MHz]

ANNEX D   SEAMCAT AND MCL

Background Information on SEAMCAT Simulations

ANNEX D.1   Differences between MCL and SEAMCAT

Explanation of the differences between the MCL method and the Monte-Carlo method

The most important characteristics of the MCL method are:
- the result generated gives isolation in dB, which may be converted into a physical separation if an appropriate path loss formula is chosen
- it is simple to use
- it is a worst case analysis
- the victim receiver is assumed to be operating 3 dB above reference sensitivity
- it considers only multiple interferers of a single type transmitting at a fixed (usually maximum) power.

Note:

The MCL method used in the present document (see Annex E) calculates the cumulative probability of interference.

The most important characteristics of the Monte Carlo method are:

- the result generated is a probability of interference
- it is a statistical technique, which requires the use of a computer
- it allows the user to model realistic scenarios and evaluate appropriate minimum frequency separations
- an appropriate path loss model is required
- the victim receiver has a variable wanted signal strength
- multiple interferers using multiple channels may be considered
- the effect of features such as power control may be included.

The main points to be considered are:

- the MCL approach is relatively straight forward. The modeling in this study uses multiple interferers of a single type. It provides a result, which although spectrally inefficient, guards against the worst case scenario.
- the Monte Carlo approach is a statistical technique, which models a victim receiver amongst a population of interferers. It is capable of modeling highly complex systems including CDMA. The result is spectrally efficient but requires careful interpretation.

ANNEX D.2   Method to calculate the minimum protection distance

(derived from the SEAMCAT results)

Usually the result of a SEAMCAT simulation is presented as a probability of interference.

However the possibility also exists to see randomly generated interferer signals:

-      as the distribution density (Figure D.2.1)
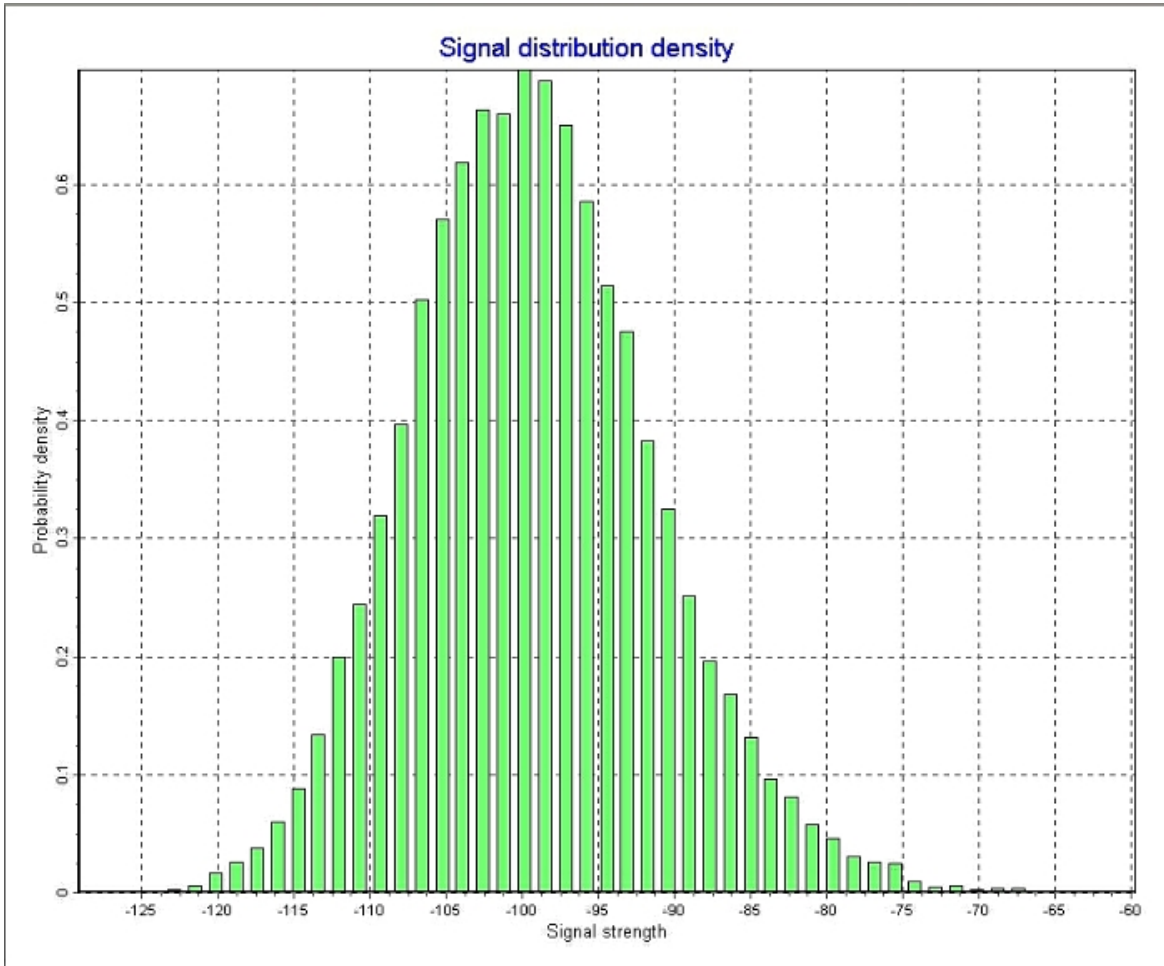
-      as the cumulative density (Figure D.2.2)

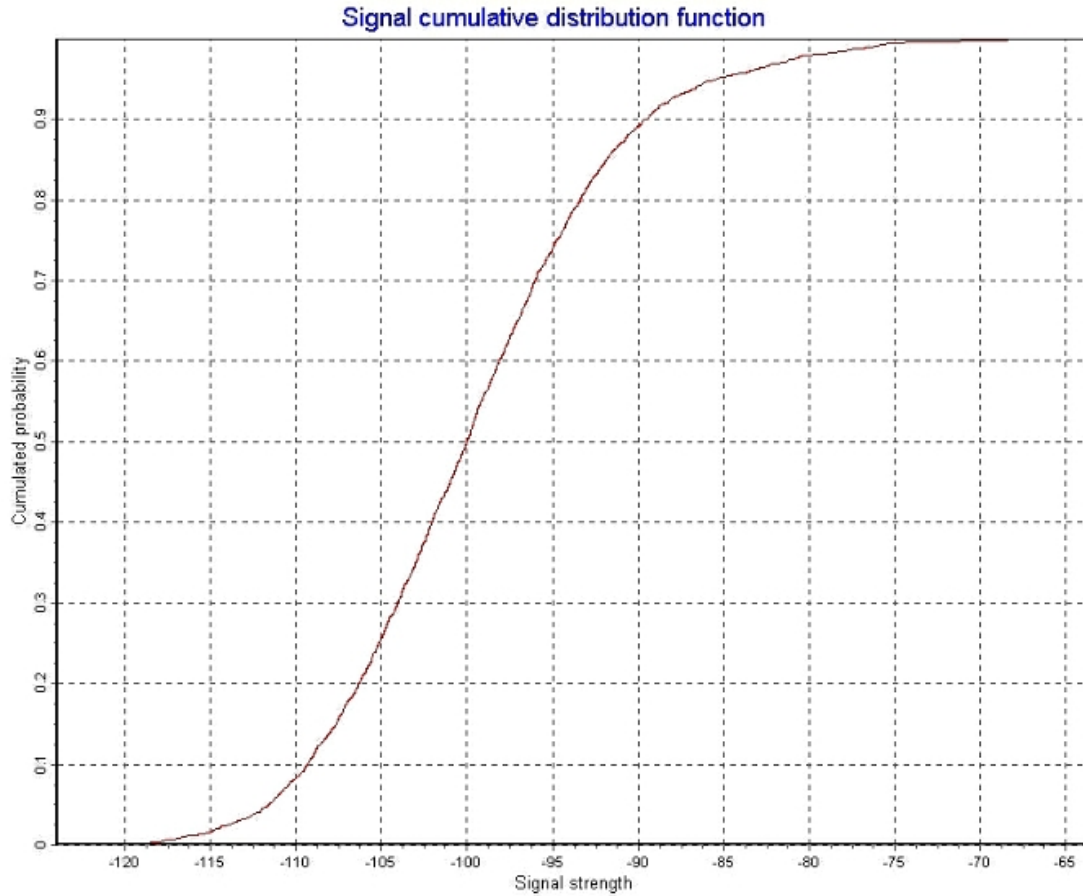**Figure D.2.1: distribution density**

Figure D.2.2: cumulative density

In this example the highest interference level is about –67 dBm, the lowest –123 dBm.

To calculate the minimum protection distance you need only the ***highest*** level.

To calculate the minimum protection distance perform the following steps:

1. Subtract the sensitivity (dBm) of the victim (e. g. –107 dBm –(-67 dBm))

2. The absolute value of this calculation is the minimum coupling loss: MCL (here: 40 dB)

3. Calculate the protection distance (d_prot) using the formula for free space path loss

$$d\_prot := 10^{\frac{MCL - 32.44 - 20 \cdot \log(f)}{20}}$$ (km)   (in this example: 0.003 km)

It is also possible to use the red line of the graph in the Figure D.2.3 below.
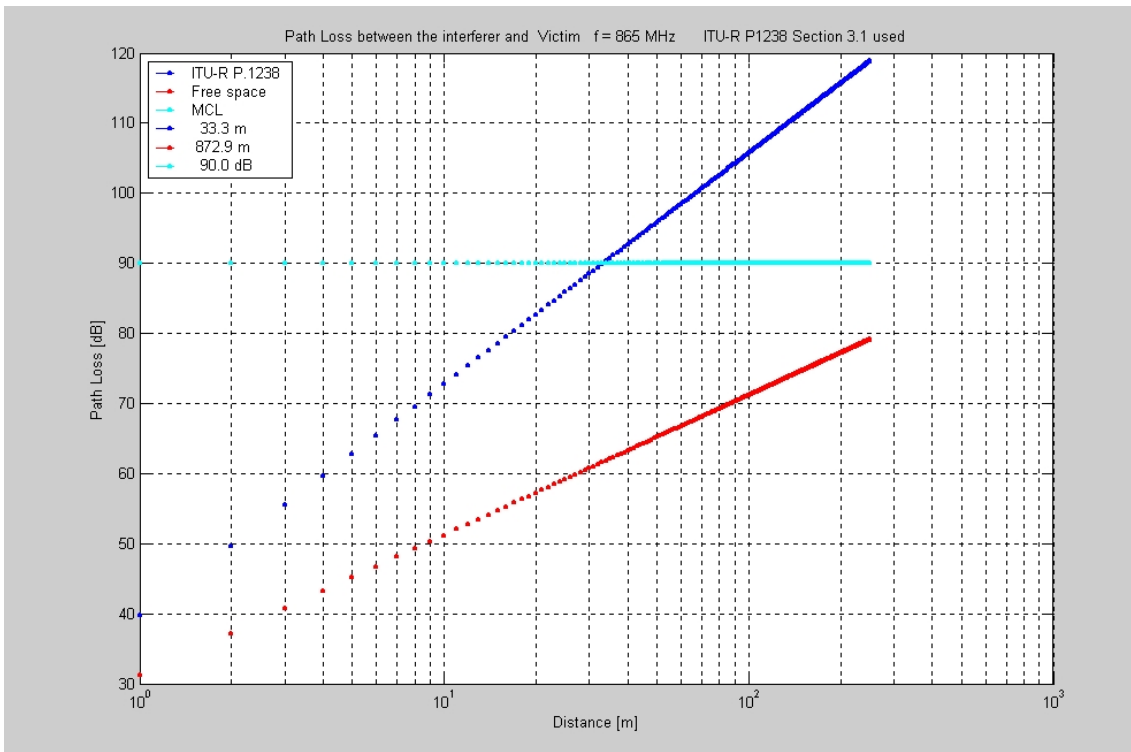
Note: The legend and the MCL-line (cyan) can be ignored.

Figure D.2.3: Path loss according to the ITU-R P.1238 [21]
indoor: blue line
free space: red line

ANNEX D.3   Filter masks

Filter masks defined by the applicable standards and used within the SEAMCAT simulation.

D.3.1   General

For the purpose of this study the following assumptions have been made:

1.   Where harmonised standards for different applications are defined by the ERC/REC 70-03, these standards
        have been used.
2.   In cases where no standards are defined, EN 300 220 is used as far as applicable.
3.   All equipment are defined as class 1 equipment in terms of the EN 300 220-1 [14]
4.   Although EN 300 220 part 2 [15] defines "*Supplementary parameters not intended for regulatory purposes*"
        the applicable parameters and their limits have been used.

Note:
        Without the above assumptions it is not possible to demonstrate co-existence between the different
        applications. This applies both for present and for new applications.

D.3.2   Transmitter

D.3.2.1 Explanation of the differences between the used transmitter filter masks

        The relevant standards (e. g. EN 300 220-1 [14]) define a filter for the measurement of the adjacent channel
        power to be used by the measurement receiver. (e. g. a spectrum analyser)- see Figure D.3.1below.
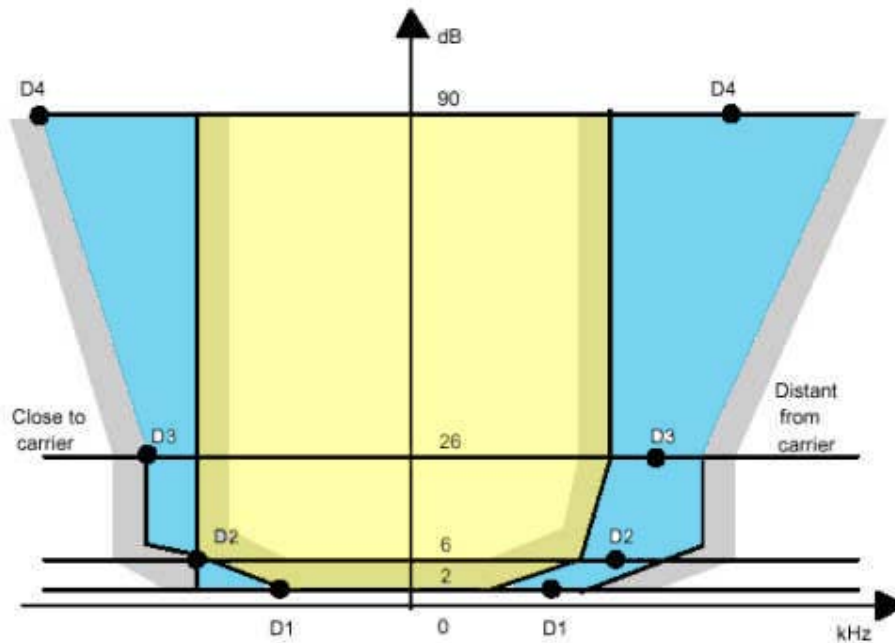
Note:

The yellow marked range shows a theoretical (ideal) filter to measure the adjacent channel power, set to the centre
frequency of the adjacent channel.

The tolerance range of the filter is marked blue.

Figure D.3.1: Selectivity characteristic of the IF-filter (graph)

The frequency points D1 to D4 depend on the channel spacing, see Table D.3.1 below.

Channel separation (kHz)	Frequency separation of filter curve from nominal centre frequency of adjacent channel (kHz)			
	D1	D2	D3	D4
10/12,5	3,0	4,25	5,5	9,5
20	4,0	7,0	8,25	12,25
25	5,0	8,0	9,25	13,25

Table D.3.1: Selectivity characteristic of the IF-filter (values)

The limits defined in the standard are only valid when the method of measurement described within the standard is used. The applicable filters must therefore be taken into account when calculating and simulating respectively the probability of interference.
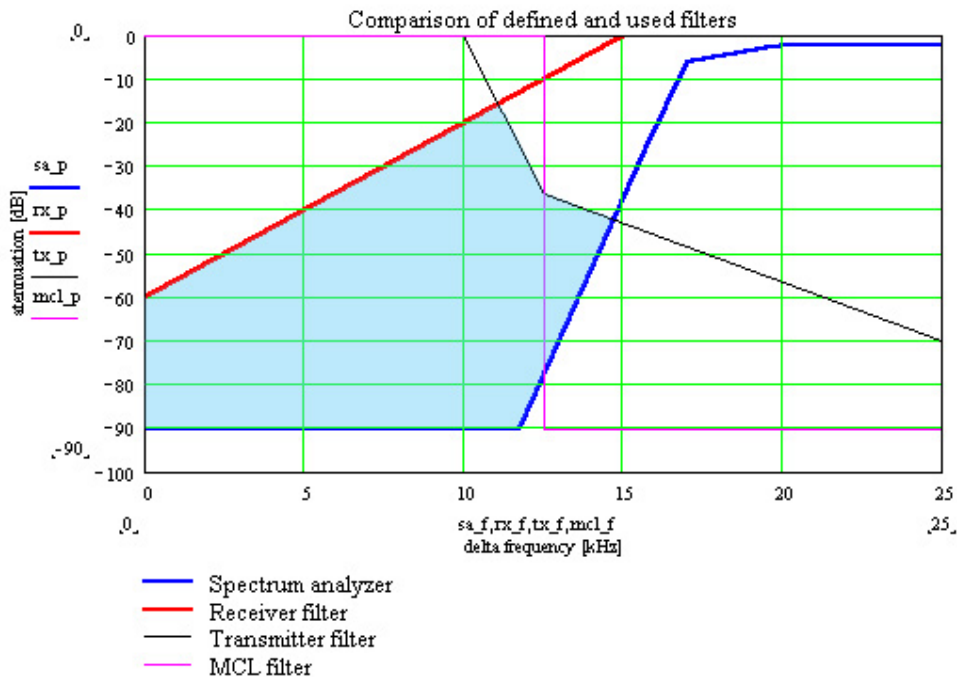
Figure D.3.2: Filter masks (according to EN 300 220, 25 kHz channel spacing)

Note: The values of the attenuation are not absolute values. The masks are made as if the receiver input would be directly connected to the transmitter output which transmits a power of 0 dBm. This figure only shows the difference between the filter defined for the measurement equipment and the simulated receiver input filter. The marked area shows that part of unwanted emissions where the victim is receiving more signal than defined by the standard.

D.3.2.2   Interpretation of the curves

D.3.2.2.1   General

The current standard EN 300 220-1 [14] defines a limit of –37 dBm for adjacent channel selectivity if the sub-band is channelised and a limit of –36 dBm at the edges of the sub-band for non-channelised sub-bands.
Since the revised version of EN 300 220-1 [14] is expected to define a single value of –36 dBm, this figure has been used throughout the study.

D.3.2.2.2   Transmitter (MCL)

The MCL calculation simulates a rectangular transmitter mask equal to the defined bandwidth. In this case the IF-filter of the spectrum analyzer is not needed because the attenuation of the MCL filter is nearly equal to the measurement filter. For example the difference between 11.85 kHz and 12.5 kHz is negligible.

D.3.2.2.3   Transmitter (SEAMCAT)

Within the SEAMCAT simulation a transmitter filter mask with a modulation bandwidth of 80% (zero dB bandwidth) of the channel spacing is used. The output power falls to –36 dBm at the edges of the channel or the sub-band respectively. From there the unwanted output power decreases to -70 dBm at a frequency equal to the defined bandwidth.

D.3.2.2.4   Conclusion

In principle the IF-filter of the spectrum analyzer should be taken into account in order to use the applicable limits for calculation of the probability of interference. However to simplify the simulation SEAMCAT does not use this additional filter.
Since this additional filter would decrease the simulated power of unwanted emissions within the adjacent channel or the adjacent band, the worst case is simulated. This range is colored blue.

D.3.3 **Receiver**

D.3.3.1 **EN 300 220**
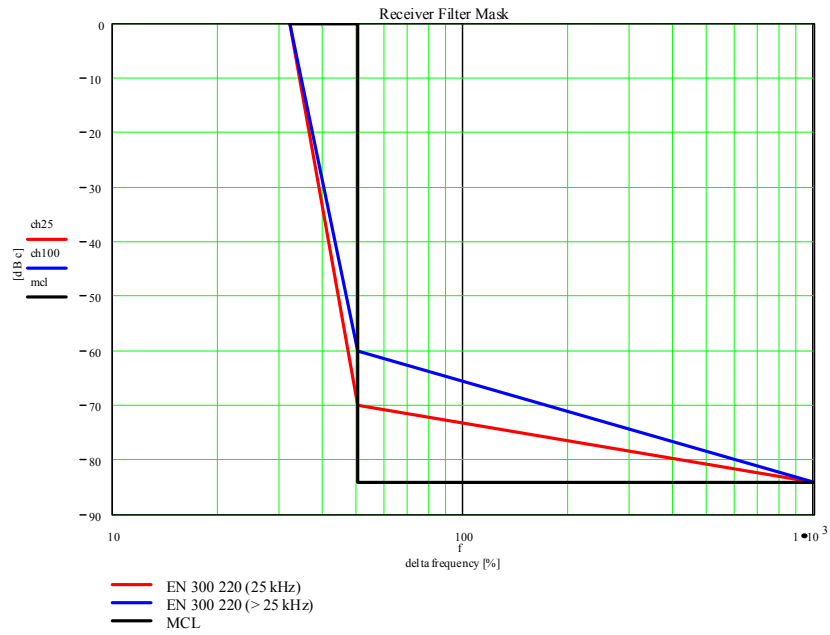
Note: *This figure shows the filter characteristic of a 100 kHz receiver. The filter masks for receiver using other bandwidths are proportionally defined.*

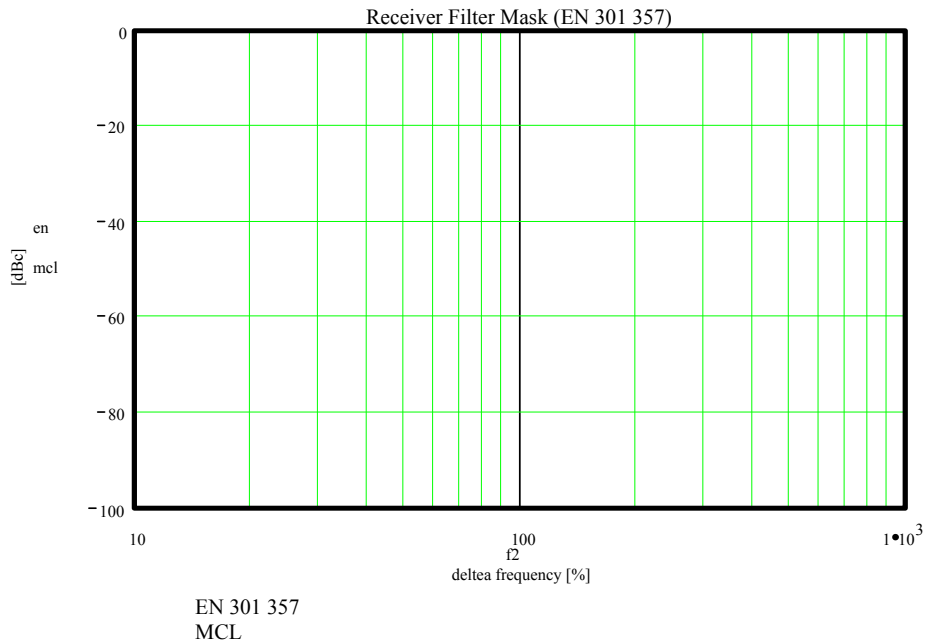**Figure D.3.3: Receiver filter masks according to the EN 300 220 [15]**

D.3.3.2 **EN 301 357**

EN 301 357
MCL

Figure D.3.4: Receiver filter masks according to the EN 301 357 [22]

ANNEX D.4   Duty Cycles used within SEAMCAT

Explanation of the method used by SEAMCAT to simulate different duty cycles
For calculation of the probability of interference SEAMCAT simulates
- one victim which is operating in continuous receive mode during the simulation
- one or more kind(s) of interferer(s) which is (are) transmitting at a duty cycle of 100% throughout the simulation.

To simulate the effect of duty cycle SEAMCAT uses this formula:

$$R_{simu} = \sqrt{\frac{n^{active}}{\pi * dens_{it}^{active}}}$$

where

n^{active} number of active interferers in the simulation (n^{active} should be sufficiently large such that the $(n+1)^{th}$ interferer would contribute negligible additional interfering power).

$dens_{it}^{active}$ density of active transmitters : $dens_{it}^{active} = dens_{it} * p_{it}^{tx} * activity(time)$

p_{it}^{tx} probability of transmission (*Note: This value is set to the duty cycle of each interferer*)

$activity(time)$ normalized temporal activity variation as a function of the time of day (expressed in hours). The time value used for calculation is specified in parameter time. (*Note: For the purpose of this study this value is set to 1 (hour) for SRDs due to the definition of the duty cycle*

$time$ Time of the day (*Note: This value is always set to 24 (hours)*)

The interpretation of this simulation is that the lower the duty cycle of an application, the larger is the simulated interference radius. This implies that the mean value of the interfering signal decreases with reducing duty cycle due to the larger average distance between victim and interferer.
The simulation assumes that all interferers are transmitting all of the time, independent of their application and duty cycles. In the real world this is clearly not the case.
SEAMCAT's treatment of duty cycle simulates the worst case. It is necessary to take this into account when interpreting the results.

Principle of simulation
For the purposes of this study SEAMCAT performs the simulation according to the following criteria:
- the victim is fixed at the centre of a circle given by the <u>calculated</u> simulation radius
- the interferer is randomly moved around the victim within this circle.

This applies to all equipment with the exception of the DVB-T transmitter as an interferer. For this scenario the simulation radius is set to 25 km, which is the assumed coverage range of the DVB-T transmitter.

During the simulation the interferer is moved around the victim.

Even if the interferer is a fixed station the result of the simulation is correct, because only the randomly generated path losses between the victim and the interferer are used to calculate the sum of the received interference powers. It is immaterial therefore to the simulation whether in the real world the interferer or the victim is moved.

ANNEX D.5   Simulations of RFID

D.5.1 Description of operation

To enable multiple interrogators to transmit simultaneously in the same geographic space and to minimise possible interference with other users of the same spectrum, TR 102 649-1 [4] proposes the use of a 4 channel plan. To obtain maximum benefit from this arrangement, it is recommended that RFID systems operate in the dense interrogator mode. The principle of the dense interrogator mode is shown in the diagram at Fig D.5.1 and is illustrative only.
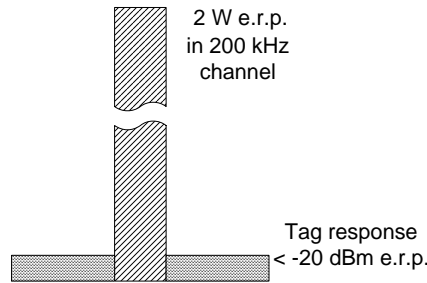

Figure D.5.1: Principle of dense interrogator mode

The transmit signal from an interrogator may be at a power level of up to 2 W e.r.p. and is shown in Fig D.5.1 as occupying the centre channel of 200 kHz. The two channels on each side of the transmit channel are reserved for the backscatter response from the tag. Typically tags will respond at offset frequencies of approximately 200 kHz or 300 kHz, which is set by the configuration of the interrogator. The power level of the response from a tag will be –20 dBm e.r.p. or less depending on its distance from the interrogator and the nature of the material to which it is attached. The dense interrogator mode separates the high power transmission of the interrogator from the low power signals of the tags, which improves system performance. It also permits transmissions from multiple interrogators on the same channel. In fact provided that an adequate minimum working distance is maintained between adjacent interrogators, there is no upper limit to the number of interrogators that may simultaneously operate at the same frequency.

Using the principle of the dense interrogator mode illustrated in Fig 1, TR 102 649-1 [6] has proposed four channels for high power use. A diagram of the 4 channel plan is in Fig D.5.2 shown below.
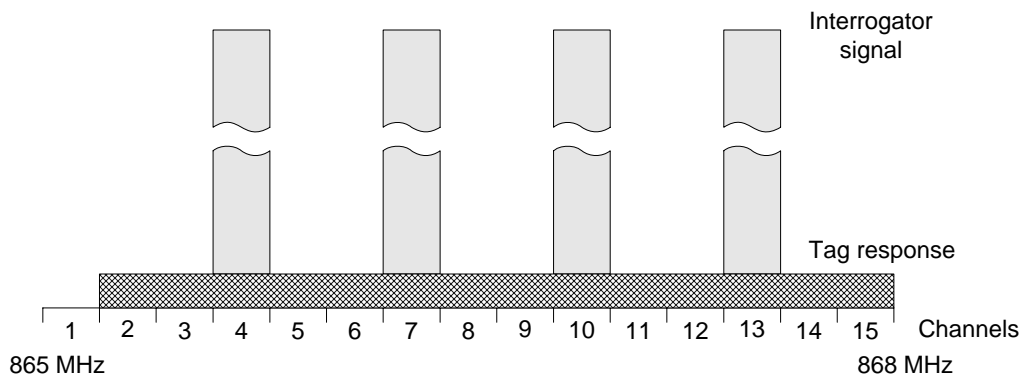

Figure D.5.2: Diagram of 4 channel plan

Interrogators may operate on any of the four specified high power channels within the band 865 MHz to 868 MHz at power levels up to 2 W e.r.p. The bandwidth of each high power channel is 200 kHz and the centre frequency of the lowest channel is 865,7 MHz. The remaining three high power channels are spaced at equal intervals of 600 kHz. Tags should preferably respond in the dense interrogator mode within the adjacent low power channels.

The simulation was performed on the basis that RFID interrogators transmitted only on four specified channels with no mandatory requirement for LBT. Tags responded in the adjacent low power channels. Five different scenarios were considered representative of the way in which RFID might be used. These included:

1.   Multiple RFID interrogators in a **hotspot** such as a distribution centre (dense interrogator scenario as described by the SRDoc ETSI TR 102 649 [6])
2.   A line of interrogators at the check-outs of a **store** (a row of checkouts at a store; due to shorter distances only 500 mW e.r.p. is assumed)
3.   RFID on conveyors at **airport** terminals for baggage handling (a baggage handling hall in an airport terminal building; such systems would be carefully designed and have to satisfy the requirements of the airport frequency management department)
4.   A typical concentration of interrogators in an outdoor environment (any other usage not specially defined)
5.   RFID in a store, i.e. a variant from the store scenario, in which individual items are tagged so that they may be identified "**item tagging**".

For the purposes of the study four classes of victim were assumed as follows

1.   SRDs operating in the band 865 – 868 MHz as defined in Annex 1 of Rec. 70-03 [7],
2.   SRDs operating in the band 863 - 870 MHz but outside from the frequency range 865 – 868 MHz as defined in Annex 1 of Rec. 70-03 [7], category 2.
3.   Social alarms as defined in Annex 7 of Rec. 70-03.
4.   Audio devices as defined in Annex 10 and Annex 13 of ERC Rec. 70-03.
5.   Devices using DSSS in the band 865 – 868 MHz as defined in Annex 1 of Rec. 70-03.

D.5.2 Parameters of interferers

Table D.5.1 provided the values assumed for interferers in the different scenarios. For the "Store" scenario, a power level of 500 mW is assumed. This is because the application must be tightly controlled and powers kept to a minimum, otherwise there is a risk of incorrectly charging customers in adjacent lanes. In the case of the airport application a protection distance of 1000 m is used. This is because every transmitting device used by airport personnel within the airport comes under the jurisdiction of the airport frequency management department. Those victims of interest in this study will therefore be outside the airport perimeter.

The densities used for the hotspot and airport scenarios were derived from the SRDoc. A large distribution centre may have up to 120 dock doors, each equipped with an interrogator. It is possible in an industrial park for up to 4 distribution centres to be located within a square kilometre, which equates to a density of 480 interrogators per sq km. It was considered reasonable to assume this same unit density for interrogators in airport terminals.

The densities of interrogators assumed for both the store and the "other" scenario were derived from data contained in the European Passive RFID Market Sizing 2007 - 2022 [19].

The SEAMCAT simulations also considered the emissions from the "activated tags" as a source of interference with similar deployment as the interrogators.

	Hotspot	Store	Airport	Other	Item tagging
Power [dBm e.r.p.]	33	27	33	33	27
Antenna gain	8 dB / Type 1	8 dB / Type 2	8 dB / Type 2	8 dB / Type 2	0 dB / Type 3
Density [km^{-2}]	480	12	480	12	See note b)
Active units	20	10	20	5	4
Duty Cycle [%] a)	20	50	97.5	5	100
Environment	Outdoor	Indoor	Indoor	Outdoor	Indoor
Protected radius [m]	100	10	1000	10	none

a) Ratio of tx_on to tx_off time (Activity in SEAMCAT)
b) The density of transmitters per km2 is not uniform in surface. The distribution of transmitters is uniform in distance. On a single floor (radius of 150 m), as a worst case 4 interrogators have been simulated, i.e. one per channel.

Table D.5.1: Parameters of the interferers

The antenna patterns used in the SEAMCAT simulation for the interferer are shown in Figures D.5.3, D.5.4 and D.5.5. For the hotspot scenario the antenna pattern in Figure D.5.4 is assumed, which takes into account the wall loss of 10 dB in the direction of the main beam.
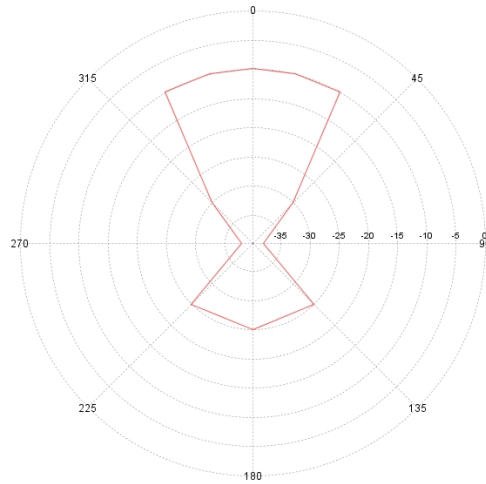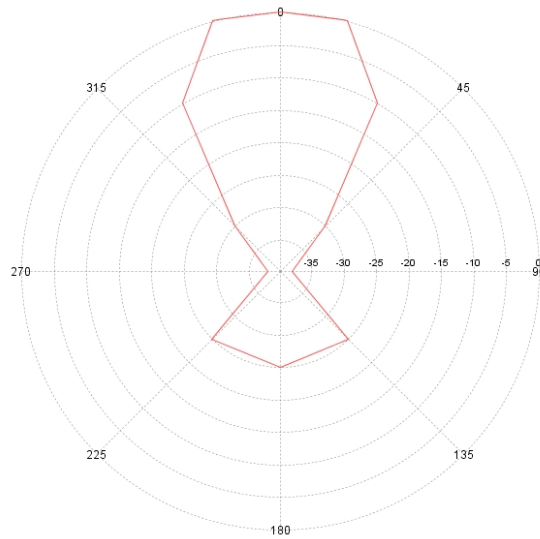
Figure D.5.3: Antenna Type 1
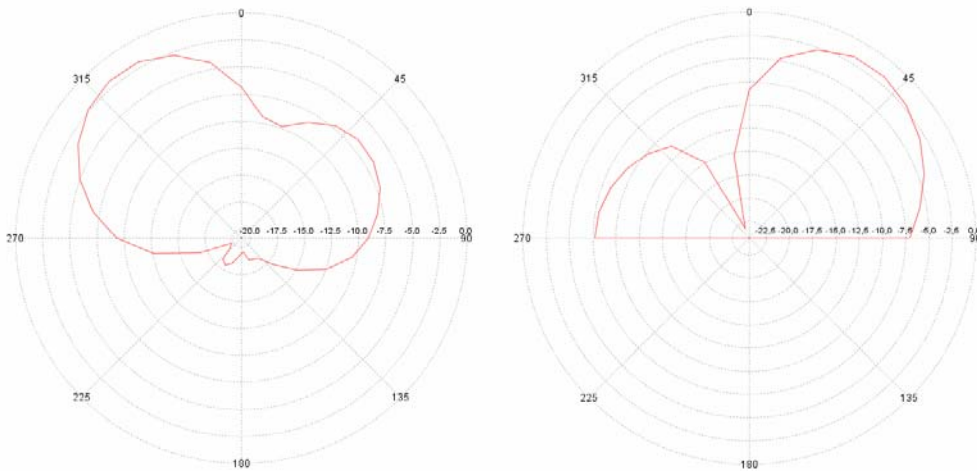

Figure D.5.4: Antenna Type 2

Figure D.5.5: Antenna Type 3 (horizontal / vertical)

Tag systems are assumed to be omni-directional, 0dB.

The spectrum mask used in the SEAMCAT simulations is provided below and is taken from ETSI TR 102 649-1 [6].
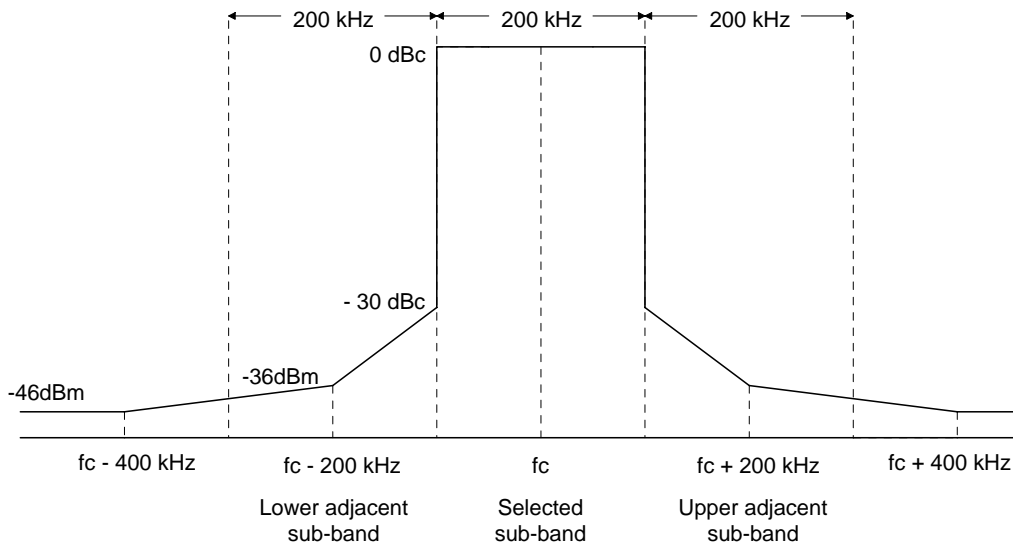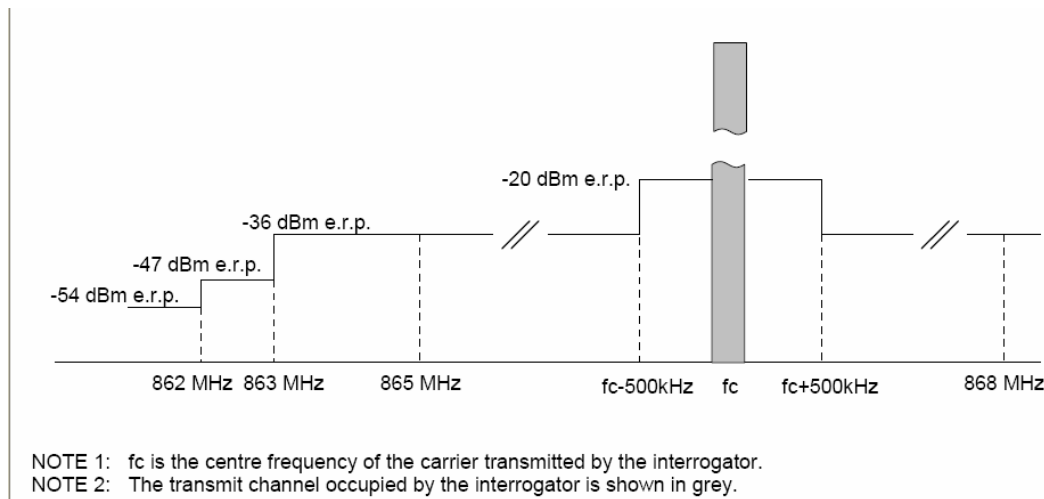

Figure D.5.6: Spectrum mask of interrogator

It has to be noted that the values measured outside the 200 kHz necessary bandwidth are measured in a 3 kHz resolution bandwidth. In addition, outside of 250 % of the necessary bandwidth, the values are given in 100 kHz (see EN 302 208-1 V1.2.1).

The spectrum mask for tag used in the SEAMCAT simulations is provided below and is taken from EN 302 208-1 V1.2.1 [26]

NOTE 1: fc is the centre frequency of the carrier transmitted by the interrogator.
NOTE 2: The transmit channel occupied by the interrogator is shown in grey.

Figure D.5.7: Spectrum mask of tag [26]

D.5.3 Parameters of victims

The parameters for the victims are shown in Table D.5.2. The devices considered include all SRDs that operate in the band 865 – 868 MHz. For the band 868 – 870 MHz, Annex 7 of Rec. 70-03 [7] has been selected since social alarms are the most sensitive of the various applications. It is considered that a favourable result for equipment under Annex 7 would represent a satisfactory outcome for all other applications in the band 868 – 870 MHz. Audio devices operating in the band 863- 865 MHz were also considered under Annex 10 and Annex 13. DSSS was also considered as a victim system.

Rec. 70-03	Annex 1	Annex 7	Annex 10	Annex 13	DSSS 3
Bandwidth [kHz]	100	25	300	50	3000
Sensitivity [dBm]	-101	-107	-90	-104	-80
C/(I+N) [dB]	8	8	17	8	-17
Selectivity (category 1) (Protection Ratio Mode)	EN 300 220 (except for item tagging scenario where category 2 is considered)	EN 300 220	EN 301 357 [22]	EN 300 220	EN 300 220 (not used in the simulations)
LBT threshold [dBm]	-90	n/a		-90	n/a
Power [dBm e.r.p.]	14	10 [2]	10	10	14
Operation range [m]	100	100	100	100	100
Antenna	Omni directional 0 dB gain				
Frequency [MHz]	865.9 MHz and 866.0 MHz [1] or 868.1 MHz [3]	869.26125 MHz	864.85 MHz	864.975 MHz	866.5 MHz
Environment	865.9 MHz and 866.0 MHz Outdoor except for the scenario "item tagging" where it is indoor	Outdoor	Outdoor	Outdoor	Outdoor

1) offset of 200 kHz and 300 kHz; see Table D.5.4
2) For social alarms: an output power of -10 dBm e.r.p. has been used for the simulation since this is representative of the radiated power due to body effects.
3) 868.1 MHz for the scenario "item tagging".

Table D.5.2: Parameter for the victims

Rec. 70-03	Annex 1	Annex 7	Annex 10	Annex 13	DSSS 3
Hotspot	865.7 MHz and 866.9 MHz	866.3 MHz and 867.5 MHz	865.7 MHz and 866.9 MHz	865.7 MHz and 866.9 MHz	865.7 MHz and 866.9 MHz
Store	865.7 MHz	867.5 MHz	865.7 MHz	865.7 MHz	866.3 MHz
Airport	865.7 MHz	867.5 MHz	865.7 MHz	865.7 MHz	866.3 MHz
Other	865.7 MHz	867.5 MHz	865.7 MHz	865.7 MHz	866.3 MHz

Table D.5. 3: centre frequencies of the interferers

D.5.4 Results of simulations

Two different types of simulation were carried out. These have each been considered separately below. The simulation has been performed using that frequency for the victim, which is either the adjacent channel, if applicable, or the closest channel to the adjacent sub-band.

The simulation in Figure D.5.8 shows the probability for an SRD with LBT of finding an available channel in scenario 1 (hotspot case). The X axis on the chart equates to the LBT threshold level of a receiver in an SRD, while the Y axis shows the cumulative probability of finding an available channel. The cumulative probability means that for a specific value of Y all received levels are 100% or less of the corresponding value for X.
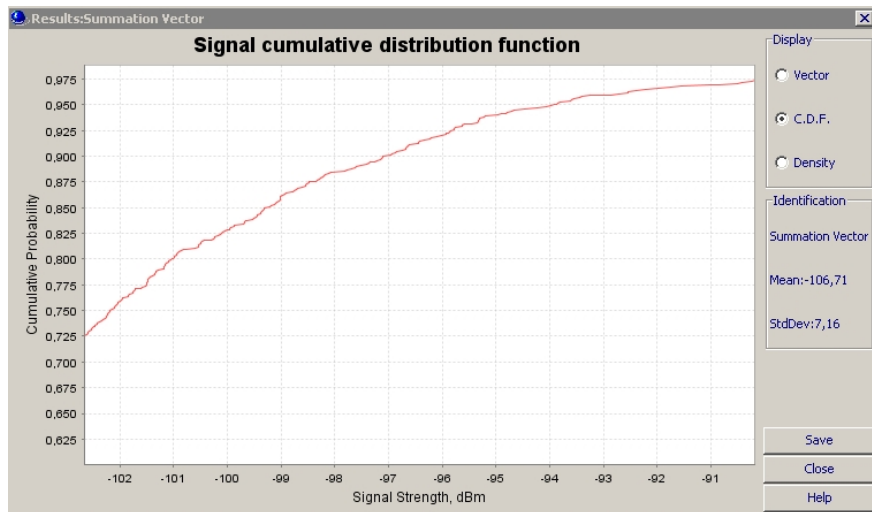
Figure D.5.8: probability of LBT threshold levels

The curve shows that, as the LBT threshold level of the victim SRD is increased from –102 dBm to -90 dBm, the probability of finding an available channel improves from 72.5% to 97.5%. The figure of 97.5% corresponds to an LBT threshold of –90 dBm, which is the level specified in ETSI EN 300 220. The figure of 97.5% for the cumulative probability of finding an available channel is considered acceptable.

The results in Table D.5.4 provide probabilities for interference under the different scenarios.

Rec. 70-03	Annex 1		Annex 7 Probabilities (%)	Annex 10 Probabilities (%)	Annex 13 Probabilities (%)	DSSS 3 [3] Probabilities (%)
	Freq Offset	Probabilities (%)				
Hotspot	200 kHz	27 % [3]	7.3 % [1] [2]	2 % [2]	0.1 % [2]	16 %
	300 kHz	27 % [3]				
Store	200 kHz	0.3 %	Below 7.3 %	Below 2 %	Below 0.1 %	Below 16 %
Airport	200 kHz	0 %	Below 7.3 %	Below 2 %	Below 0.1 %	Below 16 %
Other	200 kHz	0.1 %	Below 7.3 %	Below 2 %	Below 0.1 %	Below 16 %
Item tagging	200 kHz / 300 kHz	11 %	[4]	[4]	[4]	[4]

   1) For social alarm: an output power of -10 dBm e.r.p. has been assumed
   2) blocking is dominant
   3) blocking and unwanted emissions
   4) The victim receivers are assumed outdoor. This will result in an additional attenuation of 10 dB.
   Therefore, these scenarios have not been simulated.

Table D.5.4: Probability of interference [%]

The column "Annex 1" relates to SRDs operating both with and without LBT in channels adjacent to the interferer. Two offset frequencies were considered. The first was when the mid-point of the adjacent channel occupied by the SRD was 200 kHz from the carrier frequency of the interferer. The second case assumed an offset frequency of 300 kHz.

Due to the fact that ETSI defined the mask for tag with a resolution bandwidth of 3 kHz and a power of -20 dBm within the range of fc +/- 500 kHz, the victim using 100 kHz bandwidth (e.g. Annex 1 as a victim) within that range receives   -4.8 dBm although the total radiated power is still only -20 dBm e.r.p.; i.e. -based on that – the simulations account for a never existing worst case. For the co-channel case of the interrogator a reference bandwidth of 200 kHz was used in order to solve this issue. But for the tags there was no available value for the necessary bandwidth resulting in an overestimation of the interference probability resulting from tag. Assuming a 100 kHz bandwidth for the reference bandwidth of the tag, in the scenario hotspot - Annex 1, the probability is around 5 % (instead of 27%).

Taking into account these considerations, the figures for probability of interference for victims under Annexes 1, 7, 10 and 13 of Rec. 70-03 are considered acceptable.

In practice the performance of SRDs can be further improved by the use of certain techniques. For example where SRDs incorporate LBT and AFA, they can monitor the channels to determine which ones, if any, are already occupied. If an SRD wishes to transmit it can therefore ensure that it operates on an unused channel. However for nearby SRDs without LBT and AFA that are co-channel with an RFID interrogator, the probability of interference will be increased. The probability will exceed the figures in Table A.1.2 for RFID 33 @ D.C. of 30% (see also ETSI TR 102 649-1 [29]). This may make the operation of such SRDs impracticable on the four high power channels.

Great care is necessary in interpreting the results for DSSS 3. The simulation was performed with DSSS 3 and RFID operating co-channel. However manufacturers of DSSS systems will be aware that four channels in the band have been designated for high power use. They will therefore design their equipment so as to "notch out" signals on these channels. In such circumstances it is considered that DSSS systems will operate satisfactorily in the presence of RFID.

It should be noted that the example of DSSS 3 represents the worst case. Annex 1 permits DSSS to operate across the additional bands 865 – 870 MHz and 863 – 870 MHz. In practice manufacturers will prefer to design their equipment to operate across the widest band (i.e. 863 – 870 MHz) since this will maximize the processing gain. In this case the impact of the four high power RFID channels will be reduced.

D.5.5 Effects on other services

When developing the compatibility studies described in this report, the subject of potential interference by RFID to military and other systems was considered. A concern raised at the time was that many of these systems operate using full duplex. The case was made that an RFID device fitted with LBT should readily detect the transmit signal from a nearby duplex system.

However it may not always detect the received signal, which is at a different frequency. Under these circumstances the RFID could transmit on the receive frequency of the victim causing possible interference (see annex D.6). Those countries that believed this to be a concern have overcome the problem by defining exclusion zones around geographic areas where unacceptable levels of interference may potentially arise.

The impact on services under the proposed four channel plan is no worse than the situation that exists today. Since the benefits of LBT in RFID for duplex systems were discounted, its removal does not change the situation. Arguably the situation under the four channel plan will be better since high power transmissions by RFID will be confined to just 4 channels whereas previously it was up to 10.

Based on these considerations the removal of the mandatory requirement for LBT in the four high power channels will not adversely effect the operation of military systems and other services.

D5.6 Conclusions

The compatibility study has demonstrated that RFID operating in accordance with the RFID channel plan proposed in the SRDoc ETSI TR 102 649-1 [6] will satisfactorily co-exist with other services and SRDs that operate in both the same and adjacent bands. The principal conclusions from the study are:

1.   SRDs with LBT and AFA may satisfactorily share the same band with RFID. For nearby SRDs without LBT and AFA that are co-channel with an RFID interrogator, the probability of interference will be increased. The probability will exceed the figures in Table A.1.2 for RFID 33 at Duty Cycle of 30% (see also ETSI TR 102 649-1 [6]). This may make the operation of such SRDs impracticable on the four high power channels.

2.   The levels of interference from RFID received by social alarms and other SRDs in the band 868 – 870 MHz is considered acceptable

3.   Audio devices operating in the band 863 – 865 MHz will not be significantly effected by removal of LBT in the four high power channels

4.   It is considered that the DSSS systems operating over 3 MHz bandwidth will perform satisfactorily provided steps are taken to minimise reception of signals in the four high power channels. However, it seems likely

that for many applications, manufacturers of DSSS systems will prefer to design their equipment to operate over the full band 863 – 870 MHz. In this case, the effect of RFID transmission in the 4 high power channels will be reduced.

5.   It is considered that the removal of LBT in the four high power channels will have no adverse impact on the operation of military and other services. In fact the channelisation may even improve the current sharing situation.

ANNEX D.6: Compatibility between TRR systems and 2W UHF RFID in the 865─868 MHz frequency band

This study evaluates the impact of deployment of 2W UHF RFIDs in the 865─868 MHz frequency band (cf. Annex 11 of ERC/Rec.70-03 [7]) on military tactical radio relays (TRR).

The technical hypothesises and deployment of RFIDs are taken from this report

The technical parameters of TRR systems are taken from the ECC report 34 (note : with an exception for the receiver bandwidth, see below).

D.6.1 Hypothesis

D.6.1.1 SEAMCAT Simulations

Interference calculation: 20000 events / algorithm '*Complete 1*'

Propagation models :
1.It → Wr:	*Hata extended (SRD) - Urban / Outdoor / Above roof*
2.Wt → Vr:	*Free space*

D.6.1.2 TRR systems

Centre frequency: 866.5 MHz (worse case canal for 2W UHF RFIDs in the 865.7–867.7 MHz frequency band).
TRR link length: 80 km adjusted to obtain an availability of around 99%.

D.6.1.2.1 TRR receiver

Receiver bandwidth: 1500 kHz (ECC Rep.34 [20]: 750 kHz)
Receiver Noise: -105 dBm
Noise Factor: 7 dB
Antenna Gain: 16 dBi (main lobe); -8 dBi (at 90°)
Antenna Heigh:t 15 m (an effective height of 15 m is used in the urban case, 25 m should be used for open areas)
Protection Ratio: 15 dB
Sensitivity: -90 dBm
Rx selectivity

ΔF (MHz)	0	±0.750	±2	±5	±8
Rx selectivity (dB)	0	0	65	85	110

Table D.6.1: Tactical Radio Relay receiver selectivity

D.6.1.2.2 TRR transmitter

Tx Power: 5 W (37 dBm)
Transmitter spectrum

ΔF (MHz)	0	±0.375	±1.5
Tx spectrum (dBc)	0	0	-80

Table D.6.2: Tactical Radio Relay transmitter spectrum

Antenna: idem Rx antenna

D.6.1.3 Technical parameters of 2W UHF RFIDs in the 865.7 ─ 967.7 MHz frequency band

Antenna Height: 1.5 m

Interferer	Output Power (dBm)	Channel Bandwidth (kHz)	Channel Centre (MHz)	Duty cycle (%)	Units per km^2	Attenuation for Unwanted emissions (dBc)
2W UHF RFID	33.0	200	865.7 – 867.7	0.1	20	- 69

Table D.6.3: Technical parameters of 2W UHF RFIDs

D.6.2   Results of simulations

Result with duty cycle taken from Table 6.2.1 is given below

Interferer	Duty cycle	Units per km^2	Interference probability
2W UHF RFID	0.1%	20	**2.5%**

Table D.6.4: Results for 0.1% Duty Cycle

Result with duty cycle (i.e. activity factor) adjusted to 10% is given below:

Interferer	Duty cycle	Units per km^2	Interference probability
2W UHF RFID	10%	20	**76%**

Table D.6.5: Results for 10% Duty Cycle

D.6.3   Conclusion

The results are of course very sensitive to the activity factor. It should be noted that LBT is not efficient in case of FDD systems.

ANNEX E   MCL METHOD AND ANALYSIS

E.1   General introduction for MCL calculations

E.1.1   Used method

Protection distances are calculated for both co-channel interference and blocking from which the cumulative probability of interference is derived.

E.2   Interference criteria

E.2.1   Co-channel interference

I/N is used as the interference criteria for MCL. Co-channel interference is calculated with I/N = 0 dB and I/N = 10 dB level:

    a) The interference criteria of I/N = 0 dB equals the receiver sensitivity without margin.

    b) In order to simulate typical operation, the interference criteria of I/N = +10 dB equals the receiver sensitivity with 10 dB margin.

E.2.2   Blocking

Protection distances are calculated for blocking level of –30 dBm level at +/-1 MHz and +/-2 MHz. The reference BER is 1%.

E.3   Characteristics of existing and proposed systems

Existing devices operating in the 862-870 MHz band have different characteristics and will have different responses to potential interferers.

E.3.1   Victim and Interferer characteristics

E.3.1.1 Summary victim receiver characteristics

Victim characteristics are derived from section 3 of this Report. The characteristics are shown in table E.3.1.1 below:

	Noise level at receiver input	Noise Equiv. Bandwidth (NEB)	Antenna gain	Antenna beam-width, degrees	Antenna height
Existing systems					
Generic SRD 1	-120 dBm	15 kHz	2.1 dB	360	1.5 m
Generic SRD 2	-114 dBm	100 kHz	2.1 dB	360	1.5 m
Generic SRD 3	-110 dBm	250 kHz	2.1 dB	360	1.5 m
Radio microphones	-111 dBm	200 kHz	2.1 dB	360	1.5 m
Wireless Video	-111 dBm	300 kHz	2.1 dB	360	1.5 m
Consumer audio	-117 dBm	50 kHz	2.1 dB	360	1.5 m
CT 2 Handset	-114 dBm	100 kHz	2.1 dB	360	1.5 m
CT 2 Station	-114dBm	100 kHz	2.1 dBi	360	2.5 m
Proposed systems					
Generic FHSS	-114 dBm	100 kHz	2.1 dB	360	1.5 m
FHSS, 25 KHz, note 2	-120 dBm	15 kHz	2.1 dB	360	2.5 m
Generic DSSS	-94 dBm	600 kHz	2.1 dB	360	1.5 m
DSSS, 2 MHz, note 1	-94 dBm	2 MHz	2.1 dBi	360	1.5 m
RFID Note 3	-110 dBm	200 kHz	8 d**B**	83	1.5 m
CT 2 Handset	-114 dBm	100 kHz	2.1 dB	360	1.5 m
CT 2 Station	-114dBm	100 kHz	2.1 dBi	360	2.5 m

Note 1: Special application according to ETSI SRDoc, TR 102 134 for tracking of containers
Note 2: Special application according to ETSI SRDoc, TR 102 069 for car anti-theft [4]
Note 3: Special application according to ETSI SRDoc, TR 100 220 for RFID [23]

Table E.3.1.1. Characteristics of victim receivers

E.3.1.2 Summary of interfering transmitter characteristics

The interfering characteristics of transmitters are derived from section 3.
The values in Table E.3.1.2 below are reflected in the values used in the Excel spread sheets, see ANNEX E.6

	Maximum Radiated Power (e.r.p.)	Modulation Bandwidth (3dB)	Total TX Band- width	Max. Duty Cycle	Antenna Beam- width (degrees)	Antenna Height
Reference systems:						
Generic SRD 1	+10 dBm	25 kHz	100 kHz	100 %	360	3.0 m
Generic SRD 2	+20 dBm	100 kHz	500 kHz	1 %	360	2.5 m
Generic SRD 3	+27 dBm	250 kHz	250 kHz	10 %	360	2.5 m
Microphone	+10 dBm	200 kHz	2 MHz	100 %	360	1.5 m
Wireless Video	+10 dBm	300 kHz	2 MHz	100 %	360	1.5 m
Consumer audio	+10 dBm	50 kHz	200 kHz	100 %	360	1.5 m
CT2 lHandset	+10 dBm	100 kHz	4 MHz	15 %	360	1.5 m
CT2 Station	+10 dBm	100 kHz	4 MHz	100 %	77	2.5 m
Proposed systems						
Generic FHSS	+14 dBm	100 kHz	7 MHz	100 %	360	1.5 m
FHSS, 25 kHz note1	+27 dBm	25 kHz	2 MHz	0.003%	360	2.5 m
Generic DSSS	+14 dBm	600 kHz	7 MHz	10 %	360	1.5 m
DSSS, 2 MHz note2	+33 dBm	2 MHz	7 MHz	0.03 %	360	1.5 m
RFID note3	+33 dBm	200 kHz	3 MHz	30 %	360	1.5 m

Note 1: Special application according to ETSI SRDoc, TR 102 134 for tracking of containers[5]
Note 2: Special application according to ETSI SRDoc, TR 102 069 for car anti-theft [4]
Note 3: Special application according to ETSI SRDoc, TR 100 220 for RFID [23]

Table E.3.1.2. Characteristics of Systems for Interference Analysis

E.4.0   Calculation models
The following sections describe the method of calculating the probability and deterministic model of interference.

E.4.1   Deterministic model

E.4.1.1 General

The deterministic model focuses on one interferer and is only relevant for the MCL part of the study. To achieve an aggressive low cost goal several compromises are made particularly on fundamental receiver parameters, which normally are considered vital for an operation in the shared band 863-870 MHz. Due to the diversity of different services in this band some performance degradations are to be expected.
ANNEX E shows calculations for SRD blocking by the MCL method.
The cumulative co-channel interference effects are considered under the probabilistic MCL method, see E.4.2.

E.4.1.2   Nominal receiver signal

The MCL study bases all interference scenarios on MUS +3 dB and MUS + 13 dB. The minimum receive signal, P_{RX_MIN} is:

$$P_{RX\_MIN} = MUS + 3\ dB$$

where:

MUS = Maximum Usable Sensitivity

For the purpose of this study the MCL calculations use an interference criteria of MUS +3dB which is equal to I/N = 0dB.
For telemetry and data systems MUS is approximately equal to the receiver noise + 14 dB.

E.4.1.3 Propagation model used for deterministic method

The discussion of this section only applies to calculations performed using the deterministic method.
Propagation models for the probabilistic method are discussed in clause 6.2.2

At 865 MHz, Path Loss, PL is:

a) for distances below 10 m free-space propagation applies:

$$PL = 31.2 + 20 \log d \qquad \text{(dB)} \qquad \text{(6.1.3.a)}$$

b) for distances above 10 m:

$$PL = 51.2 + 35 \log \frac{d}{10} \qquad \text{(dB)} \qquad \text{(6.1.3.b)}$$

where d is the distance in metres.

E.4.1.4 Minimum Coupling Loss and protection distance

The protection distance, d_P , for any interference is determined by means of the Minimum Coupling Loss (MCL) method.

$$MCL = P_{RAD} - P_{RX} + C/I \qquad \text{(6.1.4)}$$

Where:

MCL = Minimum Coupling Loss in dB;
P_{RAD} = Radiated power (e.r.p.) for interfering transmitter in dBm;
P_{RX} = Victim received power in dBm;
C/I   = Carrier to interference ratio specified for the Victim receiver in dB;

The calculated MCL can be obtained by path-loss, PL , over a certain protection distance, d_P. This can be derived from an appropriate propagation model.

$$d = 10^{(PL - 31,2)/20} \qquad \text{for PL<51.2 dB, and}$$

$$d = 10 * \left(10^{(PL - 51.2)/35} \right) \qquad \text{for PL} \geq 51.2 \text{ dB}$$

E.4.1.4.1   Blocking

The following specification is used for the calculation:

Blocking level criteria: -30 dBm at a frequency separation of equal to or greater than 1 MHz.

The mechanism for blocking or co-channel interference is given by table E.4.1.4.2 below:

Interferer type	Power e.r.p (dBm)	Duty cycle (%)	Chan BW (kHz)	Primary mechanism of interference
Generic SRD 1	+10	10	15	Co-channel
Generic SRD 2	+10	1	100	Co-channel
Generic SRD 3	+10	100	250	Co-channel
Microphone	+10	100	200	Co-channel
Wireless Video	+10	100	300	Co-channel
Consumer Audio	+10	100	50	Co-channel
CT2	+10	100	100	Co-channel
Generic FHSS	+14	1/10/100	100	Co-channel
FHSS, 25 kHz note 2	+27	0.03	25	Co-channel
Generic DSSS	+27	1/10/100	600/3000/7000	Co-channel
DSSS, 2 MHz note 1	+33	0.03	2000	Blocking
RFID note 3	+33	30	200	Blocking

Note 1: Special application according to ETSI SRDoc, TR 102 134 for tracking of containers [5]
Note 2: Special application according to ETSI SRDoc, TR 102 069 for car anti-theft [4]
Note 3: Special application according to ETSI SRDoc, TR 100 220 for RFID [23]

Table E.4.1.4.2. Interference mechanisms to SRD for different types of interferer

E.4.2 Probabilistic method

Interference probability analysis is a four-step process, leading to an interference assessment for different scenarios. Those steps are:

Step 1
- Determine the "Minimum Coupling Loss (MCL)" between the interferer and the victim. The equation for this calculation is given in Annex E. 4.2.1.

Step 2
- Convert the MCL result from step 1 into a minimum protection distance for a single interferer by means of an appropriate propagation model. These propagation models are described in Annex E. 4.2.2.

Step 3
- Calculate the number of potential interferers inside the interference area. This calculation is described in Annex E. 4.2.3.

Step 4
- Evaluate the cumulative probability of interference using Equation E. 4.2.5.b described in Annex E 4.2.5.

E.4.2.1. Minimum coupling loss

The Minimum Coupling Loss between the interfering transmitter and victim receiver determines the minimum protection distance. This cell size (radius) R_{INT} is identical to the calculated protection distance has to be calculated by means of an applicable propagation model (see sub-section 5.2.2) and minimum coupling loss.

The Minimum Coupling Loss (MCL) is the minimum path loss required to avoid interference, which is given by:

$$MCL = P_{srd} + G_t - L_b - Lf_t + G_r - Lf_r + 10 \, log(B_r \cap B_t / B_t) - I \qquad (6.2.1)$$

where:

I : maximum permissible interference level at victim receiver
P_{srd} : interfering transmitter conducted power
G_t : interfering transmitter antenna gain
G_r : victim receiver antenna gain
Lf_t : interfering transmitter feeder loss
Lf_r : victim receiver feeder loss

B_t : interfering transmitter 3 dB bandwidth
B_r : victim receiver 3 dB bandwidth
L_b : building loss as appropriate
$B_r \cap B_t$: overlapping part of the transmitter and receiver frequency band.

E.4.2.2 Propagation models

For MCL calculations different propagation formulas are used for each combination of the following environments: indoor, urban, and rural. For systems operating indoors, an additional 10 dB building attenuation, M_{WALL}, is assumed per ITU-R P.1238-2 [21]. All of the propagation formulas below predict the median value of path loss.

E.4.2.2.1   In- door propagation model

The indoor model uses a free space propagation formula, which applies for distances, d, of less than 10 metre (a path loss exponent of 2). Beyond 10 metre, the exponent is 3.5. The following indoor model is assumed valid from 10m to 500m:

$$Pl\,(r)\,(dB) = 50.1 + 35 \log\left(\frac{d}{10}\right) + M_{WALL} \qquad (6.2.2)$$

Beyond 500m, this model is not applicable since most indoor building areas are smaller than 500m. The indoor propagation model is supported by numerous measurements found in literature, e.g. "Wireless Communications" by T. S. Rappaport, ISBN 0-13-375536-3, chapter 3 [25].

E.4.2.2.2.   Urban model

For the purposes of this study the CEPT SE21 urban model is used This model is described in ERC/REP 68 (mm) and is valid for frequencies between 150 MHz and 1500 MHz.

$$L_{CEPT}(urban,\ dB) = 69.6 + 26.2 \log f - 13.82 \log h_{tx} - a(h_{rx}) - a(h_{tx})$$
$$+ \ (44.9 - 6.55 \log h_{tx}) \log d$$

where $a(h_{tx})$ $= = (1.1 \log f - 0.7)\ Min(10,\ h_{rx}) - (1.56 \log f - 0.8)$
$$+ Max\ [0,\ 20 \log (h_{rx}/10)]$$

and $a(h_{rx})$ $= (1.1 \log f - 0.7)\ Min(10,\ h_{rx}) - (1.56 \log f - 0.8)$
$$+ Max\ [0,\ 20 \log (h_{rx}/10)]$$

are "antenna height gain factors" for the transmitter and receiver antennas, respectively. The equations given above predict large negative values (*e.g.,* negative18 dB) for the transmitter's antenna height gain for low antennas. This arises because the CEPT/SE21 model assumes that the transmitter antenna is mounted high (above 30 m) and in the clear. But in the situations of interest in this report, typically both transmit and receiver antennas are below 10 m, so that nearby ground clutter and reflections are no longer negligible.

For the purposes of this study for both the SEAMCAT simulations and MCL calculations, the SE21 propagation model is extended by using the "height gain" equation:

$a(h_{tx}) = (1.1 \log f - 0.7)\ Min(10,\ h_{tx}) - (1.56 \log f - 0.8)\ dB + Max\ [0,\ 20 \log (ht_{rx}/10)]$

when both antenna heights are less than 10m.

E.4.2.2.3   Rural model

The rural propagation model used within the radio line-of-sight in this report is the CEPT SE21 rural model, also referred to as the modified free space loss model. The rural model assumes free space propagation until a certain break point distance, r_{BREAK} depending on the antenna heights for the interferer and victim:

$Pl(r)(dB) = 20 \log(4\pi r/\lambda) + M_{WALL}$ for $r < r_{BREAK} = 4\pi.ht.hr/\lambda$
$Pl(r)(dB) = 20 \log(r^2/(ht.hr)) + M_{WALL}$ for $r > r_{BREAK} = 4\pi.ht.hr/\lambda$

E.4.2.3 Number of interfering units

The protection distance, R_{INT}, is equivalent to the path length, d, corresponding to the Minimum Coupling Loss (MCL), as determined in Annex E. 4.2.1 above. The protection distance, d, is used to calculate the interference area. The total number of interfering transmitters within this area, N_{INT}, is the product of the unit density and this area.

Additionally, the spatial distribution of the interfering transmitters is considered below.
Two different distribution models have been used to derive the cumulative probability of interference:
- a uniform distribution, and
- an exponential distribution.

The exponential distribution of interfering transmitters is used by MCL to assess hot-spot interference. . Consequently, the interference will mostly arise from clusters of interferers located near the victim receiver. This clustering is modelled by the exponential distribution given in equation E.4.2.3.a below.

For further information on the numbers for the related unit density used, see Annex E.6.

In the exponential distribution, the density of interferer decays as the distance from the victim increases. This is best described by the following formula:

$$N(r) = No \cdot \exp(-k \cdot r) \qquad (E.4.2.3.a)$$

where:
N: represents the interferer's density versus distance from the centre of the interference area.
No: represents the hot-spot unit density of interferers (units/km square) given in E.6.(spread sheet)
r :   is the distance from centre (r = 0) to the periphery (r = d) of the interference area
k: is the decay constant that is set to k = 2 to represent expected distribution of interferers.

The following figure illustrates exponential density:
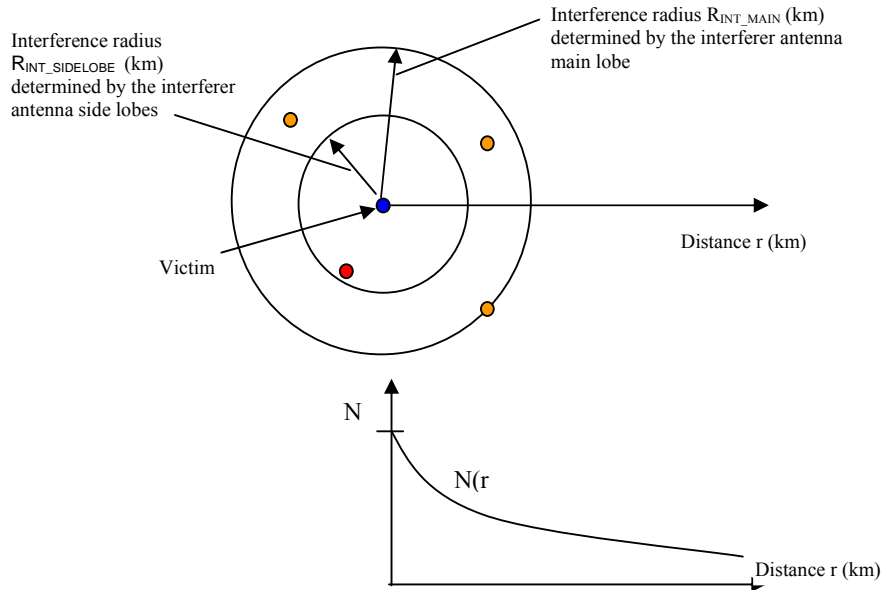

Figure. E.4.2.3. Distribution of interferers within the interference areas for main and side lobes

In Figure E.4.2.3 above, the larger interference area is determined using the gain of the interferer antenna in the direction of the main lobe. The smaller area is determined using the gain of the antenna in other directions (side-lobes).

The total number of interferers in each of the interference areas is calculated by:

$$N_{INT}(R_{INT}) = \iint\limits_{r\beta} N(r) \cdot r \cdot dr \cdot d\beta \qquad (4.2.3.b)$$

Integration over r =(0 , R_{INT}) and the angle beta, β over β = (0 , 2 π) yields:

$$N_{INT}(R_{INT}) = \frac{2\pi\ No}{k^2} \cdot [1 - (k\ R_{INT} + 1) \cdot \exp(-k\ R_{INT})] \qquad (4.2.3.c)$$

Equation (6.2.3.c) is used to calculate the number of interferers within each of the interference areas

E.4.2.4 Probability of antenna pattern, time, and frequency collision

E.4.2.4.1.   Probability of alignment of antenna main beams

In the simplest case both interferer and victim have omni-directional antennas resulting in a pattern collision probability of 100%. However, some systems of interest in this report use directional antennas to reduce interference potential.

Where the main beam of the victim's antenna lies within the main beam of the interferer's antenna the interference probability for an antenna beam angle, β for both the victim and interferer is given by:

$$P_{PAT\_COL} = \frac{\beta_{VIC\_MAINBEAM}}{360} * \frac{\beta_{INT\_MAINBEAM}}{360} \qquad (E.4.2.4.1)$$

E.4.2.4.2   Added probability for antenna side-lobes

For interfering devices that use directional antennas, the interference arising from side-lobes may be significant. Where the main beam of victim's antenna lies within a side lobe of the interferer's antenna the additional interference probability is given by:

$$P_{PAT\_COL} = \frac{360 - \beta_{INF\_MAINBEAM}}{360} * \frac{\beta_{VIC\_MAINBEAM}}{360} \qquad (E.4.2.4.2.a)$$

RFID interrogators and other Short Range Devices may use patch antennas, which are mounted on a large earth plane. The presence of the earth plane minimises radiation in the hemisphere to the rear of the antenna. In this case the overall equation is

$$P_{PAT\_COL} = \frac{180 - \beta_{INF\_MAINBEAM}}{360} * \frac{\beta_{VIC\_MAINBEAM}}{360} \qquad (E.\ 4.2.4.2.b)$$

The cumulative probability of interference from both main beam and side-lobes is given in Section E.5.2.2. For the sake of simplicity, cases where the interferer and victim antenna side-lobes are directed at each other have not been considered.

E.4.2.4.3   Probability for frequency overlap

E.4.2.4.3.1   Phenomena modelled by a universal P_{FREQ_COL} formula

For the probability of frequency collision, universal P_{FREQ_COL} formula models are described below:
- For the case of DSSS and NB (fixed SRD frequencies) systems it is the randomness of the frequency channel assignment that causes uncertainty of the "frequency collision event". Narrower channel bandwidths (either Tx or Rx) will contribute to a lower P_{FREQ_COL}. This occurs because narrowing either (or both) of these bandwidths results in a larger number of non-overlapping frequency windows available in the band and thus a larger number of non-overlapping BW_{TX} -BW_{RX} pairs.

- For the case of FHSS systems it is the randomness of the instantaneous frequency hop within the total set of hopping channels used that causes probability of the frequency collision event.

- The most complex case is a FHSS system hopping over only a portion of the band. Such a system benefits from both the randomness of the "frequency hopping span" position within the band as well as from the randomness of the instantaneous frequency hop.

E.4.2.4.3.2   Definition of the frequency collision event

The main reason for the difficulty in the calculation of the P_{FREQ_COL} is the lack of a clear definition of precisely what constitutes the "frequency collision event".

The difficulty of clearly defining the frequency collision event arises because it must properly describe a complex mix of interfering systems, having various signal bandwidths (relatively narrow or wide with respect to each other) and various frequency spectrum shapes. Also the spectrum overlap of the interfering systems (being analogue in nature) can be full or partial, resulting in different effects on the interference.

In the interest of consistency the following basic assumptions and definitions have been adopted in this report:

The interfering transmitter and victim receiver channel bandwidths used in all P_{FREQ_COL} calculations are 3 dB bandwidths. Thus, in terms of a transmitter, this is the *uniform-power-density-equivalent* of the DSSS null-to-null bandwidth. In the case of the receiver, the uniform power density equivalent is the system-noise-bandwidth. MCL spreadsheets have appropriate input "cells" for these parameters (Tx 3-dB bandwidth and Rx system-noise-bandwidth).

For DSSS and NB, "channel bandwidths" is the modulation bandwidth of a single channel.

For FHSS, "channel bandwidths" is the modulation bandwidth of a single hopping channel.

In consideration of the discussion above, the P_{FREQ_COL} is determined only by the "instantaneous bandwidth" occupied by both the interferer and the victim, normalised to the total available bandwidth (for example, the entire 7 MHz in the 863-870 MHz band).

The narrower this "instantaneous bandwidth" of either the victim receiver or the interfering transmitter, the less is the likelihood that they will overlap within the spectrum window of the full band. If the interferer or the victim is a FHSS system, the relevant "instantaneous BW" is the bandwidth of a single hop. In the case of DSSS or NB it is the DSSS or NB single channel bandwidth.

The universal formula for P_{FREQ_COL} immediately follows from the following definition of "the frequency collision event:"

The frequency collision event involving two interfering systems with "system noise bandwidths" BW_{INT} and BW_{VICT} occurs if at least half of the spectrum of the narrower bandwidth system overlaps with the spectrum of the other (wider bandwidth) system.

Notice that it really does not matter which of the two systems is the victim or interferer here. It is only their instantaneous bandwidths that determine the probability of overlap.

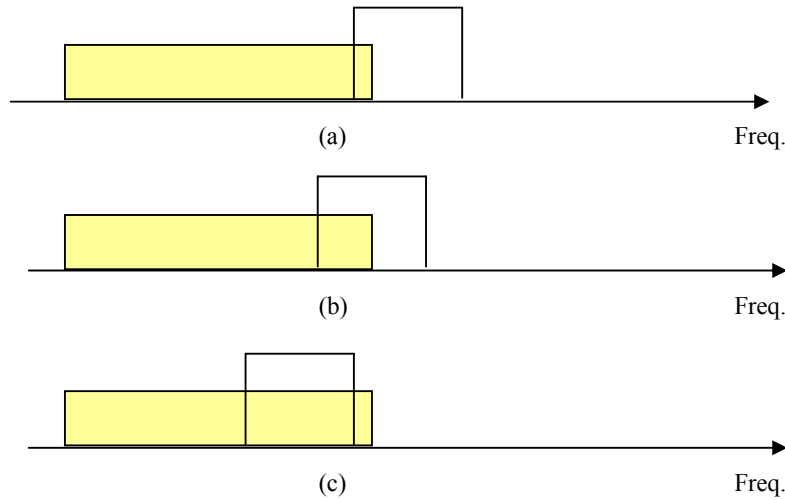The figure E.4.2.4.3.2 below illustrates the essence of this definition of the "frequency collision event.

Figure E.4.2.4.3.2. Definition of instantaneous frequency collision event

The shaded area in the drawings above represents the wider bandwidth (uniform spectral density equivalent) system spectrum. The shaded spectrum can be either interferer or victim.

Case (a) represents the situation with a marginal frequency overlap. In this case only a small fraction (and thus below the interference threshold) of the interferer power falls within the victim receiver. Although the spectra overlap somewhat, this still is not considered to be harmful interference.

Case (c) represents a total frequency overlap that definitely would cause harmful interference, if the interfering signal were sufficiently strong.

Somewhere in between Cases (a) and Case (c) is the case when the frequency overlap is such that any further increase would lead to a harmful level of interference. Case (b) represents the case when half of the spectrum of the narrower BW system overlaps with the wider bandwidth one. In this case, approximately half of the narrower system bandwidth is corrupted by interference (in the case where the narrower bandwidth system is victim) or penetrate the wider bandwidth victim (in the case where the narrower bandwidth system is interferer). This would constitute a –3 dB overlap. We have used this "half-power" (- 3dB) case as the criteria for defining the "frequency collision event", as discussed above.

The benefits of frequency hopping in terms of reduction of the probability of frequency collision are realised if just one of the interference elements (the victim or interferer) is of FHSS type. The interference situation generally does not improve by having both the transmitter and receiver frequency hopping.

Additional interference mitigation measures such as optimised channel selection (frequency use planning) are not calculated in analysis, although they can be used to reduce or sometimes even completely eliminate the interference. These techniques are applicable to all systems that feature a channel selection utility (frequency hopping systems), which adaptively select their hopping channels.

E.4.2.4.3.3   Formula for frequency collision

Following the definition of P_{FREQ_COL} given in section E.4.2.4.3.2 above, the formula is given by:

$$P_{FREQ\_COLL} = \frac{SPAN_{OVERLAP} \cdot Max(BW_{INT}, BW_{VIC})}{SPAN_{VIC} \cdot SPAN_{INT}}$$

where:

$SPAN_{OVERLAP}$: is the frequency overlap range for the interferer and the victim;

$SPAN_{VIC}$: is the allocated frequency range for the victim;

$SPAN_{INT}$: is the allocated frequency range for the interferer;

BW_{VIC} : is the receiver bandwidth of the victim;

BW_{INT} : is the transmit bandwidth of the interferer.

E.4.2.4.4 Probability for time collision

The probability for time collision, P_{time_col}, is given by:

$$P_{time\_col} = \text{transmitter duty cycle.} \qquad \text{(E.4.2.4.4.b)}$$

E.4.3 Cumulative probability of interference

Once the interference area is determined (minimum coupling loss translated into distance), a cumulative probability of interference by a single unit, P_{UNIT} , can be calculated as combined probability of the following uncorrelated events:

    a)   Probability of antenna beams (interferer and victim) crossing each other, P_{PAT_COL}, pattern collision probability;

    b)   Probability of frequency collision, P_{FREQ_COL};

    c)   Probability of interferer and victim colliding with each other in time domain, P_{TIME_COL}.

Also, one must assume a practical spatial density and calculate the corresponding total number of interferers in the area N_{INT_TOT} as described in Section 5.2.3 above.

The probability of becoming a victim of any one of the potential interferer-s in the area can be calculated as:

$$P_{INTF\_TOT} = 1 - \prod_{N_{INTF\_TOT(PAT\_COL)}} (1 - P_{TIME\_COL} \cdot P_{FREQ\_COL} \cdot P_{PAT\_COL}) \qquad \text{(6.2.5.a)}$$

The product designated by the pi notation in the equation (6.1) has two terms, when the Interferer's antenna is directional, which results in two interfering distances caused by the main beam and side-lobes respectively. Hence, the resulting formula for the total interference probability is:

$$P_{INTF\_TOT} = MIN(\frac{SPAN_{OVERLAP}}{SPAN_{VIC}}, (1 - (((1 - P_{TIME\_COL} \cdot P_{FREQ\_COL} \cdot P_{PAT\_COL\_MAIN})^{N_{INT\_MAIN}})$$
$$* (1 - P_{TIME\_COL} \cdot P_{FREQ\_COL} \cdot P_{PAT\_COL\_SIDELOBE})^{N_{INT\_SIDELOBE}})))) \qquad (4.3\,b)$$

E.4.3.1 Comments on calculations of interference probability

The probabilities of interference are calculated in the Excel worksheets in Annex E.6 and the results are presented in E.5.

Multiple columns per worksheet are related to various existing and proposed systems (Sigurd the meaning of this is unclear). Interference to different victims is covered in separate worksheets.
Simultaneous interference caused by co-located systems of different categories is not analysed by MCL.
The formulas used in each worksheet are presented in chapter E.xx and are consistent across the worksheets. Input data is entered on a separate input sheet. Each worksheet is organised in a similar manner, resulting in a set of sheets that is easy to compare, modify or expand by adding new sheets for other systems operating in the 863-870 MHz band.

Section E.5.2 presents the most relevant subset of Interference Probability calculations from E 6.

E.5.0   Presentation of calculated results

E.5.1   Deterministic method

E.5.1.1 Protection distances for blocking

The calculated protection ranges for blocking are given in a table below:

Victims	DVB-T QPSK	DVB-T 16 QAM	DVB-T 64 QAM	TETRA QPSK	SRD 15kHz	SRD 100kHz	SRD 250kHz	Microph 200kHz	Audio 300kHz	Co Audio 50kHz	FHSS 100KHz	FHSS 25kHz	DSSS 2MHz	DSSS 500kHz	RFID 200kHz	CT2 100kHz
Protection distances, m																
Prad = +10 dBm	4.2	3.7	2.3	1.5	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	2.8	0.9	2.8
Prad = +14 dBm	6.6	5.9	3.7	2.4	4.4	4.4	4.4	4.4	4.4	4.4	4.4	4.4	4.4	4.4	1.4	4.4
Prad = +27 dBm	18.4	17.4	13.2	10.5	14.6	14.6	14.6	14.6	14.6	14.6	14.6	14.6	14.6	14.6	7.6	14.6
Prad = +33 dBm	27.4	25.8	19.6	15.6	21.7	21.7	21.7	21.7	21.7	21.7	21.7	21.7	21.7	21.7	11.3	21.7

E.5.2   Probabilistic method

The interference calculations are performed for the selected scenarios. The results (interference probabilities) are calculated for each victim. In order to display the results of the study in a more informative manner, all results are grouped in the following separate graphs:

Interference Probabilities to and from existing Services,
Interference Probabilities to and from proposed Services.

The appropriate way of assessing interference in the band is to calculate the absolute interference probabilities for realistically deployed existing and proposed systems.

E.5.2.1 Protection distances.

A summary of co-channel protection distances is given in the tables below. In cases of non-overlapping frequencies an off-channel isolation is used. This may be caused for example by spectrum mask attenuation or adjacent channel selectivity.

Summary of maximum protection distances for URBAN indoor mounted interferers (km)

Interfering transmitters =>	SRD 1	SRD 2	SRD 3	Microph	Audio 1	Audio 2	SRD 4	SRD 5	SRD 6	SRD 7	SRD 8	SRD 9	SRD 10	SRD 11	RFID 1	RFID 2	RFID 3	Terminal	PABX
	NB	NB	Wideband	FM	FM	FM	FHSS 1	FHSS 2	FHSS 3	FHSS 4	DSSS 1	DSSS 2	DSSS 3	DSSS 4	ASK	ASK	ASK	FM	FM
	25kHz	100kHz	250 kHz	200kHz	300kHz	50kHz	100kHz	100kHz	100kHz	25kHz	600 kHz	600 kHz	600 kHz	2 MHz	200 kHz	200 kHz	200 kHz	100 kHz	100 kHz
	10 dBm	14 dBm	27 dBm	10 dBm	10 dBm	10 dBm	14 dBm	14 dBm	14 dBm	27 dBm	14 dBm	14 dBm	14 dBm	33 dBm	20 dBm	27 dBm	33 dBm	10 dBm	14 dbm
Victims below																			
Narrow band SRD BW=15 kHz	0.500	0.470	0.617	0.013	0.012	0.020	0.470	0.470	0.470	0.025	0.281	0.281	0.281	0.087	0.003	0.005	0.007	0.228	0.361
Narrow band SRD BW=25 kHz	0.361	0.470	0.617	0.013	0.012	0.016	0.470	0.470	0.470	0.017	0.281	0.281	0.281	0.025	0.006	0.009	0.013	0.228	0.361
Narrow band SRD BW=250 kHz	0.278	0.361	0.617	0.013	0.012	0.013	0.361	0.361	0.361	0.013	0.281	0.281	0.281	0.025	0.005	0.009	0.013	0.175	0.278
Rado Microphones	0.014	0.014	0.014	0.301	0.332	0.301	0.391	0.391	0.391	0.014	0.500	0.500	0.500	0.026	0.006	0.009	0.014	0.009	0.014
Wireless audio	0.012	0.012	0.012	0.269	0.269	0.269	0.349	0.349	0.349	0.012	0.287	0.287	0.287	0.007	0.005	0.008	0.012	0.008	0.012
Consumer audio	0.021	0.021	0.013	0.301	0.269	0.447	0.477	0.477	0.477	0.021	0.287	0.287	0.287	0.007	0.006	0.009	0.014	0.011	0.017
FHSS, BW 100 kHz	0.367	0.477	0.860	0.301	0.269	0.367	0.477	0.477	0.477	1.115	0.287	0.287	0.287	0.705	0.301	0.476	0.705	0.232	0.367
FHSS BW 25 kHz	0.087	0.059	0.045	0.048	0.043	0.072	1.648	1.648	1.648	0.087	0.991	0.991	0.991	2.438	0.021	0.033	0.048	0.803	1.269
DSSS, 500 kHz	0.003	0.003	0.003	0.003	0.003	0.003	0.094	0.094	0.094	0.221	0.094	0.094	0.094	0.232	0.140	0.221	0.327	0.046	0.073
DSSS, 2 MHz	0.010	0.010	0.010	0.010	0.010	0.010	0.276	0.276	0.276	0.763	0.276	0.276	0.276	0.803	0.409	0.647	0.957	0.135	0.213
RFID	0.002	0.003	0.006	0.002	0.002	0.002	0.260	0.260	0.260	0.500	0.190	0.190	0.190	0.469	0.385	0.500	0.585	0.126	0.200
CT2	0.016	0.016	0.013	0.013	0.012	0.016	0.470	0.470	0.470	1.115	0.281	0.281	0.281	2.438	0.500	0.658	0.974	0.008	0.013

Summary of maximum protection distances for URBAN outdoor mounted interferers (km)

Interfering transmitters =>	SRD 1	SRD 2	SRD 3	Microph	Audio 1	Audio 2	SRD 4	SRD 5	SRD 6	SRD 7	SRD 8	SRD 9	SRD 10	SRD 11	RFID 1	RFID 2	RFID 3	Terminal	PABX
	NB	NB	Wideband	FM	FM	FM	FHSS 1	FHSS 2	FHSS 3	FHSS 4	DSSS 1	DSSS 2	DSSS 3	DSSS 4	ASK	ASK	ASK	FM	FM
	25kHz	100kHz	250 kHz	200kHz	300kHz	50kHz	100kHz	100kHz	100kHz	25kHz	600 kHz	600 kHz	600 kHz	2 MHz	200 kHz	200 kHz	200 kHz	100 kHz	100 kHz
	10 dBm	14 dBm	27 dBm	10 dBm	10 dBm	10 dBm	14 dBm	14 dBm	14 dBm	27 dBm	14 dBm	14 dBm	14 dBm	33 dBm	20 dBm	27 dBm	33 dBm	10 dBm	14 dbm
Victims below																			
Narrow band SRD BW=15 kHz	0.751	0.658	1.187	0.019	0.017	0.029	0.658	0.658	0.658	0.048	0.396	0.396	0.396	0.167	0.004	0.007	0.010	0.321	0.507
Narrow band SRD BW=100 kHz	0.507	0.658	1.187	0.019	0.017	0.023	0.658	0.658	0.658	0.033	0.396	0.396	0.396	0.048	0.008	0.013	0.019	0.321	0.507
Narrow band SRD BW=250 kHz	0.391	0.507	1.187	0.019	0.017	0.018	0.507	0.507	0.507	0.025	0.396	0.396	0.396	0.048	0.008	0.012	0.018	0.247	0.391
Rado Microphones	0.027	0.027	0.025	0.580	0.516	0.580	0.753	0.753	0.753	0.027	0.551	0.551	0.551	0.014	0.011	0.018	0.027	0.017	0.027
Wireless audio	0.020	0.020	0.020	0.425	0.425	0.425	0.551	0.551	0.551	0.020	0.453	0.453	0.453	0.011	0.008	0.013	0.020	0.012	0.020
Consumer audio	0.040	0.033	0.025	0.580	0.516	0.859	0.916	0.916	0.916	0.040	0.551	0.551	0.551	0.014	0.011	0.018	0.027	0.021	0.033
FHSS, BW 100 kHz	0.706	0.916	1.653	0.580	0.516	0.706	0.916	0.916	0.916	2.144	0.551	0.551	0.551	1.356	0.580	0.916	1.356	0.446	0.706
FHSS, BW 25 kHz	0.167	0.113	0.087	0.093	0.083	0.138	3.169	3.169	3.169	0.167	1.905	1.905	1.905	4.688	0.040	0.063	0.093	1.544	2.440
DSSS, 500 kHz	0.006	0.006	0.006	0.006	0.006	0.006	0.181	0.181	0.181	0.424	0.181	0.181	0.181	0.446	0.268	0.424	0.628	0.088	0.140
DSSS, 2 MHz	0.019	0.019	0.019	0.019	0.019	0.019	0.532	0.532	0.532	1.467	0.532	0.532	0.532	1.543	0.787	1.243	1.840	0.259	0.409
RFID	0.004	0.003	0.007	0.003	0.002	0.003	0.325	0.325	0.325	0.760	0.238	0.238	0.238	0.585	0.481	0.760	1.124	0.158	0.250
CT2	0.023	0.023	0.018	0.019	0.017	0.023	0.658	0.658	0.658	2.144	0.396	0.396	0.396	4.688	0.800	1.265	1.872	0.011	0.018

Summary of maximum protection distances for URBAN outdoor mounted interferers (km), I/N = 10 dB																		
Interfering transmitters =>	SRD 1	SRD 2	SRD 3	Microph	Audio 1	Audio 2	SRD 4	SRD 5	SRD 6	SRD 7	SRD 8	SRD 9	SRD 10	SRD 11	RFID 1	RFID 2	RFID 3	Terminal	PABX
	NB	NB	Wideband	FM	FM	FM	FHSS 1	FHSS 2	FHSS 3	FHSS 4	DSSS 1	DSSS 2	DSSS 3	DSSS 4	ASK	ASK	ASK	FM	FM
	25kHz	100kHz	250 kHz	200kHz	300kHz	50kHz	100kHz	100kHz	100kHz	25kHz	600 kHz	600 kHz	600 kHz	2 MHz	200 kHz	200 kHz	200 kHz	100 kHz	100 kHz
	10 dBm	14 dBm	27 dBm	10 dBm	10 dBm	10 dBm	14 dBm	14 dBm	14 dBm	27 dBm	14 dBm	14 dBm	14 dBm	33 dBm	20 dBm	27 dBm	33 dBm	10 dBm	14 dbm
Victims below																			
Narrow band SRD BW=15 kHZ	0.391	0.342	0.617	0.010	0.009	0.015	0.342	0.342	0.342	0.025	0.206	0.206	0.206	0.087	0.002	0.004	0.005	0.167	0.264
Narrow band SRD BW=100 kHz	0.264	0.342	0.617	0.010	0.009	0.012	0.342	0.342	0.342	0.017	0.206	0.206	0.206	0.025	0.004	0.007	0.010	0.167	0.264
Narrow band SRD BW=250 kHz	0.203	0.264	0.617	0.009	0.009	0.009	0.264	0.264	0.264	0.013	0.206	0.206	0.206	0.025	0.004	0.006	0.009	0.129	0.203
Rado Microphones	0.014	0.014	0.013	0.301	0.269	0.301	0.391	0.391	0.391	0.014	0.287	0.287	0.287	0.007	0.006	0.009	0.014	0.009	0.014
Wireless audio	0.010	0.010	0.010	0.221	0.221	0.221	0.287	0.287	0.287	0.010	0.236	0.236	0.236	0.006	0.004	0.007	0.010	0.006	0.010
Consumer audio	0.021	0.017	0.013	0.301	0.269	0.447	0.477	0.477	0.477	0.021	0.287	0.287	0.287	0.007	0.006	0.009	0.014	0.011	0.017
FHSS, BW 100 kHz	0.367	0.477	0.860	0.301	0.269	0.367	0.477	0.477	0.477	1.115	0.287	0.287	0.287	0.705	0.301	0.476	0.705	0.232	0.367
FHSS, BW 25 kHz	0.087	0.059	0.045	0.048	0.043	0.072	1.648	1.648	1.648	0.087	0.991	0.991	0.991	2.438	0.021	0.033	0.048	0.803	1.269
DSSS, 500 kHz	0.003	0.003	0.003	0.003	0.003	0.003	0.094	0.094	0.094	0.221	0.094	0.094	0.094	0.232	0.140	0.221	0.327	0.046	0.073
DSSS, 2 MHz	0.010	0.010	0.010	0.010	0.010	0.010	0.276	0.276	0.276	0.763	0.276	0.276	0.276	0.803	0.409	0.647	0.957	0.135	0.213
RFID	0.002	0.003	0.004	0.003	0.001	0.001	0.325	0.325	0.325	0.760	0.238	0.238	0.238	0.585	0.481	0.760	1.124	0.158	0.250
CT2	0.012	0.012	0.009	0.010	0.009	0.012	0.342	0.342	0.342	1.115	0.206	0.206	0.206	2.438	0.416	0.658	0.974	0.006	0.009

Summary of maximum protection distances for URBAN indoor mounted interferers (km), I/N = 10 dB																		
Interfering transmitters =>	SRD 1	SRD 2	SRD 3	Microph	Audio 1	Audio 2	SRD 4	SRD 5	SRD 6	SRD 7	SRD 8	SRD 9	SRD 10	SRD 11	RFID 1	RFID 2	RFID 3	Terminal	PABX
	NB	NB	Wideband	FM	FM	FM	FHSS 1	FHSS 2	FHSS 3	FHSS 4	DSSS 1	DSSS 2	DSSS 3	DSSS 4	ASK	ASK	ASK	FM	FM
	25kHz	600kHz	250 kHz	200kHz	300kHz	50kHz	100kHz	100kHz	100kHz	25kHz	600 kHz	600 kHz	600 kHz	2 MHz	200 kHz	200 kHz	200 kHz	100 kHz	100 kHz
	10 dBm	14 dBm	27 dBm	10 dBm	10 dBm	10 dBm	14 dBm	14 dBm	14 dBm	27 dBm	14 dBm	14 dBm	14 dBm	33 dBm	20 dBm	27 dBm	33 dBm	10 dBm	14 dbm
Victims below																			
Narrow band SRD BW=15 kHZ	0.278	0.243	0.440	0.007	0.006	0.010	0.243	0.243	0.243	0.013	0.146	0.146	0.146	0.045	0.002	0.002	0.004	0.118	0.187
Narrow band SRD BW=25 kHZ	0.187	0.243	0.440	0.007	0.006	0.008	0.243	0.243	0.243	0.009	0.146	0.146	0.146	0.013	0.003	0.005	0.007	0.118	0.187
Narrow band SRD BW=250 kHz	0.144	0.187	0.440	0.007	0.006	0.007	0.187	0.187	0.187	0.007	0.146	0.146	0.146	0.013	0.003	0.004	0.007	0.091	0.144
Rado Microphones	0.007	0.007	0.007	0.157	0.172	0.157	0.204	0.204	0.204	0.007	0.273	0.273	0.273	0.013	0.003	0.005	0.007	0.005	0.007
Wireless audio	0.006	0.006	0.006	0.140	0.140	0.140	0.181	0.181	0.181	0.006	0.149	0.149	0.149	0.004	0.003	0.004	0.006	0.004	0.006
Consumer audio	0.011	0.009	0.007	0.157	0.140	0.232	0.248	0.248	0.248	0.011	0.149	0.149	0.149	0.004	0.003	0.005	0.007	0.006	0.009
FHSS, BW 100 kHz	0.191	0.248	0.447	0.157	0.140	0.191	0.248	0.248	0.248	0.580	0.149	0.149	0.149	0.367	0.157	0.248	0.367	0.121	0.191
FHSS, BW 25 kHz	0.045	0.031	0.024	0.025	0.022	0.037	0.857	0.857	0.857	0.045	0.515	0.515	0.515	1.268	0.011	0.017	0.025	0.418	0.660
DSSS, 500 kHz	0.002	0.002	0.002	0.002	0.002	0.002	0.049	0.049	0.049	0.115	0.049	0.049	0.049	0.121	0.073	0.115	0.170	0.024	0.038
DSSS, 2 MHz	0.005	0.005	0.005	0.005	0.005	0.005	0.144	0.144	0.144	0.397	0.144	0.144	0.144	0.417	0.213	0.336	0.498	0.070	0.111
RFID	0.001	0.003	0.003	0.002	0.001	0.001	0.260	0.260	0.260	0.500	0.190	0.190	0.190	0.469	0.385	0.500	0.585	0.126	0.200
CT2	0.008	0.008	0.007	0.007	0.006	0.008	0.243	0.243	0.243	0.580	0.146	0.146	0.146	1.268	0.296	0.469	0.506	0.004	0.007

E.5.2.2   Cumulative probability of interference

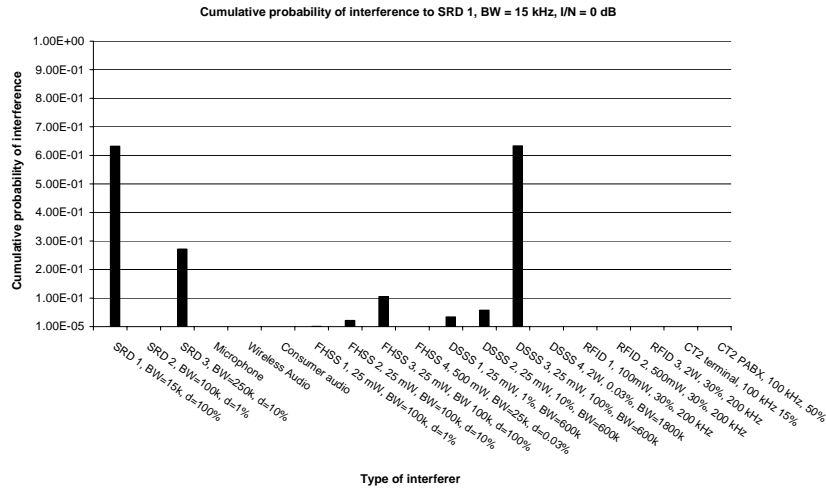The cumulative probability of interference to different types of victims is given in the figures below.

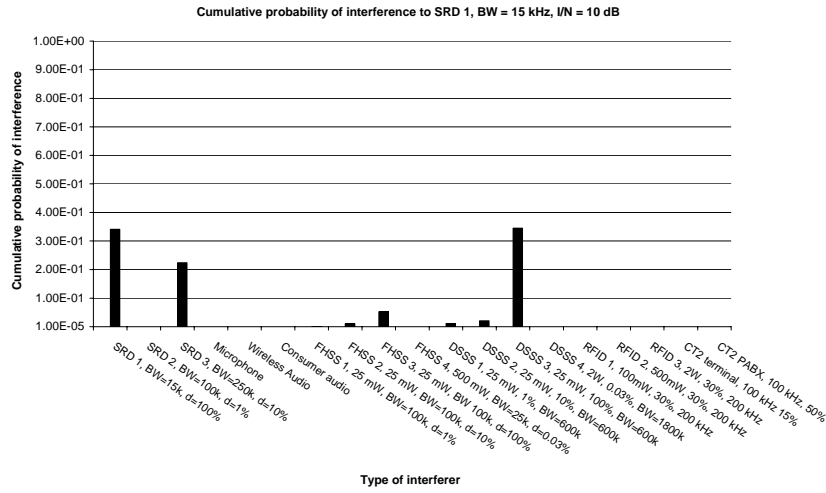**Figure E.5.2.2.1 Cumulative probability of interference to SRD 1 at I/N = 0 dB**

Cumulative probability of interference to SRD 1, BW = 15 kHz, I/N = 10 dB

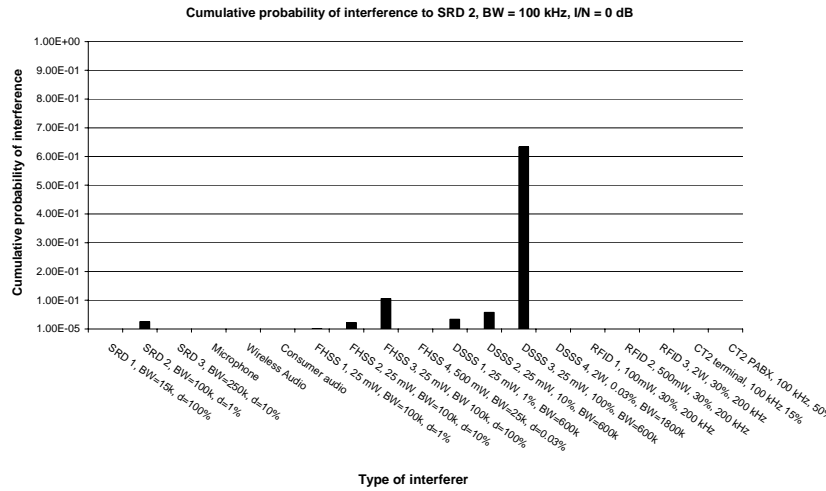**Figure E.5.2.2.2 Cumulative probability of interference to SRD 1 at I/N = +10 dB**

Cumulative probability of interference to SRD 2, BW = 100 kHz, I/N = 0 dB

Figure E.5.2.2.3 Cumulative probability of interference to SRD 2 at I/N = 0 dB
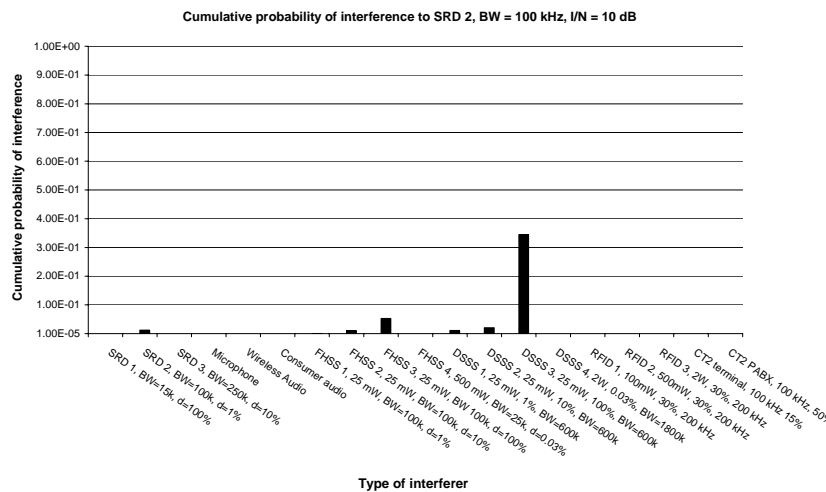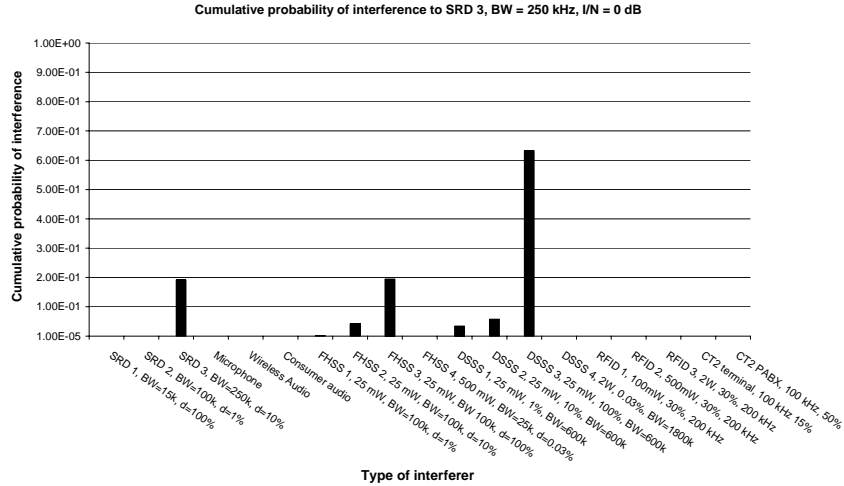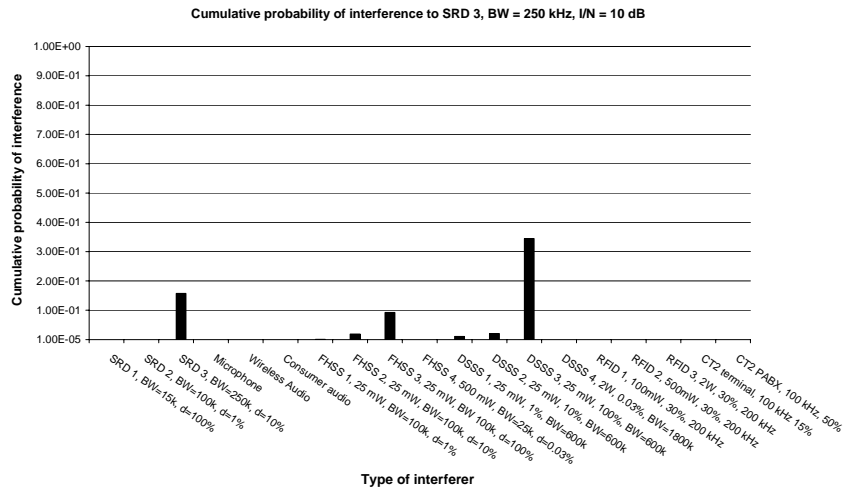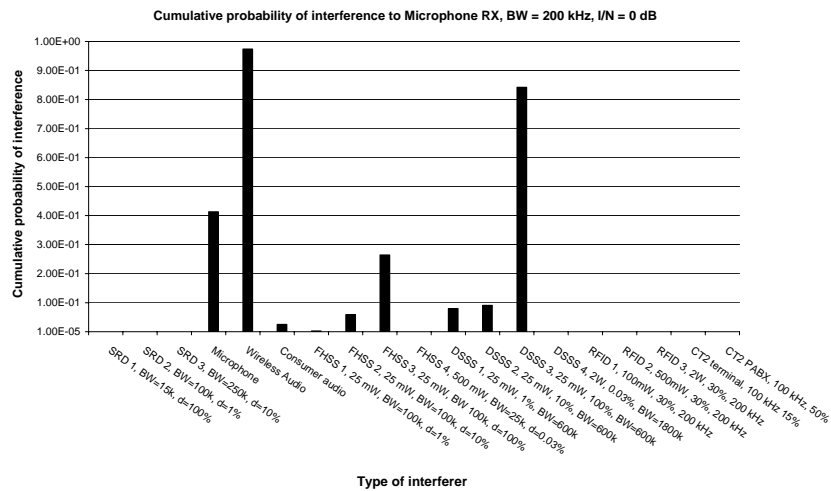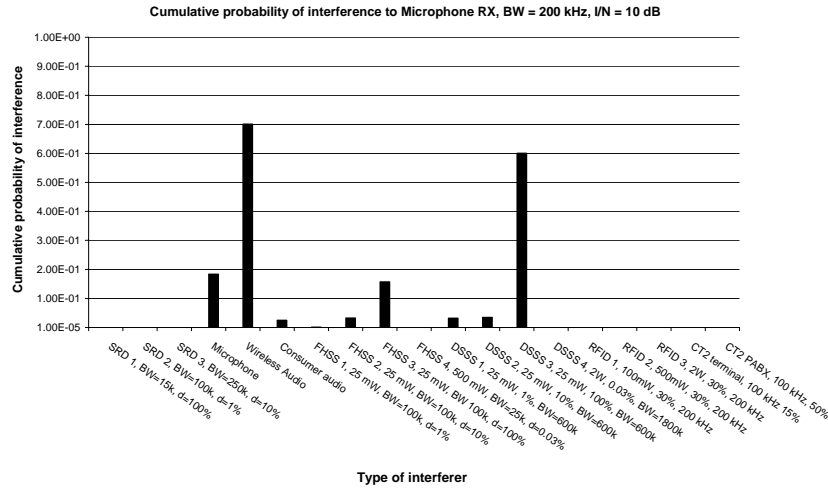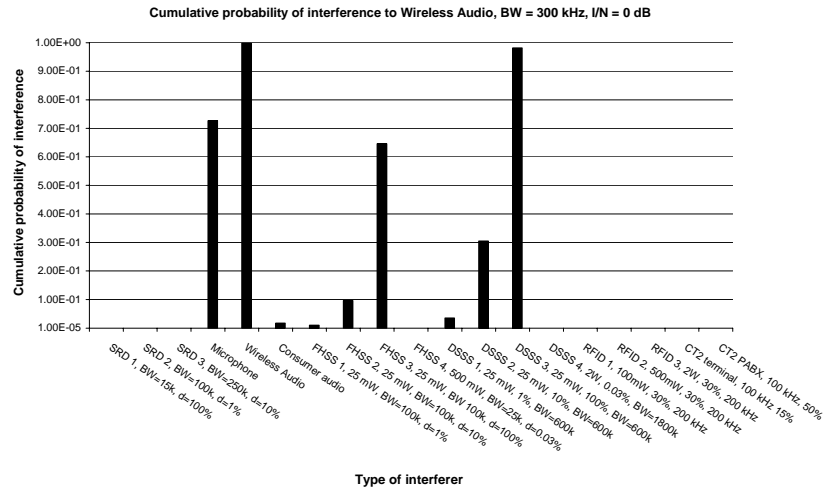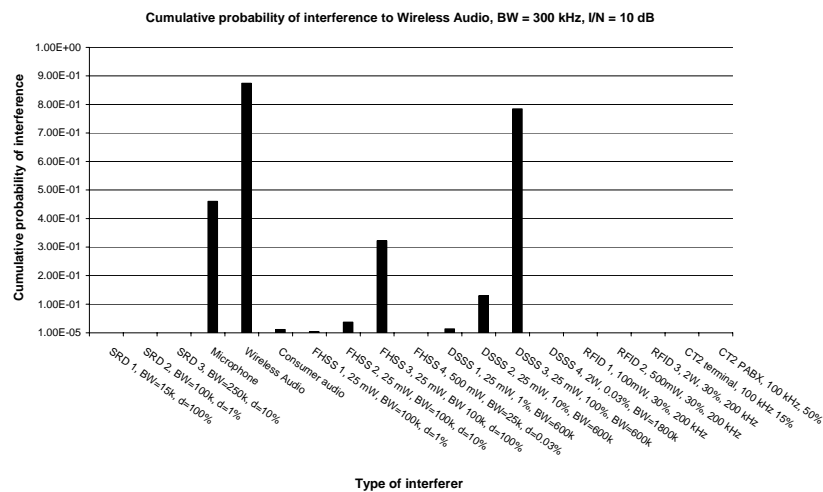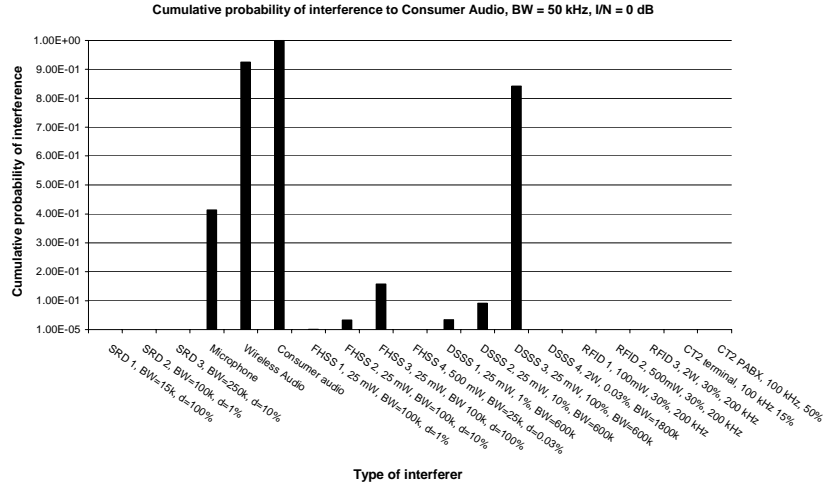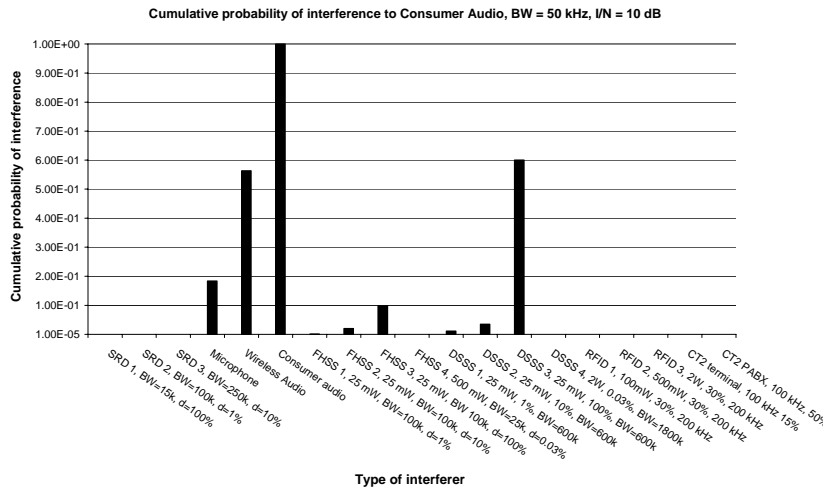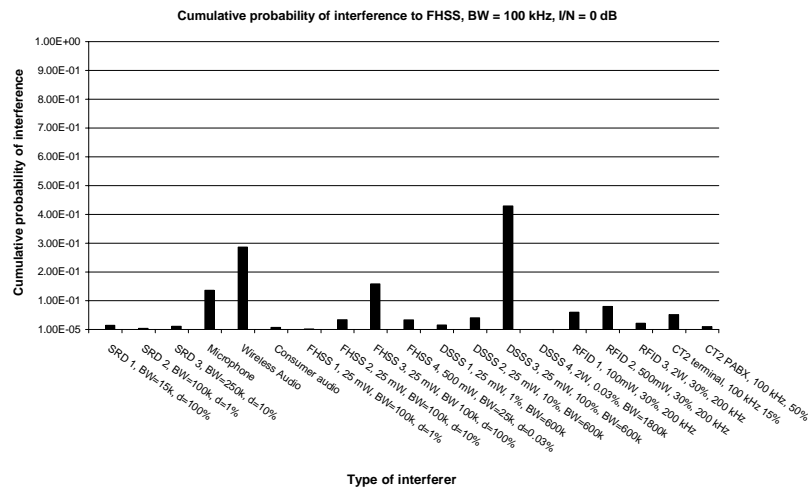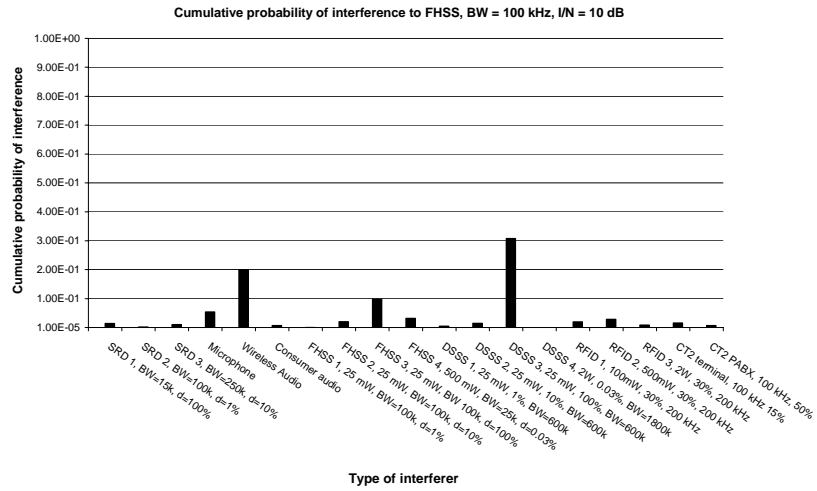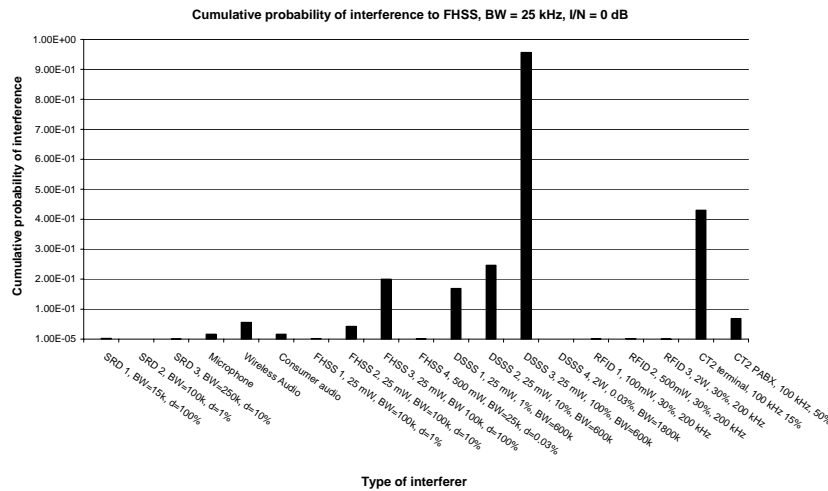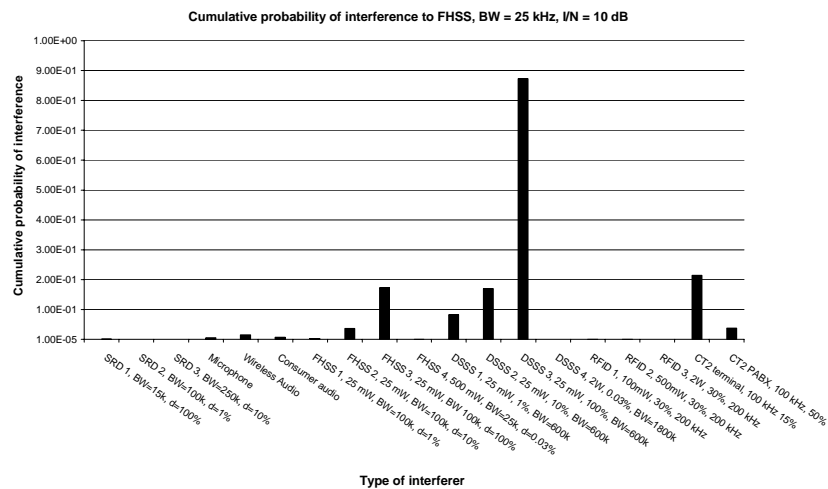
Cumulative probability of interference to SRD 2, BW = 100 kHz, I/N = 10 dB

Figure E.5.2.2.4 Cumulative probability of interference to SRD 2 at I/N = +10 dB

Cumulative probability of interference to SRD 3, BW = 250 kHz, I/N = 0 dB

Figure E.5.2.2.5 Cumulative probability of interference to SRD 3 at I/N = 0 dB

Cumulative probability of interference to SRD 3, BW = 250 kHz, I/N = 10 dB

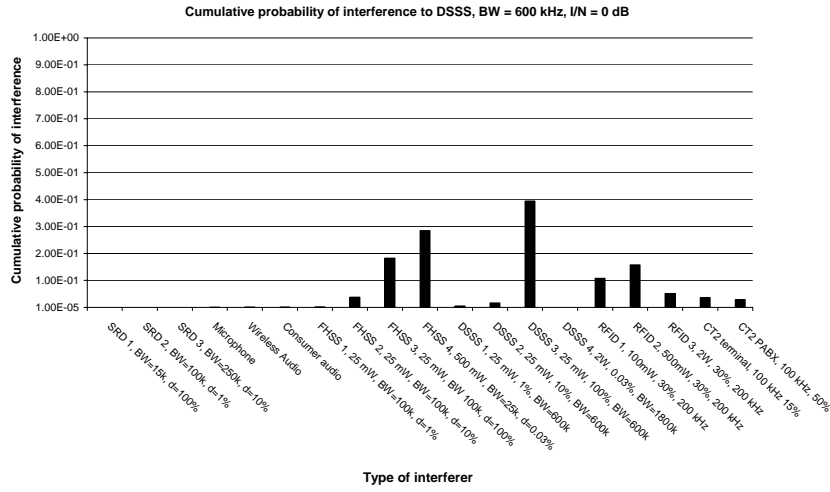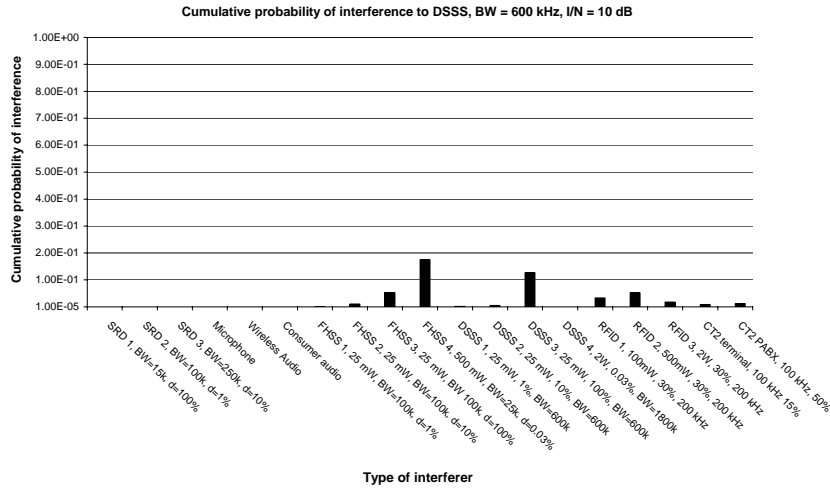**Figure E.5.2.2.6 Cumulative probability of interference to SRD 3 at I/N = +10 dB**

Cumulative probability of interference to Microphone RX, BW = 200 kHz, I/N = 0 dB

Figure E.5.2.2.7 Cumulative probability of interference to Radio Microphones at I/N = 0 dB

Cumulative probability of interference to Microphone RX, BW = 200 kHz, I/N = 10 dB

Figure E.5.2.2.8 Cumulative probability of interference to Radio Microphones at I/N = +10 dB

Cumulative probability of interference to Wireless Audio, BW = 300 kHz, I/N = 0 dB

Figure E.5.2.2.9. Cumulative probability of interference to Wireless Audio at I/N = 0 dB

Cumulative probability of interference to Wireless Audio, BW = 300 kHz, I/N = 10 dB

Figure E.5.2.2.10. Cumulative probability of interference to Wireless Audio at I/N = +10 dB

Figure E.5.2.2.11. Cumulative probability of interference to Consumer Audio at I/N = 0 dB

Figure E.5.2.2.12. Cumulative probability of interference to Consumer Audio at I/N = +10 dB

Figure E.5.2.2.13. Cumulative probability of interference to FHSS (100 kHz) at I/N = 0 dB

Figure E.5.2.2.14. Cumulative probability of interference to FHSS (100 kHz) at I/N = +10 dB
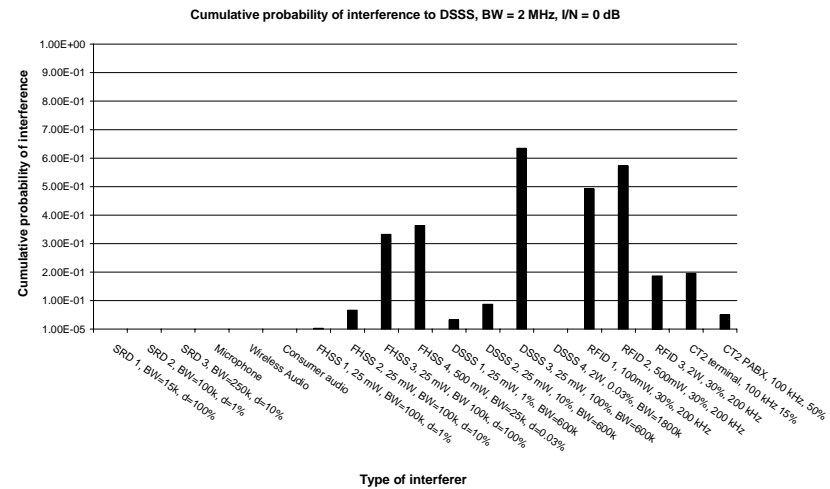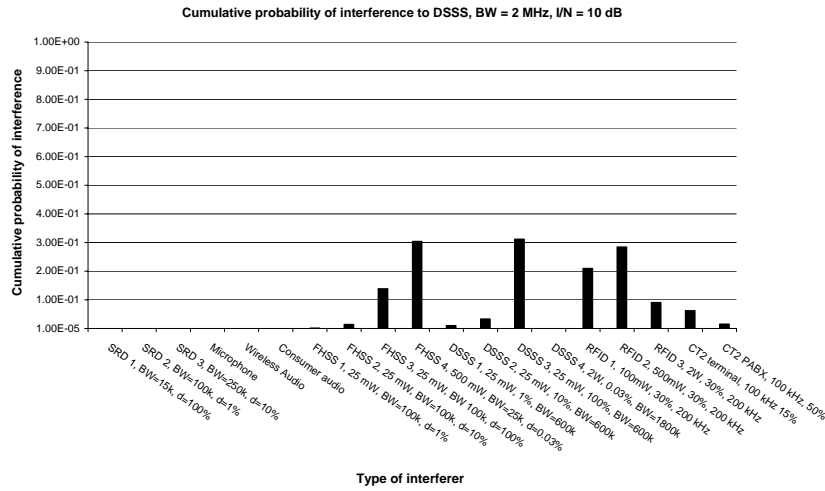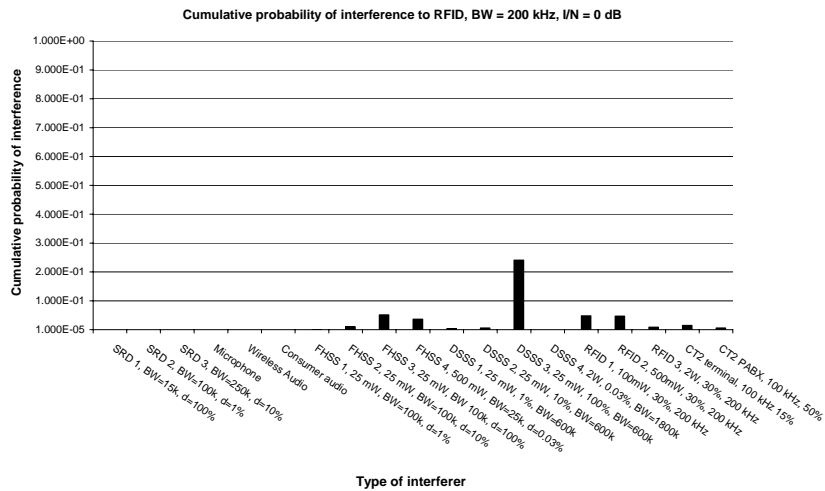

Figure E.5.2.1.15. Cumulative probability of interference to FHSS (25 kHz) at I/N = 0 dB

Figure E.5.2.2.16. Cumulative probability of interference to FHSS (25 kHz) at I/N = +10 dB

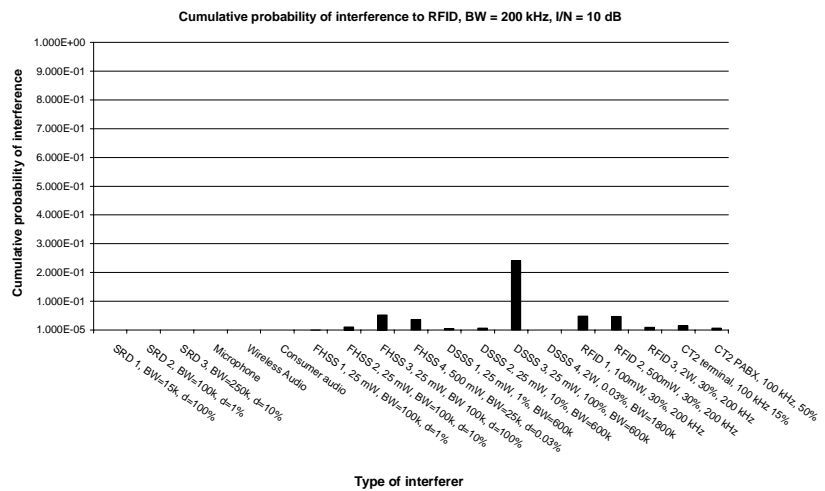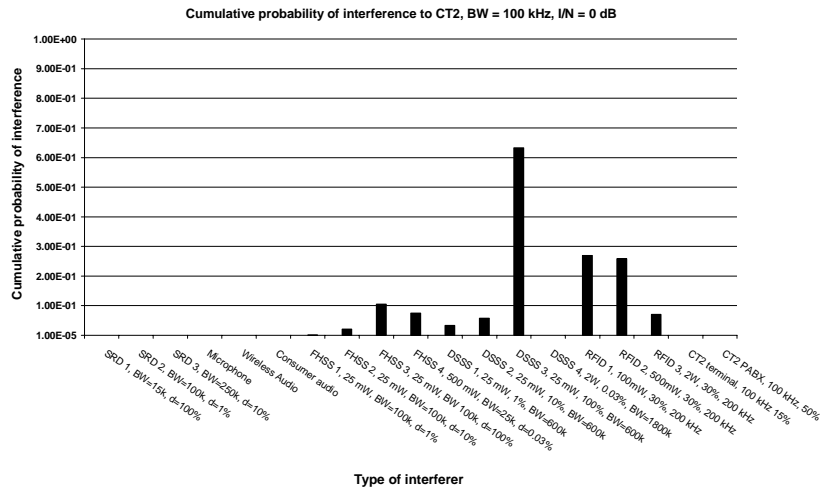**Figure E.5.2.2.17. Cumulative probability of interference to DSSS (600 kHz) at I/N = 0 dB**

Figure E.5.2.2.18. Cumulative probability of interference to DSSS (600 kHz) at I/N = +10 dB

Figure E.5.2.2.19. Cumulative probability of interference to DSSS (2 MHz) at I/N = 0 dB

Figure E.5.2.2.20. Cumulative probability of interference to DSSS (2 MHz) at I/N = +10 dB

Figure E.5.2.2.21. Cumulative probability of interference to RFID at I/N = 0 dB

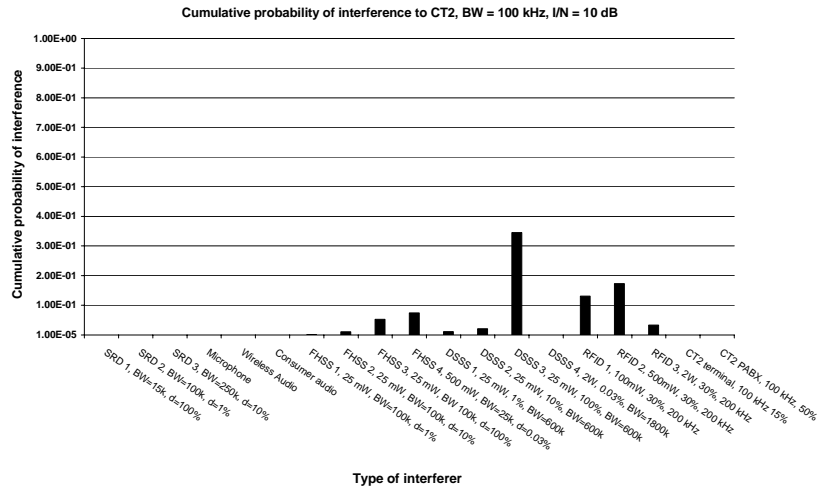**Figure E.5.2.2.22. Cumulative probability of interference to RFID at I/N = +10 dB**

Cumulative probability of interference to CT2, BW = 100 kHz, I/N = 0 dB

Figure E.5.2.2.23. Cumulative probability of interference to CT 2 at I/N= 0 dB

Cumulative probability of interference to CT2, BW = 100 kHz, I/N = 10 dB

Figure E.5.2.2.24. Cumulative probability of interference to CT 2 at I/N = +10 dB

E.6   Excel spread sheets for interference calculations

See separate attachment

ANNEX F   SOCIAL ALARMS

Social Alarm Systems are protected as an application by ERC/DEC (97)06 [8]

The interpretation of this decision, applied to this study, is as follows:

Since:
   –   no existing applications use sub band d) of Annex 7 of ERC/REC 70-03 [9]
   –   new applications are not intended to transmit continuously
   –   this study assumes that the duty cycle of all new applications shall be kept to a necessary minimum to
       avoid harmful interference to other users with particular consideration given to Social Alarm Systems.

Therefore the study has been carried out using the applicable parameters and their limits.

It has been taken into consideration that:
   –   the intended use of this application is within a building (mostly within a single apartment, i.e. the required
       range is usually less than 25 m),
   –   the usable sensitivity of the receiver is –107 dBm,
       the radiated output power of the transmitter is only 1 mW (0 dBm) e.r.p.
   –   the receivers of Social Alarm Systems comply with all of the requirements of EN 300 220-1 [14] and to the
       supplementary clauses of EN 300 220-2 [15] even if they are not yet mandatory.

The MCL calculations and SEAMCAT simulations do NOT take into account that
   –   the transmitter of the social alarm system is active for no more than once a day
       and
   –   the alarm code (ID) is transmitted several times within its transmission time of 30 seconds.

To avoid the need for propagation models different to the agreed Extended HATA (SRD) model (as used for all
other SEAMCAT simulations), a scenario was assumed in which the Social Alarm System has to be fully functional.

This scenario is based on the requirements of EN 300 220 [17] and uses:-
   –   sensitivity   =   -107 dBm
   –   adjacent channel rejection   =   60 dB
   –   blocking response   =   84 dB
   –   received input power   =   -104 dBm

Since the received power level is 3 dB above the required sensitivity, the simulated results are calculated using the
same measurement procedures as defined in the standard and no propagation model for the victim link is needed.

ANNEX G   DSSS

ANNEX G.1   General description for generic system

In a Direct Sequence Spread Spectrum system, the signal is spread according to a pseudo random (PR) code or sequence. To a receiver that does not know the code, the signal appears as noise. But a receiver that does know the code is able to de-spread the signal and extract the data stream.

One of the key parameters is the spreading ratio. This, broadly speaking, is the ratio by which the bandwidth is spread compared to conventional transmission of the same data stream.   The spreading ratio governs the amount by which it is possible to reduce the spectral density. The processing gain is the measure of how well the receiver can reconstruct the signal and separate it from noise or from another signal.

It is usually possible to overlay a DSSS signal with another spread spectrum or conventional signal, thus achieving spectrum re-use without requiring co-operation between users. Isolation between the different users is achieved by selection of different codes, so called Code Division Multiple Access (CDMA). In any given implementation, the number of suitable codes is finite, in the same way that frequency channels or time slots are finite in a conventional arrangement.

The distinguishing features of DSSS are:

-          The transmitted signal is difficult to distinguish from wideband Gaussian noise
-          There is a significant spreading ratio in the transmitter
-          There is a corresponding processing gain in the receiver.

In a DSSS transmitter the signal is spread by multiplication by a pseudo random code. The code has a long repeat interval and a fast "chip" rate.   The signal is spread out over a bandwidth determined by the chip rate.   In an optimized system the repeat rate is chosen to interact with the data rate to ensure that the spreading is finely grained and the resulting spectrum is noise like. In the general case, the spreading ratio is the chip rate divided by the data rate.

In the receiver the incoming signal is multiplied by the pseudo random code. When the codes are both identical and synchronized a spread signal is turned back into an unspread one and may be detected and demodulated. At the same time, narrow band signals are turned into spread signals; noise and other spread spectrum signals are turned into noise and noise like signals. Therefore in the receiver the wanted signal can be extracted from a background of noise and other signals. The processing gain associated with this extraction cannot exceed the spreading ratio and in a well designed receiver will be equal to it.

PR SEQUENCE   PR SEQUENCE

A generic DSSS System

Equivalent NB signal

Spectrum of DSSS Transmission
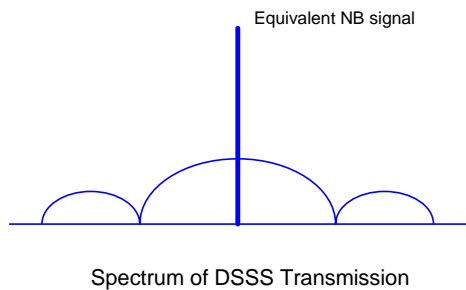
Compatibility

Because of the noise-like features of DSSS, compatibility issues between systems are amenable to a simple analysis.

At low or moderate signal levels, and with systems overlapping in frequency, the following general rules apply:

1. For a spread spectrum interferer and a conventional victim, the interferer may be treated as a co-channel noise source.
2. For a conventional interferer and a spread spectrum victim, the interference energy is the same as in two similar co-channel systems, but reduced by the processing gain of the spread spectrum receiver.
3. For a spread interferer and a spread victim, if the operating bands coincide, then it reduces to the same as 2 above.

Blocking

At higher signal levels, non-linear effects must be considered. If the receiver front-end bandwidth is large, then all or most of a spread spectrum signal may be captured. The front-end circuits are then exposed to the same peak signal levels as they would be from a conventional interferer. In this situation, the blocking effects of a spread spectrum transmission are exactly the same as those from a non-spread transmission.

Generic DSSS in the 863 to 870 MHz band

Consider a DSSS transmitter operating over the whole 863 to 870 MHz band. Assume further that it achieves the optimum spreading function and distributes the power evenly across the 7 MHz available.

A conventional receiver will receive, as unwanted interference, a proportion of the spread signal according to the bandwidth of the conventional receiver. In the case of a receiver in a 25 kHz channel with a 15 kHz receiver bandwidth, the coupling ratio is:

$$15 \text{ kHz} / 7 \text{ MHz} = 1/447 = -26.7 \text{ dB}$$

This is the best possible case, with an ideal DSSS system and the narrowest likely conventional receiver. There is only 27 dB isolation between the two systems.

In the case of wider SRD receiver bandwidths the coupling ratios are correspondingly reduced.

Conventional Receiver Bandwidth kHz	Coupling ratio from 7 MHz DSSS Tx dB
15	**-26.7**
50	-21.5
100	-18.5
200	-15.4
250	-14.5
300	-13.7

TABLE G 1

The ability of a spread spectrum receiver to reject a conventional transmitter signal depends on the signal or data bandwidth of the spread spectrum system. Assuming a good spread spectrum receiver with an effective noise bandwidth equal to the data rate, then we get the following:

DSSS system Data Rate (kbps)	Coupling ratio from conventional Tx to 7 MHz DSSS Rx (dB)
15	**-26.7**
50	-21.5
100	-18.5
200	-15.4
250	-14.5
300	-13.7

Table G 2

Note that these coupling ratios, or isolations, are much lower than the separations or isolations achieved by conventional frequency separation and filtering. This is a consequence of only having 7 MHz to spread over. If the spreading is restricted to less than the full 863 to 870 MHz, or if parts of the band are prohibited (e.g. to protect social alarms) then the isolations are reduced further.

MCL Spreadsheet

In the MCL Spreadsheet four DSSS systems were analysed.
- DSSS1 is a generic system of 25 mW power spread over 500 kHz at 1% duty cycle.
- DSSS2 is a generic system of 25 mW power spread over 500 kHz at 10% duty cycle.
- DSSS3 is a generic system of 25 mW power spread over 500 kHz at 100% duty cycle.
- DSSS4 is an application specific system.

This is described further in Annex H clause H2.

Annex G.2   Example for an SRD using DSSS

Characteristics of DSSS TLSI Transponder operating in the band 865-868 MHz

Technical Information

The principles of operation of the system are as follows.

The transmission of the spread spectrum signal from the transponder (uplink) is triggered either by a predefined event transferred to the device via physical connection (e.g. unauthorized opening of the door or box, activation of vibration of impact sensors etc.) or remotely by an interrogation signal (narrow-band paging) sent by a distant operator and addressed to the specific device (downlink).

Several remote base stations receive the spread spectrum transmission from the transponder. The base stations perform very accurate measurement of the time of arrival of the signal and send this information to the Control Center. The Center's computer calculates the location of the device using Differential Time of Arrival (DTOA) algorithms, and provides this location information to the operator or another user. Single uplink transmission is adequate to perform reliable location of the device.

The downlink from the base station utilizes the standard paging channel and is not part of this discussion.
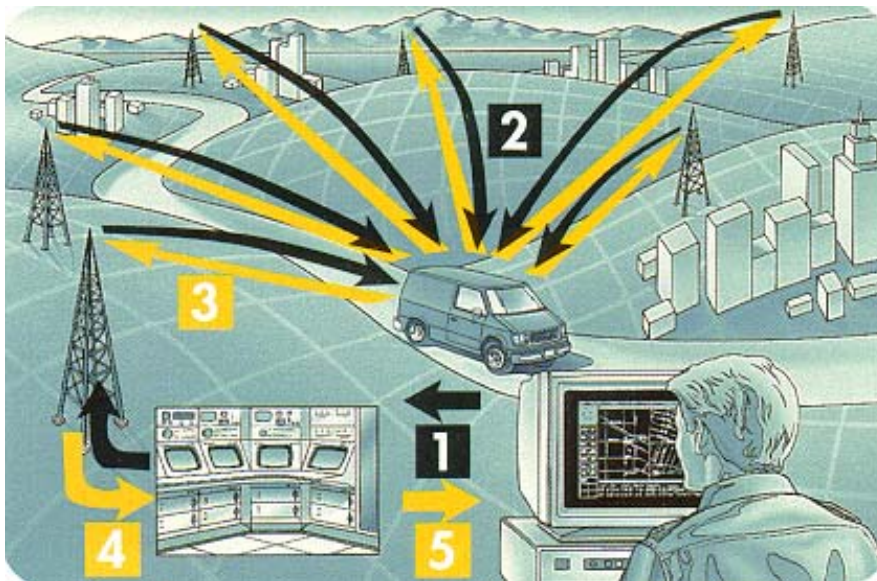

Figure G.2.1 Block diagram

The Uplink DSSS transmission is initiated by the transponder either by a predefined event or by request:
- The Uplink signal (3) is received by several Base Stations where accurate TOA is measured and transferred to the Control Centre (4).
- The Control Centre initiates the interrogation by Downlink (1 – 2).
- The Downlink transmission to interrogate the transponder is a standard paging signal from the base station and utilizes a separate frequency band.
- The Control Centre's computer utilizes DTOA (Differential TOA) algorithms for accurate determination of the location and provides this information to the operator (5).
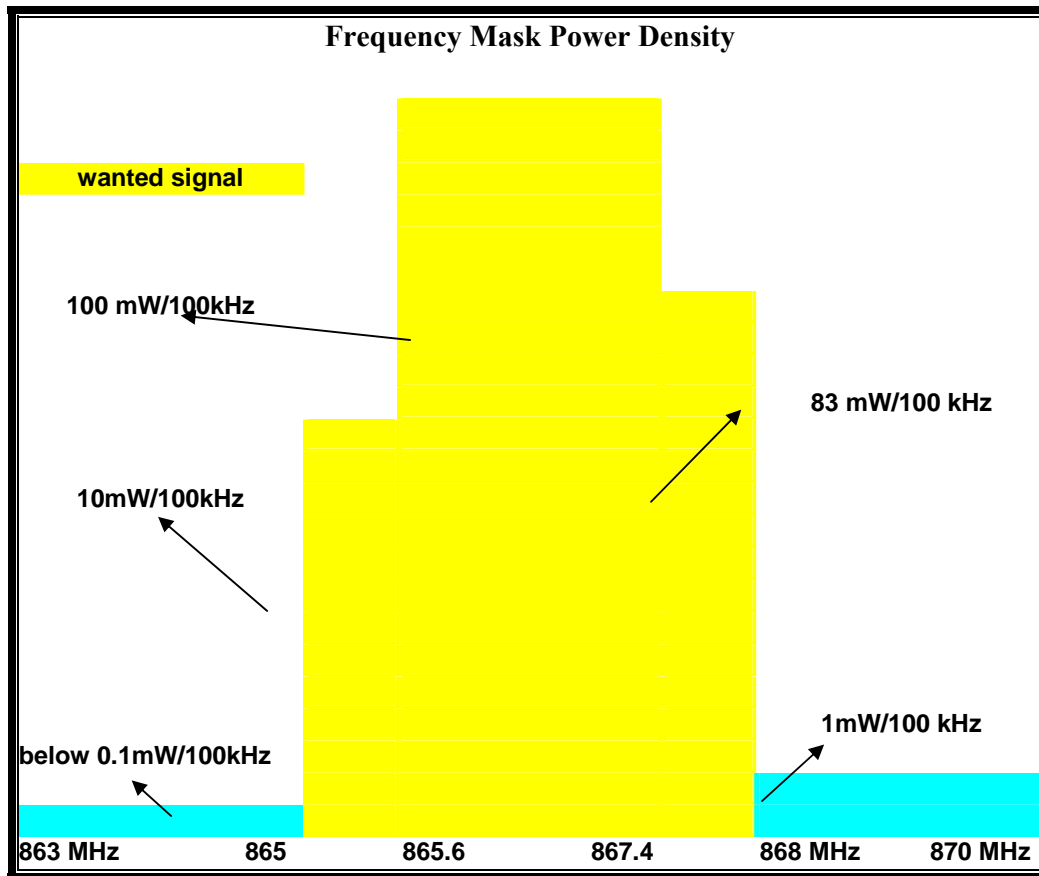
Note: 1, 4 and 5 are wire-line connections

Figure G.2.2 Power density

Estimated number of DSSS transponders (worst condition)

Assume a city with a population of 5 million people and about 2 million cars. An optimistic penetration rate after a few years of operation into the vehicle market will be about 5% (In Israel, for example, with about 2 Million cars, after 5 years of operation of the TLSI system there are 140,000 cars equipped with a DSSS transponder, representing a penetration of about 7%. It should be mentioned that the circumstances for the installation of such equipment in Israel is extremely beneficial, due to encouragement, marketing and subsidy by the insurance companies). In addition to the vehicle transponders we will assume an equal number of non-vehicle transponders. This brings the total number of transponders within the postulated city area to 200,000. The relevant area of the city will be assumed to be 2,000 sq. km, which represents a circle with a radius of about 25 km. The number of receiving base stations covering the area will be around 20 in addition to 6 –7 Paging Transmitters. It is assumed that the transponders are randomly spread over this area, giving an average of 100 location units per square kilometre.

Estimated number of active transponders (worst condition):

In the TLSI system transmissions from a transponder are caused by an event, which is defined as an attempt to steal an asset equipped with this device. In the vehicle market, theft of 3% annually of an overall fleet is considered high. This figure is used in the analysis.

There is no authoritative statistical data regarding the theft of non-vehicle assets. Furthermore there is no known comparable TLSI system used for such an application on a mass scale. The same annual figure of a 3% "theft rate" is also assumed for this market.

Based on the above estimates 6,000 theft "events" will be reported each year by the 200,000 strong customer base within the defined area. Randomly spread over the year, this gives around 17 events each day.

Upon the occurrence of an "event" a transponder will send a single 26-millisecond transmission of a spread spectrum signal. This will be followed by infrequent interrogations by the relevant location units for further monitoring of its movements. This will continue until completion of the recovery mission. Based on experience gained over several years of successful operation typically 100 interrogations are necessary for the recovery of each vehicle. The time delay between consecutive interrogations can range from few seconds to several hours. Assuming that all 100 interrogations are performed during the same day, the total number of interrogations per day is 1,700. In other words each day 1,700 transmissions of 26 milliseconds are made within an area of 25 km radius. This equates to a total transmission time of 44.2 seconds per day. It is reasonable to assume that the majority of theft attempts are performed during a 12 hour period. This gives an average of one 26 millisecond transmission every 25 seconds, occurring at a random location within an area of 2,000 sq. km. Thus on average, the number of activated stolen assets per day will be less than one per 100 sq. km.

Limitation of the duty cycle of the transponders

The sub clause above demonstrates the low number of active transponders within a given area. In order however to assure interference free operation an automatic limit of 0.03% is imposed on the duty cycle of each transponder.

Advantage of the use of DSSS and DTOA

Current solutions to the location of stolen items are often susceptible to radio jamming. If such systems should be widely installed, they could be subjected to "electronic warfare" by thieves, which would largely negate their value.

DTOA location technology using DSSS communication is substantially immune to jamming. In addition it also permits the location of objects in dense urban areas and inside buildings.

ANNEX H   GENERIC FHSS

H.1 General description

In a FHSS system the transmitter and the receiver hop in synchronism from one channel to another. The hop pattern will be a pseudo random sequence covering a large number of channels. The transmitted energy is thus shared out over a large bandwidth, but the transmitter to receiver link can still appear as a narrow band link.

The hop rate does not affect the occupied bandwidth, but is nevertheless a crucial parameter. It is important to distinguish between slow hopping and fast hopping. A slow hopper is one that hops channel at a rate slower than the data rate. I.e., a slow hopper sends a burst of data on each channel and then moves on. A fast hopper, however, may hop once per data bit, or even many times per bit.

From the point of view of another user of the spectrum, a fast hopper will appear as an elevated background noise, while a slow hopper will appear as time divided burst interference. The distinction is important when considering interactions between different systems because a fast hopper will appear similar to DSSS but a slow hopper requires a different analysis.

Many types of FHSS systems are possible. There are those with more than one simultaneously hopping carrier. Some systems convey the data stream by altering the hop sequence rather than modulating the carrier. Hybrid systems are also possible, combining both direct sequence modulation and frequency hopping.

This study, however, is confined to the most commonly found and generic FHSS system. This is a one frequency slow hopper, in which a single carrier is hopped among a number of discrete frequencies. On each frequency it dwells long enough for a short burst of data to be sent. This data burst is sent by modulating the carrier by conventional means (ASK, FSK, PSK, etc.).

If there are N channels to hop over, then the hop sequence length M should be equal to or greater than N. Setting M>N gives advantages over potential eavesdroppers but makes synchronisation of the receiver more difficult. In the generic case therefore, it is assumed that M=N and that each channel is visited once during the sequence. An example of a time-frequency pattern and the spectrum are shown below.
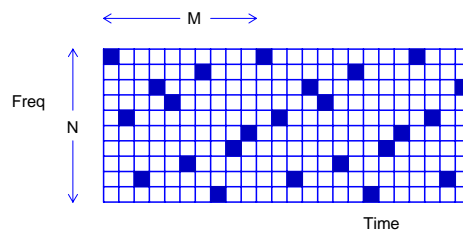
One Carrier Hopping Scheme

Instantaneous (Single Sweep)   Cumulative (Max Hold)
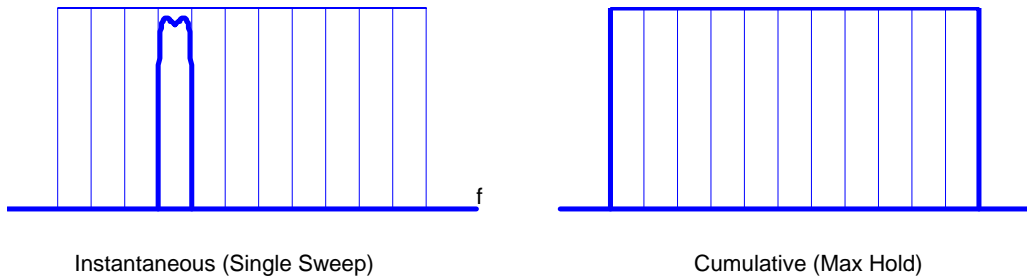
Spectrum of FHSS Transmission

Compatibility

Consider an FHSS transmitter and a conventional victim receiver operating on one of the channels in the hop sequence. For part of the time the interferer will be co-channel and for parts of the time it may be far enough away to be outside the front-end bandwidth of the victim.

At low levels of coupling the interferer may be below the level at which it is not seen even when co-channel. In this case no interference is caused and it makes no difference whether the transmitter hops at all.

At high levels of coupling the interferer may be strong enough to cause blocking. In this case, destructive interference is caused for large parts of the time. If the spread bandwidth fits inside the victim receiver's front-end bandwidth, then continuous destructive interference occurs. Again in this case, it makes no difference whether the transmitter hops fast or slowly, or even at all.

At intermediate levels of coupling interference occurs only when the transmitter is co-channel, or possibly on a small group of adjacent channels. The wanted signal is blanked out for a percentage of the time on a repetitive basis. The victim receiver experiences a series of short outages.

The above discussion is in terms of an FHSS transmitter and a conventional receiver. It can be seen that exactly the same considerations apply for a FHSS victim and a conventional interferer and indeed, between two FHSS systems.

At this intermediate coupling level, the hop pattern and the number of channels is of great importance in determining the pattern of interference.

Generic FHSS in the 863 to 870 MHz band

Assume the FHSS system divides the available spectrum into N channels and hops over them all with a (pseudo) random sequence. On average each channel is visited every N hops.

The following table shows what can be achieved using FHSS over a 7 MHz band. The duty cycles are the percentage of time that a conventional receiver receives the FHSS transmitter, and also the percentage of time that the FHSS receiver receives a conventional transmitter.

Hopping Scheme	Duty cycle of interference %
280 channels of 25 kHz	**0.35**
140 channels of 50 kHz	0.7
70 channels of 100 kHz	1.4
35 channels of 200 kHz	2.8

Table H 1.1

Note that with only 7 MHz available it is not possible to use FHSS to drive the effective duty cycle down to 0.1%. Therefore an FHSS system might not be appropriate in those parts of the band with a 0.1% duty cycle limit.

The pattern of interruptions from FHSS is likely to be unacceptable to Cordless Audio devices. Therefore, it may also be appropriate to exclude the 863 to 865 MHz band.

The following table shows the result of using FHSS over a 3 MHz band.

Hopping Scheme	Duty cycle of interference %
120 channels of 25 kHz	**0.83**
60 channels of 50 kHz	1.66
30 channels of 100 kHz	3.33
15 channels of 200 kHz	6.66

Table H 1.2

Switching Transients

In tests on FHSS systems it has been observed that the switching transients associated with the frequency hopping can cause energy to spill-over into adjacent channels and also into adjacent bands.

This effect could cause the apparent duty cycle of interference experienced by a conventional receiver in the same band as an FHSS system to be greater than that shown in the tables above.

It is also a mechanism by which, for instance, an FHSS transmitter operating in the 865 to 868 MHz band might cause interference to a Cordless Audio device in the 863 to 865 MHz band.

This area needs further study. It is recommended that this effect should be addressed when setting technical specifications for FHSS equipment.

MCL Spreadsheet

In the MCL Spreadsheet, four FHSS systems were analysed:
- FHSS1 is a generic system of 25 mW power hopping over 70 channels of 100 kHz each. Transmissions are made with a 1 % duty cycle.
- FHSS2 is a generic system of 25 mW power hopping over 70 channels of 100 kHz each. Transmissions are made with a 10 % duty cycle.
- FHSS3 is a generic system of 25 mW power hopping over 70 channels of 100 kHz each. Transmissions are made with a 100 % duty cycle.
- FHSS4 is an application specific system.

This is described further in Annex H clause H.2

H.2   Example for an SRD using FHSS

Asset Tracking System

Introduction This annex describes a system using FHSS, which is intended for use as an asset-tracking device for the materials handling industry. It is particularly advantageous for the location and tracking of containers, cars and pallets that are moved by road or rail. In addition the system is capable of interfacing to sensors that are fitted to containers carrying perishable or hazardous materials. In the event of a problem with the contents of any of these containers, the system can transmit an alarm.

Outline Description The system comprises a number of end unit transmitters. Each end unit is attached to one item that is to be tracked. The end unit periodically transmits a signal containing its identity number using FHSS modulation. This signal is detected by receiving base stations that are sited at strategic positions across the country. Using phase interferometry each site is able to measure the bearing (angle) to an end unit from its position to an accuracy of 0.3 degrees. A communication system at the fixed sites passes the bearing for each container to a command control centre. Once the angle of an end unit is known, this information is relayed through a communication network to the interested parties. By obtaining the angles from 3 fixed sites, the location of the end unit can be determined.
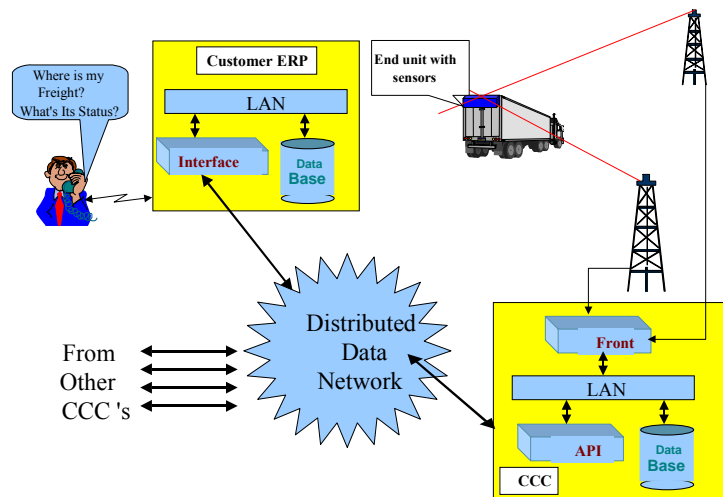
A diagram of a typical system is shown in Fig H 2.1 below

Figure H 2.1. Typical system layout

End units may be pre-programmed to transmit a routine status message twice per day. In addition, in the event that an end unit receives an alarm input from one of its environment sensors it may initiate an alarm message. Also if the position of an end unit is required at any particular time, a base station may request the end unit to transmit its status message. The request from each base station to an end unit is performed at frequencies within the radio paging bands, which is outside the 865-868 MHz band.

Base stations in urban surroundings will be located at separations of 15 km. In rural conditions separations will typically be from 25 to 40 km, depending on the nature of local terrain. To minimise the effects of reflections and standing wave nulls, base stations measure the signals received from end units at seven different frequencies.

Preferably the end units should transmit in the band 865 - 868 MHz using FHSS modulation in channels of 25 kHz. UHF is considered the most suitable frequency for this application. The reasons for this are that a 2 MHz band will provide an acceptable number of channels for FHSS operation at a data rate that fully meets the needs of the application. The characteristics of this band also permit the location of containers to be determined with acceptable accuracy while enabling the transmissions from end units to be detected at a satisfactory range.

FHSS modulation has been selected since it minimizes the effect of differential path loss and spurious signals caused by reflections. UHF transmissions are prone to both of these effects. FHSS modulation may provide an improvement of 10 to 15 dB in fading margin.

Market Benefits A survey of the market has shown that Europe has approximately 20 million containers that would benefit from asset tracking. Knowledge of the location of each container will greatly assist in its efficient movement and in the prediction of its time of arrival at its destination. Studies indicate that this knowledge potentially could generate annual savings within the materials handling industry in Europe equivalent to 0.5% – 5% of the value of the shipment.

The construction of the end units and fixed stations in the volumes required represents a major task and will generate significant employment within the Community. Furthermore a large additional workforce will be necessary to fit the end units and install the receiver base stations together with their associated communications network.

Technical Parameters It is proposed that the end units shall operate within a 2 MHz spreading band in channels of 25 kHz using FHSS modulation. The transmitted peak instantaneous power in any channel shall not exceed 500 mW e.r.p.

The end units transmit their data at a rate of 200 bps using BPSK modulation, which corresponds to a bandwidth of 400 Hz. In addition to sending the identity number of the end unit, a further 180 bits are reserved for use as an alarm message, error correction, sync information etc.

Each message sent by an end unit has a transmission length of 3.6 sec. There are 7 frequency hops within this single message, randomly chosen from the 80 channels within the available bandwidth of 2 MHz. The transmit duration of each frequency hop is 165 milliseconds. The percentage transmission time during a message is therefore less than 40%, which gives ample time for shaping of the transmission at each hop frequency.

The base stations transmit messages to the end units only in bands that are presently assigned for paging systems and not in the 865-868 MHz band.

Hot Spots A potential market of 20 million containers, leads to an average density within Europe of 2 end units per square kilometre. However it is anticipated that containers will frequently be assembled in railway marshalling yards, container ports and other distribution points. These will constitute hot spots and may contain up to 5000 end units at any one time. At any instant approximately 2/7 of the end units will be attached to containers that are moving.

Typically a stationary end unit will send a status message twice a day. An end unit that is moving will be triggered by a motion sensor and transmit a status message once every hour. Messages will also be transmitted in the event of an alarm condition. Assuming one alarm every hour as the worst case the resulting duty cycle is less than 0.03% on each hop frequency.

Compatibility Informal studies have been made showing that the system is compatible with other systems in the band. A diagram of the spectrum mask is shown in Fig. H2.2 below. Based on these figures it is considered that there should be no problem of compatibility either with audio systems or with existing SRDs in the band 868 – 870 MHz.
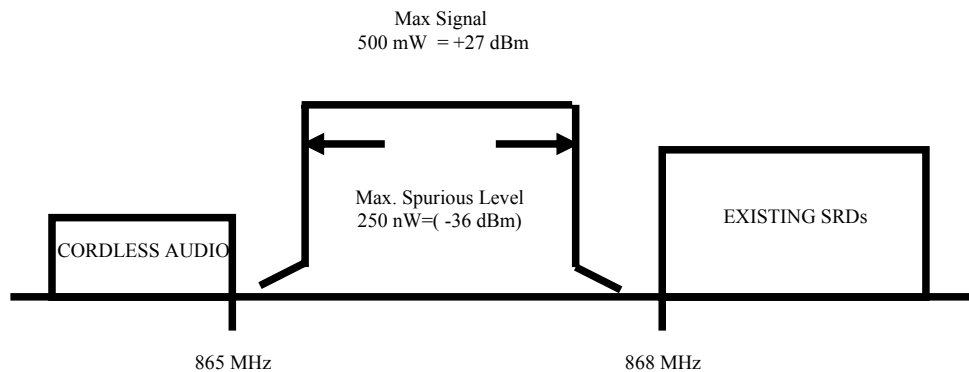

Figure H.2.2. Proposed spectrum mask

Practical tests have been conducted with CT2 equipment. Further information on this work is contained in SRDoc reference ETSI ERM 17_068. The results indicate that there is no incompatibility between this FHSS system and CT2.

Conclusions The following conclusions may be drawn from this report:

The application is best suited to operate in the UHF band in the proposed band 865 – 868 MHz.

     i.   Due to the environment in which the application will be used, FHSS with a spreading band of 2 MHz is a most appropriate and advanced technology.

    ii.   Transmission duty cycle per end unit at a hot spot is only 0.03%

   iii.   Informal studies and tests indicate that there is no incompatibility with existing and potential users of the proposed and adjacent bands.

    iv.   Due to a very low duty cycle and low data rate within a 25 KHz randomly chosen channel bandwidth, a power level of 500 mW can be justified for each transmission.

ANNEX I   EXAMPLE OF RFID USING 2 W E.R.P.

General The use of RFID in materials handling is a new application of this technology. The rate at which it will be adopted and the extent to which it will be used continue to be the subject of considerable debate. The figures used in this report have been derived from the opinions of people within the RFID industry. Nevertheless there remains the possibility for a significant margin of error. It is important therefore that the conclusions in this report are treated accordingly.

The principle data for the study was provided by EAN (European Article Numbering) International. This data was presented originally within the SRDoc for 2W RFID at UHF (ETSI SRDoc, TR 100 220 [23]) and shows the cumulative world sales of RFID equipment in the materials handling sector from 2002 to 2020. A copy of this diagram is provided at Fig I.1 below. In a subsequent discussion EAN International estimated that Western Europe would represent 25% of the total sales figure.
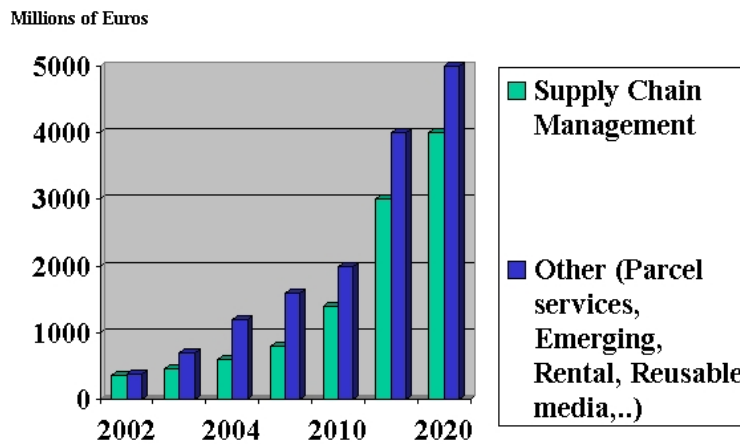

Figure I.1

From Fig I.1 it will be seen that total cumulative world sales for RFID at UHF in 2010 are estimated at 3,400 million Euros. On the basis that Western Europe accounts for 25% of this, European cumulative sales will be 850 million Euros.

In estimating the density of RFID interrogators it is necessary to consider a number of other factors. These are:
>   The ratio of tags to interrogators
>   The price of interrogators and tags over the period
>   The installation cost of fixed RFID equipment
>   The probable areas where the equipment will be deployed
>   The ratio of handheld to fixed interrogators

Each of these factors is considered in turn below.

Ratio of tags to interrogators In many of the early RFID applications, the ratio of tags to readers was surprisingly low. For access control applications the ratio was typically 50 although on rare occasions rose to 100. For Time and Attendance the ratios were higher but were still limited by the need for high throughput during peak rush-hour periods. This pattern has changed with the arrival of RFID in mass transit applications. Here interrogators are typically integrated into turnstiles. The quantity of turnstiles is defined by the layout of the transit system and is frequently quite low. On the other hand the number of passengers can run into low millions. This can lead to tag to reader ratios in the low 1000s.

Present opinion is of the view that materials handling will closely follow the mass transit model. Interrogators will frequently be installed at specified monitoring points. This will provide a natural limit on the number of fixed interrogators that will be deployed. By comparison the extent to which goods are tagged may ultimately be determined by tag price. On this basis it seems probable that the tag to interrogator ratios will increase as the technology becomes more widely accepted and mass markets develop. This in turn will be directly linked to falling tag prices as volumes increase. However it is difficult to predict how this ratio will change over the next ten years.

For the purpose of this study therefore densities have been calculated with tag to interrogator ratios of 1,000 and 10,000. These represent the likely limits for the different applications both at introduction of the technology and when finally it has been fully accepted.

Price Current prices for both handheld and fixed interrogators operating in the UHF band are typically of the order of 1,600 Euros. As development costs are amortised and production volumes increase, prices will inevitably fall. By 2010 there is a consensus view that prices for interrogators will have fallen to about 1,000 Euros.

The picture is very similar for tags. Initial prices are likely to be of the order of 2 Euros each. However as production volumes rapidly increase, prices by 2010 might drop to as little as 1 Euro.

Looking at Fig 1, it will be seen that during the period 2002 to 2010, the increase in cumulative sales is approximately linear. In estimating prices over this period, it is reasonable therefore to assume average figures of 1,300 Euros for interrogators and 1.50 Euros or less for tags.

Installation In addition to the price of the interrogator, there is a further charge associated with the cost of its installation. In general it is reasonable to assume a price for installation equal to the cost of the equipment. On this basis a figure of 1,300 Euros should be added to the price of each fixed interrogator.

Deployment For the purpose of this analysis, only countries in Western Europe have been included. The size of each of the relevant countries is shown in the table below

Country	Area - sq km x 10^3
Austria	84
Belgium	30
Denmark	43
Eire	70
France	544
Germany	358
Italy	301
Netherlands	42
Norway	324
Portugal	89
Spain	505
Sweden	450
Switzerland	41
UK	244
Total	**3,125**

Source: Times Atlas of the World
Table I.1

It seems most likely that RFID will be predominantly used in urban and semi-urban areas. On the basis that these areas represents about 10% of the west European landmass, it is reasonable for compatibility purposes to consider an area of 312,000 sq km.

Ratio of Handheld to Fixed Interrogators Market data from RFID applications at 13.56 MHz has shown that the ratio of handheld to fixed interrogators is significantly in excess of 100 : 1. It is recognized that the requirements of the materials handling industry will be different to applications at 13.56 MHz. Nevertheless it seems probable that the materials handling industry will require a very similar ratio. Handheld devices will typically operate up to 500 mW e.r.p., while fixed interrogators will radiate at levels of up to 2 W e.r.p.

The compatibility study should take into account that the majority of interrogators at UHF will operate at levels up to 500 mW. At a conservative estimate only 10% of all interrogators will radiate at 2 W e.r.p.

Calculations From the above factors it is a straightforward matter to estimate the probable density of RFID interrogators.

For a tag to interrogator ratio of 1,000

Cumulative sales in Western Europe by 2010	850 million Euros	(a)

Average price of interrogator	1,300 Euros	
Installation cost for 10% of interrogators	130 Euros	
Price of 1,000 tags	1,500 Euros	

Total	2,930 Euros	(b)
Number of interrogators deployed in 2010 (a/b)	290 k interrogators	(c)
Applicable area where interrogators will be installed	312,000 sq km	(d)
Estimated average density of interrogators (c/d)	0.9 interrogators /sq km	

For a tag to interrogator ratio of 10,000

Average price of interrogator	1,300 Euros	
Installation cost for 10% of interrogators	130 Euros	
Price of 10,000 tags	15,000 Euros	

Total	16,430 Euros	(e)
Number of interrogators deployed in 2010 (a/e)	52 k interrogators	(f)
Estimated average density of interrogators (f/d)	0.2 interrogators /sq km	

Hotspots In materials handling applications there will often be a number of interrogators at a single site. These will constitute hotspots. They will normally be located in industrial areas and business parks. While the compatibility study must include consideration of hotspots, it should also take note of the type of sites where hotspots will predominantly exist.

There is insufficient market data available to predict reliably the number of interrogators that will be located at hotspots. It is proposed therefore to assume the same numbers that were used for the compatibility study between Bluetooth and RFID at 2.45 GHz. This information is contained in ERC Report 109 dated October 2001 [24]. The report proposed the following categories:-

Scenario	Number of Interrogators
Common case	8
Very high density case	16
Extreme but very seldom case	32

Table I.2

Based on the above information the study has used the following assumptions:
- Average densities of interrogators should be based on equipment installed in urban and semi-urban of Western Europe.
- The interrogator to tag ratios should be based on the lowest and highest figures most likely to occur. These are ratios of 1 : 1000 and 1 : 10.000.
- The average density of interrogators for a tag ratio of 1 : 1000 is 0.9 interrogators/sq km. The average density for a tag ratio of 1 : 10.000 is 0.2 interrogators/sq km.
- The majority of interrogators will operate at levels of 500 mW. Only about 10% of interrogators will radiate at 2 W e.r.p.
- For hotspots, the density of interrogators contained in ERC Report 109 should be assumed also for RFID applications in the band 865 to 868 MHz.

ANNEX J   ADAPTIVE FREQUENCY AGILE TECHNIQUES

Introduction

This Annex describes a generic scheme for Dynamic Channel Allocation (DCA) in the 863 to 870 MHz band. In the SRD bands a DCA scheme relying on a central controller is not feasible. Instead it must operate on a peer to peer basis and therefore requires the use of Adaptive Frequency Agile (AFA) devices.

The scheme described is not the only way in which automatic or dynamic channel allocation might be achieved, but it is presented as typical of such schemes. It is a generic system in that it is not targeted at a particular application or applications.

The scheme described here is intended to be suitable for all applications and caters for a wide range of user requirements and expectations, which include:
*   To pop up, establish communication, send a short message and stand down. For battery-operated equipment the time spent establishing the link is important.
*   To set up a link to transfer large amounts of data. This might take the form of long packets with short return acknowledgements.
*   To rapidly switch between transmit and receive, sending short bursts in each direction in order to simulate a full duplex link.
*   To organise multiple nodes into a network.

In an AFA system each user listens before transmitting on a particular channel. If the channel is occupied he may either wait until the channel is free or look for another channel. The aim is not to force interoperability between different users but to facilitate band sharing between users, including between users with very different requirements and types of equipment.

The preferred channel width for the system is 100 kHz. Therefore, up to 70 channels are available.

The primary aim is to spread the users among the channels so that they may take advantage of frequency and geographical diversity. Therefore, when the band is less than fully congested, each user may operate in isolation from the others.

The secondary aim is to manage the situation when the band is fully congested. In this case it is desirable that users experience graceful degradation of the quality of service rather than sudden death, and that the spectrum resources are shared in an equitable manner.

Guiding Principles

The guiding principles for an AFA system are:
1.   Each device must check for channel contention before using a channel.
2.   If contention is discovered the device must look for another channel. Having chosen a channel the device should not change channels unless contention is discovered.
3.   Having chosen a channel the device may use it in any fashion consistent with the regulations.
4.   Periodic checks for contention must also be made while using the channel.

What happens then is that the AFA devices self organise themselves into the available channels. If another transmitter, not operating AFA, is present, the AFA devices organise themselves around it.

The reason for point 3 above, that devices should not change channel unless forced to, is that each device is attempting to generate its own "map" of which channels are occupied and this is difficult if the other devices are hopping in frequency.

The reason for point 4, that periodic checks should be made, is twofold. In most cases a new device should detect the presence of an existing device before transmitting. This is not always possible, however, so an existing device needs to be able to detect the incomer and change channel. The second reason is that it facilitates equitable channel sharing in the congested case.

Parameters of the AFA system

The following is a set of parameters for a generic AFA system. These are minimum requirements and in many cases manufacturers will obtain benefits by bettering them.

> Before transmitting, a device must listen for time: 5 ms
> Max time from end of listen period to start of transmission: 1 ms
> Maximum length of transmission: 500 ms
> A device must listen before each transmission unless it has listened in the last 500 ms (This is to allow rapid ping-pong type duplex).

After the channel has been in use for 1 sec the listen time rises to 10 ms; it reverts to 5 ms after the device has been quiet for 500 ms.

The listening threshold for detecting contention is a field strength of 63 uV/m or +36 dBuV/m. (This is equivalent to power received of –100 dBm from an isotropic antenna.)

The 863 to 870 MHz band is divided into 70 x 100 kHz channels. Of these, 10 are reserved to protect existing or special applications such as Alarm and Social Alarms. 10 channels are limited to devices with an average duty cycle of 0.1%, in addition to the length of transmission limit above. In the remaining 50 channels, subdivision to 50 or 25 kHz widths is permitted. A device need only listen over the same channel width as it is intending to use for transmitting.

The algorithms used to seek a clear channel and the means by which transmitters and receivers co-ordinate themselves are left to manufacturers.

The Uncongested Case If there are sufficient channels available the users are not competing for air time but are best served by having a channel each. In this case it is in the individual interest of each user to conduct the check for contention as well as possible. This is a desirable situation because instead of designing equipment to meet the letter of the regulations, manufacturers will be striving to do better.

The Congested Case It can be seen that an AFA regime will work very well with a minimum set of parameters in the case where the number of simultaneous devices is less than the available channels, but what of the case of a congested band where there are more devices than channels?

In this case it is considered preferable and more equitable that each device receives a lower quality of service than that some devices are locked out. A lower quality of service may mean a lower data rate or a longer wait to get access to a channel.

The generic AFA scheme described here provides ways in which such graceful degradation can be achieved: Narrowing of channels, Turnover of users, Time multiplexing in a channel.

Narrowing of Channels. Some devices will be able to operate in channels of less than 100 kHz. If a device must listen for contention with the same channel width as it uses for transmit, then there are benefits to the device that chooses the narrower width. These benefits are improved link budget and greater probability of finding a free channel. This is further enhanced by setting the listening threshold field strength constant regardless of channel width.

Different channel widths can co-exist and will self organise themselves across the band. Manufacturers are encouraged to use smaller widths because it gives them a benefit rather than coerced by regulation.

Turnover of Users. High duty cycle applications ideally want a clear channel to themselves. In a congested band with users coming and going it is simply a matter of waiting for such a free channel. If, however, all channels are occupied and there is not a natural turnover of users, then the parameters above provide a way for a new device to cut in after a given time (1 sec). If the previous device cannot find a new channel then the channel can be alternated between the two users at a relatively low switching rate.

Time Multiplexing. Low duty cycle users are better served by rapid time switching in a small number of channels. Listen before transmit requirements and a 500ms maximum transmission length limit are already in place. If overall

duty cycle limits are imposed, then devices will be unlikely to use the maximum transmission time. In that case a more rapid time multiplexing of a single channel becomes possible on a peer to peer basis.