



ECC Report 192

The Current Status of DFS (Dynamic Frequency Selection) In the 5 GHz frequency range

Approved 6 February 2014

Annex 2 amended 13 February 2015

Updated 21 November 2017

0 EXECUTIVE SUMMARY

ECC WGFM adopted a work item to study the DFS mechanism (Dynamic Frequency Selection) and current situation regarding interference into radars in 2011. Under an ECC WG FM questionnaire on the current status of in the 5 GHz frequency range, more than 200 cases have been reported and analysed in 2012.

This Report was intended to keep the collected information and study further in detail the issue of Wireless Access Systems including radio local area networks (WAS/RLAN) 5 GHz interference to meteorological radars. It has been shown that all investigated interference cases relate to outdoor WAS/RLAN fixed installations operating co-channel with the radar, although, due to the lack of information which did not allow concluding on the origin of the interference, some of these cases were not further investigated. It is also emphasised that short-term interference events have been reported but the short duration of these cases does not give the opportunity for administrations to further investigate the situation and to identify the source of the interference.

The analysis of reported interference cases leads to the following categories:

Intentional illegal use:

- A considerable number of the reported interference cases were caused by equipment where the DFS mechanism was disabled;
- In some cases, higher gain antennas were used resulting in e.i.r.p. levels above the regulatory limits, However, if the DFS) mechanism is active and efficient the use of higher gain antennas should not result in interference towards radars.

Non-compliant equipment

The main reasons for non-compliance are:

- Alteration/ disablement of DFS settings possible by the user (ETSI EN 301 893 version 1.4.1 [1] and higher does not allow the user to disable DFS or alter the DFS settings). In some of these cases, Notified Bodies had issued a positive opinion to this non-compliant equipment.
- In those interference cases where the DFS mechanism in the WAS/RLAN equipment is disabled, or where the equipment could be configured to a country where different or no DFS requirements apply, market enforcement shall not allow such equipment to be operated or remain in use and no effort should be undertaken to resolve the interference case by re-configuring the country of operation or by re-enabling DFS;
- In some cases, where DFS was disabled, re-enabling DFS did not cause the equipment to detect the radar. The DFS did not function as intended (non-compliant DFS).
- Market enforcement and surveillance authorities are also advised to initiate appropriate actions to prevent further that such equipment is placed on the market. It is also recommended that the equipment is submitted to a test laboratory to determine why the DFS mechanism is failing.

The findings of the present report have been confirmed by the TCAM ADCO market surveillance campaign that shows quite a high percentage of non-compliant equipment among those considered. TCAM/ADCO recommends that market surveillance authorities to increase the amount of inspections on 5GHz WLANs until the situation will have improved.

In those cases where the WAS/RLAN is operating co-channel with the radar and is causing interference into the radar, market enforcement shall not allow such equipment to be operated or remain in use and no effort should be made to solve the interference case by

1. Re-configuring the WAS/RLAN equipment to a different channel, or by
2. Re-enabling DFS again (where it was disabled), or by
3. Reducing the Tx-output power.

The case should be passed to the national responsible market surveillance authority for an action that can end in a safeguard clause procedure to ban the considered equipment from the European market.

Interferences due to equipment placed on the market at an earlier stage (compliant with an earlier standard version) should be dealt with on a case by case basis to solve the interference.

It could be beneficial to maintain and publish a list of non-compliant equipment for which Member States had initiated a safeguard clause in accordance with the R&TTE Directive [10]. It would be desirable to find solutions such that users/ consumers and retailers become more aware of the existing problems with non-compliant equipment and get some guidance from authorities and such a list may help them.

Notified Bodies

Notified Bodies shall not issue a positive opinion for the cases described above where the equipment is clearly non-compliant. Notified Bodies should consider the guidance provided in the present Report when assessing 5 GHz WAS/RLAN equipment.

The development of additional guidance to manufacturers and Notified Bodies is recommended (see section 2.6.1).

Incomplete investigation / inadequate actions by enforcement authorities

Most of the reported interference cases remained ultimately inconclusive because of key information were not collected, the investigations were incomplete or the action was inadequate.

However, despite these incomplete investigations, it can still be concluded that there is a considerable number of cases of intentional illegal use or non-compliant equipment.

Market enforcement authorities should consider the guidance provided in this report and increase their efforts to take appropriate action against non-compliant equipment or non-compliant operation of equipment.

There was

1. Insufficient or no investigation at all on why DFS did not work as intended;
2. No action against non-compliant or illegally used equipment.

A good cooperation and coordination between national market surveillance and market enforcement action is important to solve 5 GHz DFS interference problems.

Enforcement authorities should inform WAS/RLAN users about the consequences of the illegal use of WAS/RLAN equipment, i.e. causing interference to meteorological radars.

Compliance with ETSI standards

Considering investigated interference cases, no issues have been identified with regard to short comings in the specifications of the DFS mechanism itself as specified in the current version of the Harmonised European Standard EN 301 893 (i.e. – v1.5.1 and above). No investigated interference case can be traced back to failure of the DFS mechanism. Therefore, it may be assumed that equipment fully compliant with this standard provides adequate protection to radars.

Although ETSI EN 301 893 [1] prohibits the equipment to provide the user direct access to any of the DFS settings, this Report identifies means which may indirectly impact the DFS mechanism, including potential disablement of DFS (see section 2.6.1.3). Solutions may potentially be found through a further enhancement of the applicable standards.

TABLE OF CONTENTS

0	EXECUTIVE SUMMARY	2
1	INTRODUCTION.....	7
1.1	Objective.....	7
1.2	Background	7
1.2.1	DFS Operation.....	8
1.2.2	RLAN and Meteorological Radars	9
1.2.2.1	<i>RLAN Applications</i>	9
1.2.2.2	<i>Meteorological Radar Applications</i>	10
1.3	Current Regulations	12
1.3.1	WRC-03 Outcome	12
1.3.2	EC Decision for 5 GHz WAS/RLANs.....	12
1.3.3	Placing on the Market.....	13
1.3.4	Regulations in other regions.....	13
1.4	ETSI EN 301 893	14
1.4.1	Initial Version of EN 301 893 - Version 1.2.3	15
1.4.2	EN 301 893 - Versions 1.3.1 and 1.4.1	15
1.4.3	EN 301 893 Version 1.5.1 and Later Versions	15
1.4.4	Consequences for Radars.....	16
1.5	Interference to Meteorological Radars	16
1.5.1	Effect of interference to Meteorological Radars	16
1.5.2	Impact of interference on Meteorological Radars.....	19
1.5.3	Investigation of interference cases	20
2	QUESTIONNAIRE ON DFS IN THE 5 GHZ FREQUENCY RANGE	21
2.1	Interference Reports.....	21
2.2	Results, Analysis and Key Findings of the CEPT Questionnaire.....	21
2.2.1	Result and Analysis of the WGFM Questionnaire On The Current Status Of DFS (Dynamic Frequency Selection) In The 5 GHz Frequency Range	21
2.2.2	Additional Information from Czech Republic, Estonia, Spain, Portugal, The Netherlands and Romania	25
2.2.3	Summary of info received from 33 CEPT administrations on reported interference cases and the results of the investigations	26
2.3	Software Issues	26
2.3.1	Background.....	26
2.3.2	Issue	27
2.3.3	Regulation.....	27
2.3.4	Prevention of unintended and non-compliant modification	27
2.3.5	Recent developments	28
2.4	ADCO R&TTE market surveillance campaign	28
2.5	Interference situations in other regions	29
2.5.1	US.....	29
2.5.2	South Africa	30
2.6	Possible Solutions and Actions	30
2.6.1	Guidance to manufacturers and notified bodies.....	30
2.6.1.1	<i>Background</i>	30
2.6.1.2	<i>Responsibility</i>	30
2.6.1.3	<i>Requirement</i>	31
2.6.2	Guidance to Enforcement Authorities.....	32
2.6.2.1	<i>Background</i>	32
2.6.2.2	<i>Changing the WAS/RLAN operating frequency</i>	32
2.6.2.3	<i>(re-) Enabling DFS</i>	33
2.6.2.4	<i>Adjusting Tx-power</i>	33

2.6.2.5	<i>Conclusion</i>	33
2.6.2.6	<i>Other aspects to be verified by enforcement authorities</i>	34
2.6.3	Additional solutions to improve the situation	34
3	CONCLUSIONS	36
	ANNEX 1: ITU-R RESOLUTION 229	38
	ANNEX 2: COUNTRY CASE IMPLEMENTING GUIDANCES PROVIDED IN THE PRESENT ECC REPORT 41	
	ANNEX 3: LIST OF REFERENCE	44

LIST OF ABBREVIATIONS

Abbreviation	Explanation
ADCO	Administrative Co-operation group
BFWA	Broadband Fixed Wireless Access
CEPT	European Conference of Postal and Telecommunications Administrations
DFS	Dynamic Frequency Selection
EC	European Commission
ECC	Electronic Communications Committee
e.i.r.p.	equivalent isotropically radiated power
ESOs	European Standards Organizations
ETSI	European Telecommunications Standards Institute
EUMETNET	European Meteorological Network
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
IEEE	Institute for Electrical and Electronics Engineers
HIPERLAN	High Performance Radio
ITU	International Telecommunication Union
NTIA	National Telecommunications and Information Administration
NWP	Numerical Weather Prediction
RFI	Radio Frequency Interference
RLAN	Radio Local Area Networks
RR	Radio Regulation
RSPG	Radio Spectrum Policy Group
TCAM	Telecommunication Conformity Assessment and Market Surveillance Committee
TDWR	Terminal Doppler Weather Radars
TPC	Transmit Power Control
Tx	Transmitter
WAS	Wireless Access Systems
WiFi	Wireless Fidelity ISO/IEC local area network standard (IEEE 802.11 family)
WMO	World Meteorological Organisation
WRC	World Radio Conference

1 INTRODUCTION

1.1 Objective

This Report is intended to further investigate the issue of RLAN 5 GHz interference to meteorological radars and to review the information received in response to the ECC “DFS questionnaire” initiated by WGFM in October 2011. Based on this information, this report assesses the reasons for the interference cases such as non-compliant equipment and unlawful operation, and lists solutions and guidance for improving the situation.

The information and conclusions in this Report are based on those cases where the interference lasted long enough to allow for identifying the source of the interference and an investigation which resulted in clear conclusions with respect to the cause for the interference.

In response to the questionnaire, 17 CEPT administrations recorded more than 200 reported interference cases during 2010/2011. 16 other CEPT administrations responded that no interference cases were reported during this period.

A summary of discussions based on the replies of CEPT administrations to another questionnaire on interference cases in the 2015-2016 timeframe caused by WAS/RLAN in meteorological radars operating in the 5600 - 5650 MHz frequency range is provided in [13].

1.2 Background

Dynamic Frequency Selection (DFS) is a mechanism to allow 5 GHz Wireless Access Systems including radio local area networks (WAS/RLANs) to operate without causing undue interference to terrestrial radars operating in the 5250-5350 MHz and 5470-5725 MHz bands. The same mechanism also enables 5.8 GHz BFWA systems to operate in the 5725-5850 MHz band, at least in those countries that have implemented the ECC/REC/(06)04 [2]. DFS is a politeness mitigation technique, intended to sense the presence of radar signals in a given channel and prevent any WAS/RLAN or BFWA device from transmitting on that channel.

The allocation of the 5150-5350 MHz and 5470-5725 MHz to the mobile service for the implementation of WAS/RLANs was made on a co-primary basis at the International Telecommunication Union (ITU) World Radiocommunication Conference 2003 (WRC-03), under the conditions of the Radio Regulations Footnote N° **5.446A**:

“The use of the bands 5150-5350 MHz and 5470-5725 MHz by the stations in the mobile service shall be in accordance with Resolution **229 (WRC-03)**.”

This Resolution 229 (WRC-03) (see Annex 1) specifies the conditions under which this allocation was made.

- Considering j) highlights the need for using mitigation techniques such as DFS in order to enable sharing with Radiodetermination / Radiolocation services (i.e. radars);
- DFS is further specified in Resolves 8 that refers to Annex 1 of Recommendation ITU-R M.1652 for the details of the DFS requirements;
- Resolves 6 and 7 contain other requirements that contribute to the protection of radars.
- Recognizing a) also states *‘that in the band 5 600-5 650 MHz, ground-based meteorological radars are extensively deployed and support critical national weather services, according to footnote No. 5.452’*.

The DFS principle is recognisant of the fact that WAS/RLAN operating co-channel with a radar may interfere with the radar and therefore there is a need to avoid co-channel operation. To do so, the WAS/RLAN DFS mechanism has to perform radar signal detection on the channel it intends to use prior to have any transmissions on that channel. If a radar signal is identified, then this channel becomes unavailable for use by the WAS/RLAN. .

Following WRC-03, both the ECC and the European Commission translated this International regulation into European regulations, adopting respectively ECC Decision ECC/DEC/(04)08 (9 July 2004) and EC Decision 2005/513/EC (11 July 2005) on “*the harmonised use of the 5 GHz frequency bands for the implementation of Wireless Access Systems including Radio Local Area Networks (WAS/RLANs)*”. ECC/DEC/(04)08 [6] has been implemented by 41 CEPT administrations in May 2013.

The implementation of EC Decision 2005/513/EC [7] into national regulation has been mandatory and therefore has resulted in a general authorisation status for WAS/RLANs across the EU. Without derogation, Member States cannot impose additional requirements in their national regulations beyond those specified in the EC Decisions.

1.2.1 DFS Operation

Within the context of the operation of the DFS function, a WAS/RLAN device shall operate as either a master or a slave. RLAN devices operating as a slave shall only operate in a network controlled by an RLAN device operating as a master. A device which is capable of operating as either a master or a slave shall comply with the requirements applicable to the mode in which it operates.

The master/slave concept, where the master performs the radar detection on behalf of the slaves, was accepted with the assumption that the slave devices were in close vicinity to the master (e.g an office type of indoor application, or an outdoor public hotspot application, where ‘slave’ devices like PCs, notebooks, tablets and WIFI equipment smart phones are just a few meters away from the Access Point that operates as a ‘master’. This is also reflected in the requirement for slave devices with more than 200 mW e.i.r.p. to perform their own DFS operation.

The master/slave concept cannot be applied in cases where the slave is further away from the master, e.g. outdoor point to point or point to multipoint applications where the master and slave devices can be separated by up to a few kilometres. In such a scenario, both devices should perform their own radar detection, even if the maximum power of the client is below 200 mW e.i.r.p.

A brief overview of the DFS related requirements associated with master and slave devices are provided below. Please see ETSI EN 301 893 [1]¹ for more details.

Master devices:

- The master device shall use a radar detection function to:
 - Before normal operation: perform an initial check of the channel on which it intends to operate, to verify no radar is operating on that channel. This is a contiguous check for a certain period during which no transmissions are allowed;
 - During normal operation: continuous monitoring of the channel to verify no radar is operating on the channel.
- If a radar is detected on the channel, the master device shall stop normal operation on this channel and shall also instruct all its associated slave devices to stop transmitting on this channel. The channel shall be blocked for 30 minutes. After that a new initial check (check without transmissions) is required before it may consider this channel again for normal operation.

Slave devices:

- Slave devices shall not transmit unless being authorised by the master;
- Slave devices shall stop transmitting whenever instructed by the master;
- Slave devices with an e.i.r.p. of 200 mW or above, shall perform their own radar detection.

¹ At the time of writing this Report, version 1.7.1 of ETSI EN 301 893 was the latest published version.

1.2.2 RLAN and Meteorological Radars

1.2.2.1 RLAN Applications

Operating in harmonised shared access bands for RLAN wireless broadband infrastructures based on Wi-Fi technologies is essential to provide affordable internet connections to European citizens. This stimulates the development of online services to realise the growth potential of cloud computing applications in Europe.

In addition, mobile network operators are relying on the shared use of the same licence-exempt RLAN frequencies for data off-loading to increase their network capacity, to improve coverage in buildings and to save costs. More than half of all smartphone traffic appears to be routed over Wi-Fi networks, and this nomadic traffic is growing 4-6 times faster than mobile traffic. Global sales of Wi-Fi-enabled equipment should reach 3.5 billion in 2014. As regards those exclusive rights of use common use of frequencies in a specific geographical area also allows operators to increase efficiencies in their mobile networks. It is obvious that the 2.4 GHz RLAN band cannot by itself accommodate the growth of both private broadband access and mobile data traffic off-loading.

At the end of 2013, available WAS/RLAN equipment can achieve a maximum (theoretical) data rate of 1.3 Gbit/s, thus more than doubling the previous one, such as specified in IEEE 802.11n, and approaching the user data rates of wired networks. While depending on existing WAS/RLAN spectrum at 5 GHz, such developments will require very broad frequency channels, which are limited in number.

Figure 1: WiFi Chipset Shipments by Band

More than 1 billion WiFi chipsets (and 2 billion Bluetooth chipsets) have been shipped in 2011 alone.

The forecasts (*Reference: Cisco White Paper on "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017"*) indicate that mobile data traffic grew 70 % and will have a 13-fold growth

between 2012 and 2017, where Europe accounts for a considerable amount of this growth. As a result, WiFi networks in Europe will play a crucial role as a complement to cellular networks in responding to this tremendous need for mobile data traffic. Currently, there is a trend towards offloading mobile data in urban hotspots from cellular networks to smaller cells, WiFi-based and femtos. In 2012, already 33 % of the total mobile traffic was offloaded. This trend will be accelerated in the future and a considerable amount of Smartphone traffic will be routed over WiFi networks. The role of WiFi for data traffic over fixed networks is even more important. In this sector, WiFi networks carry in Europe more than 20 times as much Internet data as carried over cellular networks. Global sales of WiFi based equipment is expected to reach 3,5 billion euro in 2014 (Reference: 'Promoting the Shared Use of Radio Spectrum' by Pearse O'Donohue, Head of Unit, Radio Spectrum Policy, DG Information Society and Media, European Commission).

1.2.2.2 Meteorological Radar Applications

The use of radio-frequencies for remote observation of environmental phenomena is essential as part of an effective early warning and emergency management system to mitigate loss of life and damage to property from natural hazards.

Among these applications, meteorological radars are important surface-based instruments which data are input to now casting (e.g. the next six hours) and to the Numerical Weather Prediction (NWP) models for short-term and medium-term forecasting. Meteorological radars perform precipitation and wind measurements that play a crucial role in the immediate meteorological and hydrological alert processes. The radar data are also used to provide services to a number of sectors, transports, defence, aviation, agriculture, industry.

A typical description of the technical characteristics of C-Band meteorological radars is given in Table 1 below.

Table 1: Typical description of a C-Band Meteorological Radar

Frequency range	Typically 5600-5650MHz but possibility to be operated in the whole 5350-5850 MHz band
Peak power:	250kW
Pulse Duration	0.5 µsec to 2.0 µsec
Pulse Repetition Frequency (PRF)	typical 250 to 3000 Hz within various schemes
Antenna gain	Typically 45 dBi (parabolic dish)
Elevation	Typically 0.5° to 90° (volume scanning)
Rotation speed	Typical 1 to 6 rpm
Receiver noise figure	≤2 dB
Dynamic range	100 dB
Receiver sensitivity	(MDS - Minimal Detectable Signal) versus band at the reception: -112dBm@0.75MHz -109dBm@1.5MHz -105dBm@3 MHz
Protection criteria	-122 dBm/MHz

There are currently more than 200 meteorological radars operated by European countries that are members of EUMETNET, of which 180 are operated in the 5GHz (C-Band). The importance of these radars is recognised in Recommendation ITU-R M.1638 [9]:

“The meteorological radars are used for detection of severe weather elements such as tornadoes, hurricanes and violent thunderstorms. These meteorological radars also provide the quantitative area precipitation measurements so important in hydrologic forecasting of potential flooding. This information is used to provide warnings to the public and it therefore provides a safety-of-life service.”

In this respect, meteorological radars provide an important lead time to emergency responders in protecting against loss of life and property in flash floods and severe storms events, such as those that occurred recently in (e.g.) Eastern Europe, UK, France and Greece and for these reasons cannot be put at any risk. Thus RR Article 4.10 calls on administrations to ensure that special measures are undertaken to protect such safety services.

The importance of meteorological radars has subsequently been reiterated in many instances by the World Meteorological Organisation (WMO) and was, in particular, confirmed in the EU Radio Spectrum Policy Group (RSPG) Report and Opinion on “A coordinated EU spectrum approach for scientific use of the spectrum” (October 2006).

Meteorological radar networks operate 24/7/365 and are essential to monitoring the location and intensity of a range of weather hazards, including hail and snow; indeed, radar is the only means currently available for the measurement of rainfall and associated flash flood risk in real-time over large areas in critical rapidly responding catchments and urban areas. Doppler radar functions are also used for the detection of dangerous wind conditions (e.g. wind shear) which constitute a significant hazard to aviation safety. Such hazards can not only create significant disruption to transport systems and the economy, but also pose a significant threat to safety (e.g. the major UK snow events of November & December 2010, etc.). Radar data is not only used directly by forecasters and decision makers but is also ingested into meteorological and hydrological forecast models, underpinning the accuracy of warnings for river/flash flooding events and other critical weather parameters.

Images below show (i) the Met Office meteorological radar at Clee Hill, Shropshire, UK; (ii) precipitation distribution across the UK composite area; (iii) Doppler wind from the Chenies meteorological radar (north west London) showing wind shear from a tornado which caused damage to property and passed close to Heathrow Airport, on 7th December 2006 and (iv) precipitation visualisation on BBC media weather forecast, as based on radar products.

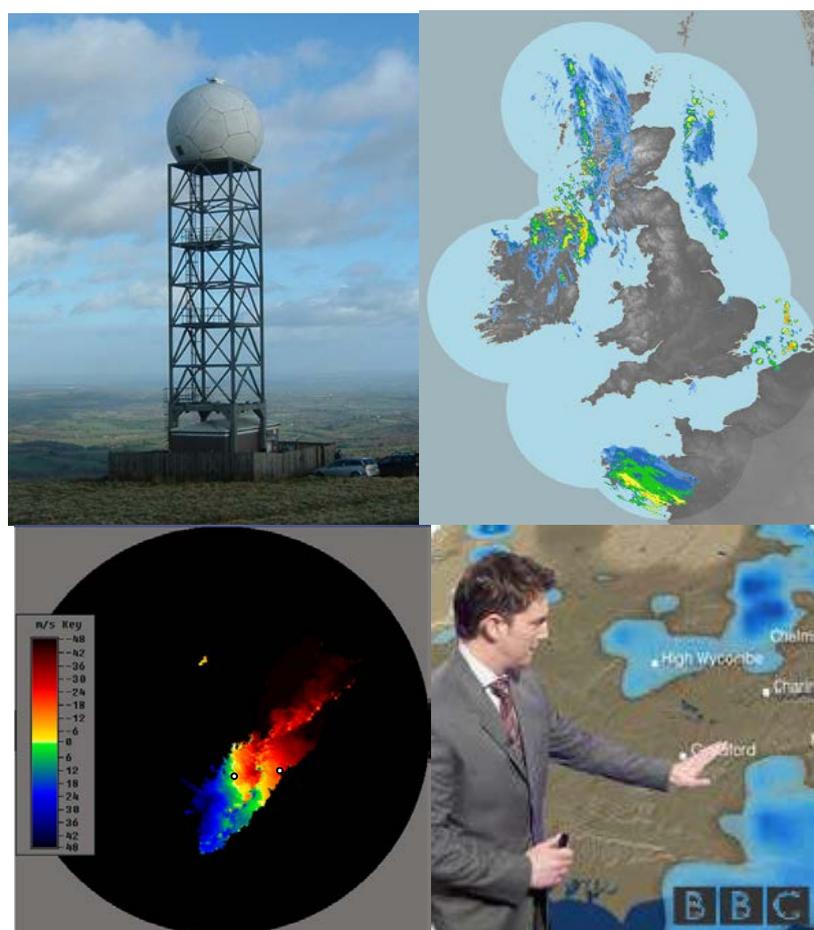


Figure 2: Met Office meteorological radar at Clee Hill – Visualisations

In Europe, through its programme in charge of Meteorological radars (OPERA), EUMETNET (the European METeorological NETwork) facilitates the operational exchange of meteorological radar information between national meteorological services and, in particular, supports the application of radar data from the European Meteorological radar Network. Such data enables the generation of European scale radar images (so-called “Odyssey composite”) such as below (captured 15 March 2012).

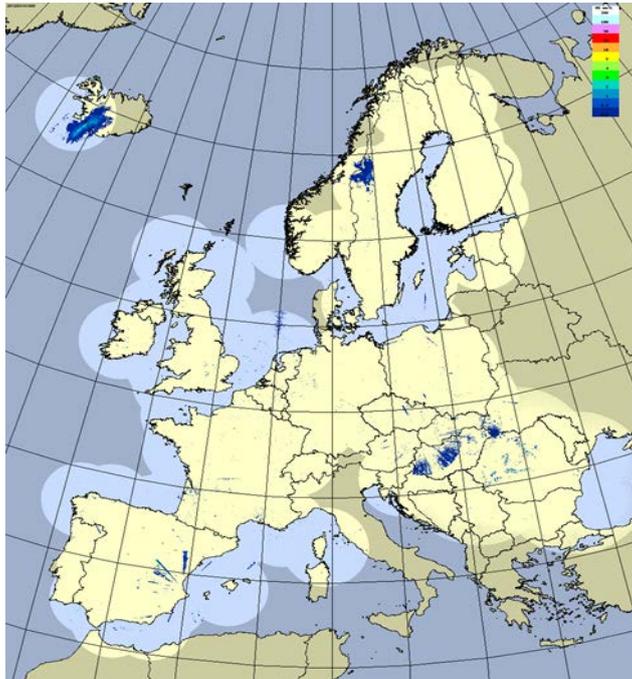


Figure 3: European Scale Radar Image

1.3 Current Regulations

1.3.1 WRC-03 Outcome

The World Radiocommunication Conference 2003 (WRC-03) agreed on a new frequency allocation on a co-primary basis to the mobile service for the implementation of “wireless access systems including radio local area networks” (WAS/RLANs) in the bands 5150-5350 MHz and 5470-5725 MHz. This was subject to technical and regulatory provisions included in the radio regulations, given in Resolution 229 (WRC-03) that makes the Annex 1 of ITU-R Recommendation M.1652 mandatory. This decision noted however that in these bands the stations in the mobile service shall not claim protection from radiodetermination services. The decision includes specific provisions to protect the incumbent systems; including military and meteorological radars.

1.3.2 EC Decision for 5 GHz WAS/RLANs

By mid-2005, the European Commission published EC Decision 2005/513/EC requiring all EU Member States to open the 5 GHz bands for the implementation of WAS/RLANs by 31 October 2005. The technical requirements contained in this Commission Decision are identical to those contained in ECC/DEC/(04)08 and consistent with Resolution 229 (WRC-03).

The EC Decision 2005/513/EC was amended by EC Decision 2007/90/EC of 12 February 2007 but there was no change with regard to the protection of radars. The EC Decision 2005/513/EC clearly specifies that

the military and meteorological radars operating in the 5250-5850 MHz band requires protection against harmful interference from WAS/RLANs.

Member states of the EU may not impose additional constraints in their nation regulations beyond those specified in the EC Decisions. CEPT administrations not subject to the EC Decision may impose additional conditions on or allow certain relaxation for RLAN apparatus subject to their adoption of ECC Decision (04)08.

1.3.3 Placing on the Market

The placing on the market and putting into service of radio equipment within the EU is regulated by the Directive 1999/5/EC (R&TTE Directive). The European Commission mandates European Standards Organizations (ESOs) to develop so-called Harmonized Standards. With the respect to the spectrum aspects of radio equipment, the relevant Harmonized Standards are developed by ETSI.

For 5 GHz WAS/RLANs, the appropriate Harmonised Standard is ETSI EN 301 893 [1] and for 5.8 GHz BFWA, the appropriate Harmonised Standard is ETSI EN 302 502 [11]. The DFS mechanism is an essential technical requirement in both standards, but the requirement to prevent the user to have access to the DFS settings only exists in ETSI EN 301 893 [1]. According to the R&TTE Directive, compliance with a Harmonized Standard allows the manufacturer to enjoy a presumption of conformity with the essential requirements of Directive 1999/5/EC [10] and as such they are allowed to place their products on the Community market. Although using harmonised standards is the most obvious and easiest way to place product on the market, the R&TTE directive provides for alternative routes. If alternative routes are used, the manufacturer will have to prove that his equipment provides the same level of protection to radars as equipment which has implemented DFS as described in the harmonised standard.

However as the ETSI standard EN 301 893 [1] prohibits equipment to provide the user the means to disable DFS or to alter any of the DFS related settings, this obviously also applies to other mechanisms to protect radar implemented by manufacturers which have chosen the alternative route described above.

5 GHz RLAN equipment where the user can disable DFS, or alter any of the DFS related settings, does not comply with the essential requirements of the R&TTE Directive. Such equipment shall not be allowed to be placed on the EU market.

1.3.4 Regulations in other regions

In 2000, as the RLAN industry in the US was preparing to enter the 5 GHz spectrum market with products designed to the IEEE 802.11a standard, manufacturers with worldwide distribution were concerned that Europe would restrict this band to HIPERLAN (High Performance Radio LAN) products as specified in ERC/DEC/(99)23 (withdrawn and replaced by ECC/DEC/(04)08) [6]. HIPERLAN was a specific RLAN technology developed by ETSI. The ERC/DEC/(99)23 (withdrawn and replaced by ECC/DEC/(04)08) mandated two mechanisms to protect radars and other primary users of this band: DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control). As a result, a project, P802.11TGh, was started to add these mechanisms in the IEEE 802.11 standard, with the assumption that if these additional regulatory requirements were met, global adoption of IEEE 802.11a-1999 would be possible.

At that time the 5 GHz band for RLANs in the US was restricted to the bands 5150-5250 MHz, 5250-5350 MHz and 5725-5825 MHz, but planning was already in the preparatory works for WRC-03 to add the 5470-5725 MHz band. This made DFS even more important for the US market. Over the course of the next three years, the FCC, with the help of the wireless LAN industry and the NTIA, developed the DFS rules for the US.

The spectrum used within US Federal agencies is administered by an Executive Branch organization known as the NTIA (National Telecommunications and Information Administration). Spectrum allocated for use by US commercial and private citizens is administered by the FCC (Federal Communications Commission).

When considering opening the 5 GHz band for use by wireless LANs, the NTIA expressed a strong desire that products entering the new band would adequately protect US military radars. This requirement was the basis of the US position at the WRC-03 which developed the first DFS requirements document - ITU-R Recommendation M.1652 [5].

During the period 2003 to 2006, the FCC with the help of the wireless LAN industry and the NTIA, developed the DFS rules for the US.

Since ETSI TC BRAN developed the first 5 GHz Harmonized European Standard (ETSI EN 301 893 (V1.2.3) in 2003 [1], the DFS test specification included in this standard became the basis for the development of the FCC DFS test specification and other test specifications in other countries.

Reported interference cases into meteorological radars by WAS/RLAN are also a concern in the USA. Devices certified under FCC Part 15, Subpart E of the Rules may be operated as U-NII devices. For those U-NII devices operating as a master device in the 5025-5350 MHz and 5470-5725 MHz bands, a Dynamic Frequency Selection (DFS) radar detection mechanism must be implemented and enabled. A piece of equipment is no longer compliant with the FCC rules if it is installed or configured to defeat DFS. The FCC encouraged users of U-NII devices near the aeronautical meteorological radars to register in a voluntary database system as discussed in the guidance DA 12-459 [3] and took action in 2012 against operating devices that caused interference to meteorological radars maintained by the Federal Aviation Administration (FAA) operating in the 5600-5650 MHz band.

In addition to applying its enforcement authority against specific manufacturers or service providers, the FCC provided revised guidance to manufacturers seeking certification authority for the 5470-5725 MHz band:

1. Requiring devices to notch the 5600-5650 MHz band (2009);
2. Requiring indoor devices to be labelled for indoor use only (2009);
3. Requiring professional installation of outdoor equipment and encouraging registration of location and ownership of outdoor transmitters in a voluntary industry database (2010);
4. Requiring outdoor devices operating on the TDWR channels to be 35 km removed from the radar site and separated in frequency from the radar (2010);
5. Specifically declaring that user configuration cannot include the ability to set a jurisdiction for the device that would have the effect of disabling DFS (2010).

In addition, the FCC has also proposed a new test for U-NII devices in this band that for the first time includes TDWR waveforms, which had not been part of prior tests. Now pending at the FCC is a rulemaking proposal to resolve these issues and to adopt the guidance into rules.

The above describes the measures taken by the FCC. However, the regulatory regime in Europe is different from the one in the US, hence why both regions may need to implement different measures to address the issue.

It should finally be noted that some administrations (notably Australia & Canada) do not allow WAS/RLAN to use the band 5600-5650 MHz with the objective to protect meteorological radar operations.

1.4 ETSI EN 301 893

ETSI BRAN has developed a European harmonized standard (Norm) EN 301 893 [1] which includes technical requirements and related test methods (including those for DFS) which can be used by manufacturers to prove compliance with the essential requirements of the R&TTE Directive [11].

Annex 1 of Recommendation ITU-R M.1652 on DFS was used as a basis when developing the DFS (performance) requirements contained in EN 301 893. Although the DFS requirements are applicable on the network, the ETSI standard details how these requirements and the corresponding conformance tests were transposed on a device level.

1.4.1 Initial Version of EN 301 893 - Version 1.2.3

The first version of EN 301 893 (V1.2.3) was published by ETSI in August 2003. That standard detailed 3 specific radar test signals and referred to ITU-R Recommendation M.1652 that covers a wider range of radar signals.

1.4.2 EN 301 893 - Versions 1.3.1 and 1.4.1

EU administrations found equipment on the market whose detection capabilities were limited to the 3 specific radar test signals defined in the version V 1.2.3 of this standard but no other radar signals. These were examples of equipment that were compliant with EN 301 893 (V1.2.3) but not with the intent of the regulation which requires protection of radars. EN 301 893 (V1.3.1) was produced in conjunction with the administrations of several EU member states including military experts and was therefore published in August 2005 to address this issue and included a wide range of radar test signals with pulse widths between 1 μ s and 30 μ s and PRF rates between 200 Hz and 4000 Hz.

Subsequently at the end of 2006, some administrations reported the first RLAN interference cases to meteorological radars, due to the fact that the DFS mechanism was disabled by the user or the operator of the network. It was found that there existed RLAN equipment which allowed users the possibility to switch-off the DFS mechanisms.

At the same time, ETSI was developing a new version of the standard to address an urgent need from industry to have a harmonized standard that also covers MIMO or other high throughput technologies and/or channel bonding.

ETSI therefore took the opportunity of the work on this new EN 301 893 V1.4.1 to include the requirement that DFS controls (hardware or software) related to radar detection shall not be accessible to the user. It was clarified that it should not be possible for a user to disable DFS or to alter any of the DFS settings. This was maintained in all later versions of EN 301 893 [1].

1.4.3 EN 301 893 Version 1.5.1 and Later Versions

The above interference cases also led to testing performed by member states to verify the efficiency of DFS as implemented by different manufacturers. The results showed that some RLAN equipment, although being compliant with EN 301 893 (V1.3.1), may not provide protection to some types of radars. During the same period new cases were reported where RLANs had caused interference into meteorological radars. A detailed investigation showed that meteorological radars are typically using complex transmission schemes with staggered/interleaved PRF and/or pulse widths below 1 μ s as well as noise calibration scans where no emissions occur. Since those radar operational modes were not covered in EN 301 893 V1.3.1 or V1.4.1 meteorological radars were shown as not necessarily protected by equipment compliant with these versions of the standard.

This issue was brought to the attention of the European Commission and TCAM that, after a detailed consideration, instructed ETSI to further revise EN 301 893 to include radar signals based on staggered/interleaved PRF and/or pulse widths below 1 μ s. In addition a solution for the protection of meteorological radars employing complex scanning schemes (sometimes including receives only noise calibration scans) was also required for the band 5600-5650 MHz. A phased approach was agreed with the European Commission from which the most important step was the completion of EN 301 893 V1.5.1 by mid-2008. This standard entered into force on 1 July 2010. The most important DFS related changes introduced in version 1.5.1 can be summarised as follows:

- Staggered PRF detection capability across all DFS channels;
- Minimum pulse width detection of 0.8 μ Sec (versus 1 μ Sec in earlier versions);
- Solution for the noise calibration of meteorological radars in the 5600-5650 MHz band;
- The ability for the RLAN to exclude channels within the meteorological radar band (5600 to 5650 MHz).

The last phase of the agreement was completed by ETSI with the publication of EN 301 893 V1.6.1 which entered into force on 1 January 2013. The main difference (with respect to DFS) with version 1.5.1 is that the minimum pulse width detection has been further reduced from 0.8 μ s to 0.5 μ s. Other changes were

introduced into this version which will allow industry to bring new products on the market supporting wider WAS/RLAN channel bandwidths up to 160 MHz.

The last version of EN 301 893 [1] produced by ETSI is version 1.7.1. This version will improve the intra-system sharing but the DFS requirements have not changed compared to version 1.6.1.

1.4.4 Consequences for Radars

As part of agreement reached in TCAM, a specific Recommendation was adopted by the 35th EUMETNET council (Reading, UK) in December 2008 to provide the following technical and operational guidelines to be considered with the highest care and priority by meteorological services:

- only operate radars in the 5600-5650 MHz band;
- transmit minimum number of detectable signals over scanning strategies (so-called “Minimum detectable signal concept”);
- improve to the best extent and at minimum to the future regulated levels the out-of-band emissions of radars;
- improve to the best extent the out-of-band signal rejection of the radar receiver, with a particular focus on the image-frequency.

Overall, the rationale behind this recommendation was to avoid the scenario that future development of radar technology could lead to a new request to RLAN industry and ETSI to further improve the DFS mechanism. It was agreed that further revision of standard could be avoided without much constraint on future radar developments by implementing minimum detectable signals based on version 1.6.1 of EN 301 893 by the radar and the 10 minute Channel Availability Check (CAC) by the RLAN in the 5600-5650 MHz band.

1.5 Interference to Meteorological Radars

1.5.1 Effect of interference to Meteorological Radars

Initial cases of interference from 5 GHz WAS/RLAN to meteorological radars in the C band (5600-5650 MHz) were reported in 2005 by the Hungarian and Polish meteorological services and since then about 15 other European meteorological services have now reported similar interference events.

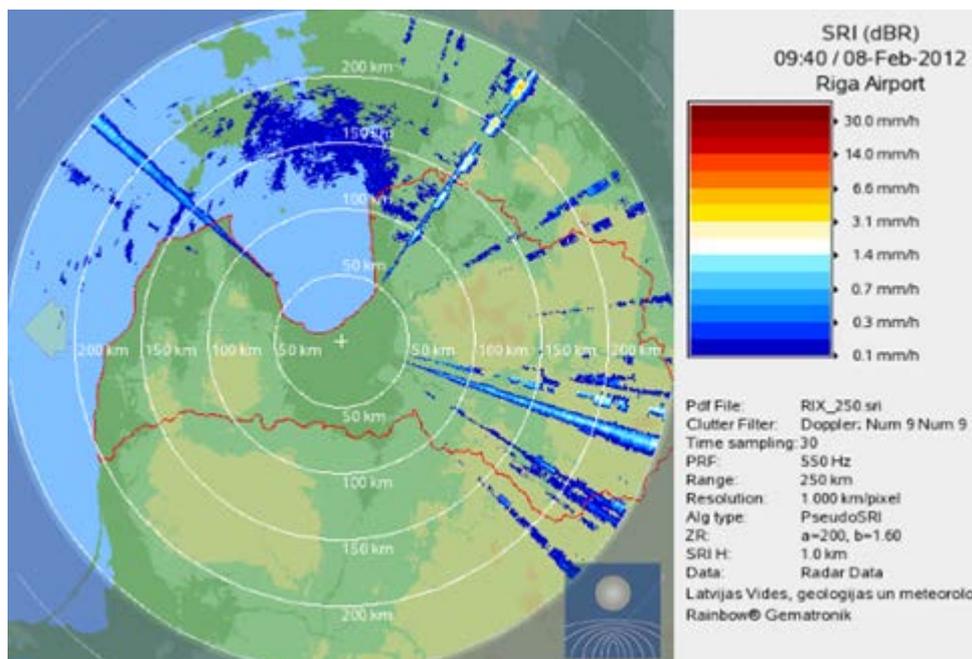


Figure 4: Wider Sector Interference in Latvia

A typical interference event appears as a straight line from the centre of the screen along a fixed azimuth towards the edge of the radar visualisation. This straight line could also be wider sector depending on the environment (e.g. terrain, buildings, etc) of the radar location and the proximity of the interferer as shown on figures below: (examples given for the UK Cleve Hill, Dean Hill and Crug-Y-Gorllwyn radars in 2012).

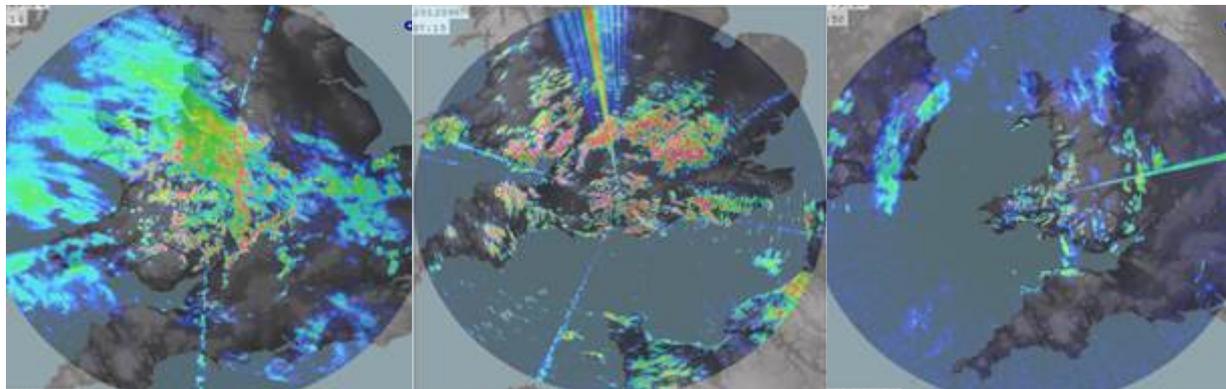


Figure 5: Narrow Sector Interference Examples

In addition to the visual identification of an interference (radar display), some meteorological offices use a specific software to monitor the presence of interference. As an example, the UK Met Office has run an automated interference software monitoring system since 2011 to record the occurrence of interference events across its network. Whilst this neither can capture and identify every single interference event nor identify the source of the interference, on-going efforts are being made to analyse data and link software monitoring outputs to reported or observed interference events. Examples of output are given below:

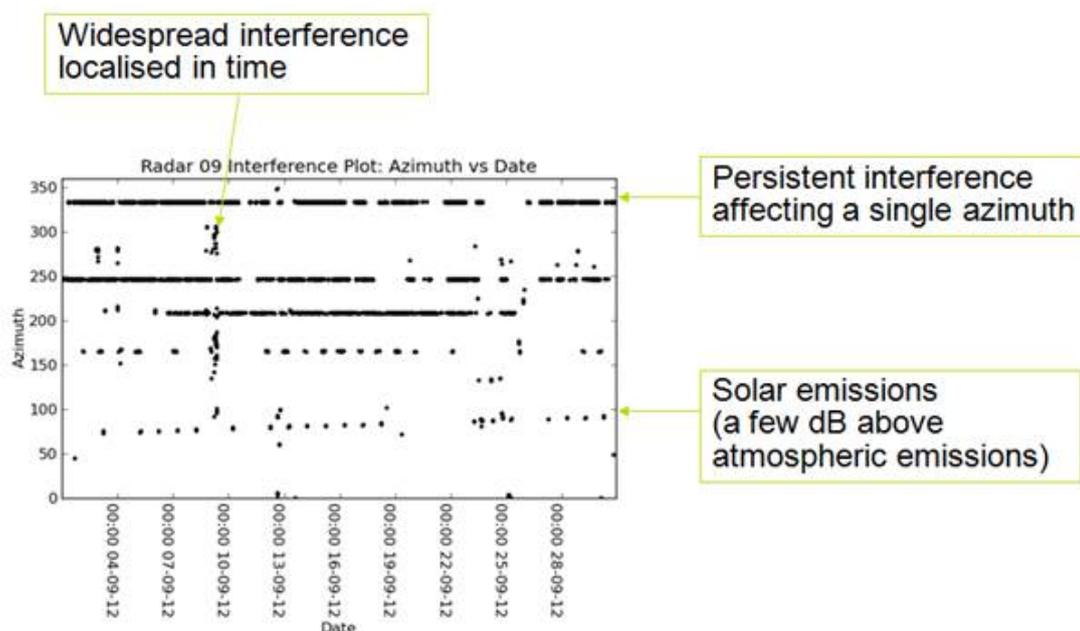


Figure 6: Interference in time

The image above shows typical monitoring of radar reflectivity data from the lowest elevation scan (0.5 degrees) from the radar at Ingham in Lincolnshire, UK.

The figure below shows an example of interference caused by RLAN device at around 210 degrees. The radar concerned is the Dean Hill weather radar in the UK.

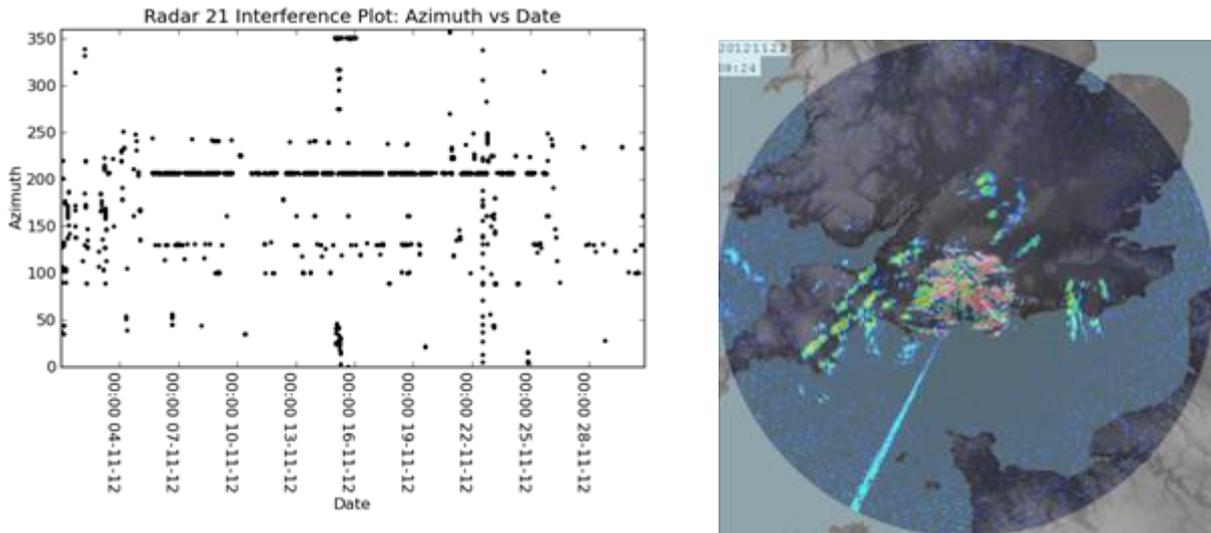


Figure 7: Interference caused by RLAN

What these plots show is not only the regularity with which meteorological radars can be interfered with, but that interference can be both widespread and localized in time, and also persistent in time over only a limited azimuth. It should be noted that attribution is not indicated by these plots and that further work is required to reveal trends in RLAN interference and radar noise floor.

The need for cross-border enforcement actions

This section briefly highlights the need for cross-border co-ordinate enforcement actions in case of interference into radar.

Interference can manifest itself in the following two cases:

- A radar in one state can be interfered from a source in a neighbouring country;
- Where data from interfered radar in one country is used or composited by a neighbouring country.

As an example, the figure below shows an example of disruption to a composite radar image, where the UK Met Office is using data from the Dublin radar (Ireland) to produce an accurate weather forecast for the UK.

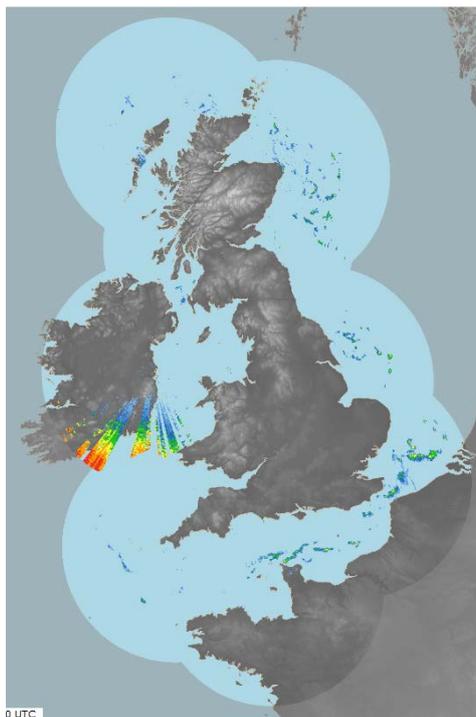


Figure 8: Example of disruption to a composite radar image

Similarly, cross-border issues apply to the European-wide EUMETNET composite radar (see section 1.2.2.2 for reference).

1.5.2 Impact of interference on Meteorological Radars

Monitoring of weather using radar relies on the detection and quantification of very weak return signals and being able for radars to scan at low elevations. Therefore radars are sensitive to disruption and even low levels of interference can impact the accuracy of the data, reducing the ability of the radar to detect weather-related phenomena.

In terms of impacts on meteorological and hydrological forecasting capability, interference can have three main consequences:

- General deterioration in forecast accuracy: Weather radar data pervades most meteorological services. Any reduction in the quality of observational data will have a knock-on effect on the accuracy of those services.
- Missed warnings: Interference can obscure real precipitation signals, resulting in the failure to issue a warning.
- False alarms: Interference can be incorrectly interpreted as precipitation, in some cases triggering false warnings of heavy rainfall and flooding (with associated costs). There is a risk that these false alarms could reduce public confidence in and reaction to warnings.

Radar based precipitation rates are operationally assimilated in NWP models and therefore have a significant impact in defining the initial precipitation conditions for a forecast run. Doppler radial winds are also assimilated in the models from radars and have been shown to be beneficial to forecast accuracy.

In future the intention is to move to assimilating reflectivity volume data as well as surface precipitation estimates. Radar refractivity is also derived and this is due to be assimilated in future; refractivity is directly related to changes in humidity, which is more straightforward to assimilate in NWP models.

RFI (Radio Frequency Interference) can significantly distort and obscure this data for a given location/sector and thus as a result degrade forecast accuracy.

Radars are used to underpin a range of warnings and forecast services and the data feeds into now casting models and longer-range NWP. Erroneous data not only obscures real weather information, hindering early warning of severe weather or flooding, but can then also be propagated into forecast data through said now casting/NWP applications. This affects not only the Severe Weather Warning Service to the public and forecast services to sectors such as aviation, but the data is also used directly by the national Environment Agency and other emergency responder organisations to issue warnings and take mitigating action.

1.5.3 Investigation of interference cases

1. The following describes the common procedure applied by enforcement experts to identify the cause of the interference. Drawing the interfered azimuth on a map (starting from the location of the radar);
2. Identifying higher elevation locations such as hills and buildings along the azimuth (in order to restrict the area of investigation);
3. Search for outdoor antennas or outdoor devices with integral antennas, along the azimuth line, which could be the interference causing device;
4. Identify the owner/user of the interfering device.

In respect of interference caused by WAS/RLAN, two important aspects should be emphasised:

- a) the locations (and other relevant information) of the outdoor installed devices is not known because of the general authorisation regime for WAS/RLANs.
- b) In the case of wider azimuth interference, locating the interferer is even more challenging.

This description emphasises the difficulty to investigate such interference cases. This can take several weeks to be handled noting that amongst collected interference cases during the questionnaire, interference can occur at a separation distance between RLAN and Radar greater than 100 km.

The above general procedure is only applicable in case of a continuous perturbation. However, short-term interferences have also been highlighted in the responses to the questionnaire. To handle this, more analysis and also more time is required to investigate such a situation. If the interference is not continuous, it is difficult for enforcement experts to locate the interferer. The meteorological service could help by performing a long term monitoring of the interfering signal by the interfered radars. This permits identifying the direction and also estimating the distance using the signal strength of the interfering signal measured at the radar site. In addition, this could also help the behaviour over time of the interference which can help the investigator to be at the suspected location when the interference may occur.

2 QUESTIONNAIRE ON DFS IN THE 5 GHz FREQUENCY RANGE

At its October 2011 meeting, ECC WG FM agreed on a questionnaire to be sent to CEPT administrations to collect information regarding the current status of the DFS in the 5 GHz frequency range.

The consultation results provided by the ECO were considered by the SRD/MG during their March 2012 meeting in London. From a total of 33 countries that responded, 17 countries reported more than 200 interference cases which occurred during 2010/2011. The other 16 countries responded that not any interference case was reported during that period.

Table 2 in section 2.1 is structured in a way to allow the analysis of the reported and documented interference cases in such a way that the relation of these cases with regard to market surveillance, enforcement, standardisation and frequency management is clearly visible.

2.1 Interference Reports

The analysis made in this report is based on the interference cases reported and investigated by the administrations and for which they provided details which enabled their feedback to be taken into account in the analysis.

One administration (UK) reported, in addition to long lasting interference cases, many thousands of short duration interference events.

2.2 Results, Analysis and Key Findings of the CEPT Questionnaire

2.2.1 Result and Analysis of the WGFM Questionnaire On The Current Status Of DFS (Dynamic Frequency Selection) In The 5 GHz Frequency Range

Table 2: RLAN /Meteorological Radar interference analysis

Country	Outdoor / indoor	Illegal device/use	Notified body in conformity assessment	Standards	Case notes	How interference cases were resolved
Albania	-		-	-	-	No interference cases reported
Austria	All outdoor (various applications)	DFS disabled in all cases	Notified body not involved	No info	Inconclusive – insufficient information	11 cases Interference cases resolved by enabling DFS
Belarus	-	-	-	-	-	No interference cases reported
Belgium	Outdoor	DFS was switched off and Tx power too high	yes	EN 301 893 1.5.1	Non-compliant equipment	1 case: Enabling DFS and adjustment of Tx power?
Bosnia and Herzegovina	-	-	-	-	-	No interference cases reported
Croatia	-	-	-		-	No interference cases reported

Country	Outdoor / indoor	Illegal device/use	Notified body in conformity assessment	Standards	Case notes	How interference cases were resolved
Cyprus	-	-	-	-	-	No interference cases reported
Czech Republic	Vast majority outdoor (different types of applications)	DFS switched off, Un-allowed frequencies	Yes	EN 301 893 1.5.1 & EN 302 502 1.2.1	Intentional illegal use	50 cases Majority of cases: (1)Retuning RLAN frequencies; (2)Enabling DFS but didn't solved the problem in some cases. In some (unspecified number) cases, interference remained after DFS switched on (so, it can't relate to V1.5.1)
Estonia	All outdoor (p-t-p)	DFS switched off	Notified Body not involved	1.4.1	Intentional illegal use	10 cases (some cases solved by retuning RLAN frequencies)
Finland	Outdoor RLAN	Yes - DFS was enabled	Notified body not involved.	No info	Inconclusive – insufficient information	1 case Case resolved by retuning RLAN frequencies
Former Yugoslavian Republic of Macedonia	-	-	-	-	-	No interference cases reported
France	All outdoor	DFS off: 3 cases Tx power too high: 1 case DFS repeatedly switched off 2 cases	Yes: 2 cases No: 7 cases	EN 301 893 1.3.1 & 1.4.1, in some cases, provider did not identify the DFS version	Non-compliant equipment	9 x retuning of RLAN frequencies 1 x reduction of Tx Power (DFS was enabled but was ineffective)
Germany	No info	No info	No info	No info	Inconclusive – insufficient information	9 cases of interference
Georgia	-	-	-	-	-	No interference cases reported
Hungary	Vast majority outdoor (majority P-P)		yes	1.3.1, 1.4.1 and 1.5.1 and also EN 302 502 V1.2.1	Intentional illegal use	45 cases Retuning of RLAN frequencies
Ireland	No info	No info		No info	-	Co-channel interference cases reported in 2006
Italy	All outdoor RLAN	No info	No info	No info	Inconclusive – insufficient information	Retuning of radar frequency

Country	Outdoor / indoor	Illegal device/use	Notified body in conformity assessment	Standards	Case notes	How interference cases were resolved
Latvia	All outdoor but mainly P-P	DFS disabled (some cases?) The equipments with reconfiguration possibility (i.e. DFS switching and frequency selection etc.	Notified body not involved. Self declaration.	1.2.3, 1.3.1 , 1.4.1, 1.5.1 and illegal equipments	Non-compliant equipment	23 Retuning and enabling DFS Some equipment wrongly declared
Lithuania	-	-	-	-	-	No interference cases reported
Malta	-	-	-	-	-	No interference cases reported
Montenegro	-	-	-	-	-	No interference cases reported
Netherlands	All P-P (wireless camera)	DFS switch off frequency selection	Notified body involved	V1.3.1 and also EN 302 502 V1.2.1	No	15 cases Retuning RLAN frequency & enabling DFS
Norway	-	-	-	-	-	No interference cases reported
Poland	All outdoor RLAN	DFS was switched off in unspecified nb of cases	Yes	Possibility to alter DFS settings in some cases (although standard version number not checked)-		20 cases All solved by retuning RLAN frequencies
Portugal	--		-	-	Non-compliant equipment -	1 case reported
Romania	All outdoor	OK	Notified body involved	1.3.1 and 1.5.1 (DFS as in the standard not effective enough, pulse durations down to 0.8 us)	Inconclusive – insufficient information	2 cases Retuning RLAN frequencies
Serbia	-		-	-	-	No cases of interference reported
Slovakia	No info		No info	No info		Interference disappeared before investigation

Country	Outdoor / indoor	Illegal device/use	Notified body in conformity assessment	Standards	Case notes	How interference cases were resolved
Slovenia	-	-	-	-	-	No interference cases reported -
Spain	Outdoor (P-P)	No	yes	EN 301 893 1.5.1 & EN 302 502 1.2.1	Inconclusive – insufficient information	(2 cases) Shifting BFWA frequencies 1 additional case: interference due to poor image frequency rejection at the radar reception Spain reported Met-Radar with pulses of 1 us
Sweden	-	-	-	-	-	No interference cases reported
Turkey	-	-	-	-	-	No interference cases reported
UK	All outdoor 8 x p-p plus 2	3x DFS switched off	No info	No info	Inconclusive – insufficient information	Only 24 recorded cases of which 10 were caused by WAS/RLAN equipment 7 x retuning frequencies 3 x enabling DFS. Further testing/information expected from the Met Office / OFCOM

Notes:

- A considerable number of the reported interference cases were caused by equipment where the DFS mechanism was disabled, even though the equipment was declared to be compliant with version 1.5.1 of EN 301 893. This is in violation with the requirement in clause 4.9 of EN 301 893 v1.5.1. The manufacturer should not have declared the equipment to be compliant with the essential requirements of Directive 1999/5/EC when the user can simply disable or alter the DFS settings. The same applies to the Notified Bodies there where they were involved in the assessment of the product against the essential requirements of the R&TTE Directive. They should not have issued a positive opinion for such equipment. This aspect (user access to DFS) is specifically addressed in EN 301 893 (version 1.4.1 and later versions). Therefore we may conclude that the majority of the interference causing equipment referred to in the feedback received, is non-compliant equipment.
- Some cases were reported where harmful interference was caused into radars located up to 100 Km from the RLAN location, also due to the specific geographical situation. Further investigation is required, but this could indicate that the e.i.r.p limits may not be respected by the concerned RLAN equipment. The use of high gain directional antennas is not forbidden but requires a reduction of the Tx output power and this may be omitted in these cases. Using higher gain antennas does not necessarily lead to an increased risk of causing interference into radars as the DFS sensitivity also improves. Only in the case of (DFS) non-compliant equipment, using higher gain antennas pointing towards the radar may pose a higher risk.
- The majority of reported interference cases referred to a separation distance from 1 to 30 km.
- It has to be noted that in some cases where DFS was disabled, re-enabling the DFS mechanism did not solve the interference case. Existing reported interference cases were not conclusive. Such cases need to be more fully investigated and equipment may need to be verified before one can make conclusions with regard to the DFS performance of the equipment. The focus needs to be on equipment for which compliance is declared against version 1.5.1 or later.
- The Czech Republic reports that there is currently estimated more than 275 000 RLAN 5 GHz P2P or P2MP equipment installed. They reported to have 50 interference cases per year that requires their involvement in order to be solved.
- Many interference cases were solved by manually changing the operating channel of the interferer. All aspects of manual changing of the settings of 5 GHz RLAN equipment need further investigation, in particular with regard to the requirements stipulated on article 4.4 of the 2005/513/EC, also from the market enforcement perspective, and how the equipment could possibly meet the requirements. ⁴

2.2.2 Additional Information from Czech Republic, Estonia, Spain, Portugal, The Netherlands and Romania

Czech Republic

The Czech Republic emphasised that it is also needed to understand why operators operate their networks on discrete channels (DFS is switched off). The main reason is seen to be caused by high rate of penetration of devices in the network area. The more devices in network area the more channels are necessary. Due to channel occupancy, devices are still looking for free channel. It will cause the significant decrease of reliability of connection. To solve this problem operator usually switches DFS off and makes common agreement among rest of providers and coordinate discrete channels. This is smoothing, which is not allowed by the general authorisation, however this is the actual real situation. The second reason is that providers are using 5 GHz band for infrastructure (P – P connectivity). Due to reasons mentioned above and because operators would like to provide consumers with some level of QoS, they usually switch DFS off.

Spain

In these two cases it was not verified if DFS was operating or no, simply the frequency was changed and the interference disappeared.

In this case the WAS/WLAN was operating in conformity to EN 301 893 V1.5.1

Portugal

The WLAN/RLAN was operating in the 5 GHz band, i.e. within the EN 301 893 standard specifications, which version was declared by the manufacturer as V1.5.1. However, the operator has disabled the DFS mechanism when he was contacted by ICP-ANACOM, prejudging that DFS mechanism was the responsible feature to create the interference. This means that the exact version of the standard is not known, given the fact that version V1.5.1 prohibits users to disable the DFS. The operator has claimed that the DFS was operating.

The Netherlands

The Netherlands has two main meteorological radar systems located in “De Bilt” en “Den Helder” Interference cases are reported since begin 2009. The interference cases can be roughly divided in 4 categories.

- Interference caused by non-compliant equipment as the result of wrong firmware installed by the manufacturer. This is very unusual, manufacturers are keen on providing equipment conform the latest version of the harmonised standard.
- Equipment compliant with older versions of the standard: Several cases are reported, the time path for migrating to the newer versions of the standard has proven to be too long.
- Non-compliant equipment, wrong or old firmware installed by the supplier on request of customer or directly by the end user. Multiple cases were reported, older firmware compliant with versions of the standard prior to version 1.7.1 has the possibility to disable DFS. This is a problem usually in combination with outdoor installed equipment to fulfil a larger coverage than assumed for the intended use of the equipment. Also firmware for the USA market was encountered.
- High power outdoor installations (hidden node effect): some cases reported usually in combination with equipment compliant with older versions of the standard.

Romania

Conclusions regarding the interferences between Hiperlan and civil radars in Romania in 5.5 GHz:

- DFS/ RID/ TCP techniques were implemented in all equipment involved, but seemed to be not enough effective to avoid the interference; that's the reason why, the only way to solve these

complaints was to disable two radio channels in the Hiperlan controlling software; and finally, the meteorological radar from Bucharest has left the 5.5 GHz band;

- It can be possible that DFS wasn't effective enough because the radar central frequency (5531 MHz) fell between two Hiperlan channels (the one with 5520 MHz and the other one with 5540 MHz central frequency), that means that the condition stated in '4.7.2 DFS technical requirements specifications' (available only in versions 1.5.1 and later of the standard): "The radar detection requirements specified in clauses 4.7.2.1 to 4.7.2.3 assume that the centre frequencies of the radar signals fall within 80 % of the Occupied Bandwidth of the RLAN (see clause 4.3) centred around the declared channel centre frequency." was not satisfied in our cases.

Estonia

The actual number of interferers is well above 10. Only one company using outdoor p-t-p link on the meteorological radar frequency has been found so far and was working without DFS (default settings) and using the 20/40 MHz bandwidth.

2.2.3 Summary of info received from 33 CEPT administrations on reported interference cases and the results of the investigations

All reported interference cases were caused by outdoor fixed installed devices that were operating co-channel with the radar. In addition, these interference cases were attributed to one or more of the following causes:

Intentional illegal use:

- A considerable number of the reported interference cases were caused by equipment where the DFS mechanism was disabled.
- In some cases, higher gain antennas were used resulting in e.i.r.p. levels above the regulatory limits. However, if the DFS mechanism is active and efficient, the use of higher gain antennas should not result in an interference.

Non-compliant equipment

- Alteration/disablement of DFS settings possible by the user (EN 301 893.version 1.4.1 and higher does not allow the user to disable DFS or alter the DFS settings). In some of these cases Notified Bodies had issued a positive opinion to these non-compliant equipment's.

Incomplete investigation / inadequate actions by enforcement authorities

- Interference investigated and resolved by retuning RLAN frequency to different channel. However the actual reason for the DFS not working was not analysed (i.e. recording info on standard version, testing etc.);
- There was no action against non-compliant equipment.

One interference case was reported where the RLAN was operating on the image frequency of the radar and this was outside the meteorological radar band. As there are no radar signals on that frequency, DFS will not detect the radar. However in such case the RLAN cannot be held responsible for having caused the interference as it is entitled to operate on that frequency. This effect is more a filtering issue on the radar.

2.3 Software Issues

2.3.1 Background

Every WAS/RLAN equipment is shipped with a tested version of firmware/software provided by the manufacturer. However, most WAS/RLAN equipment is also designed to support a firmware/software

upgrade process. This allows the manufacturer to provide enhancements or to address bug fixes to equipment already placed on the market and installed. Manufacturers generally provide firmware upgrades as free downloads from their Web site. Additionally, a few manufacturers provide their firmware as open source code on the Internet. Programmers worldwide are free to modify and extend the code with new features for their routers. Several versions of this modified firmware can be found on the Web. However, the risk exists that such firmware upgrades impact the compliance of the WAS/RLAN equipment.

2.3.2 Issue

As the regulations governing the use of 5 GHz WAS/RLAN are not uniform across all regions or countries, the manufacturer will try to find solutions by which they can market a single product worldwide. Some manufacturers build a global product and request the end-user to select the appropriate country of operation during initial setup or configuration of the equipment. The selection of the country is intended to automatically configure the device in accordance with the regulations applicable in that country. But there remains the risk that incorrect selection of the country will result in non-compliant operation.

In both the US and in Europe, the regulations do not allow the user to have access to any setting which could disable or alter the DFS of the equipment. Therefore, to preserve conformity, manufacturers need to create regional or country specific products which cannot be re-configured in any way by the end user to support another region or country where different or no DFS requirements apply. To provide for the earlier mentioned software or firmware upgrades that enable product enhancements or to address bug fixes, the manufacturers need to make separate downloads available for each regional or country specific product.

2.3.3 Regulation

Under the European single market, new approach Directives, the manufacturer or the person that places the product on the market and that issues the Declaration of Conformity, remains fully responsible for the compliance of that particular product. Where a product has been modified without the consent of the manufacturer, it is clear that the responsibility for compliance cannot remain with the original manufacturer. However, the original manufacturer could design his product in such a way as to limit the possibilities for modifying the regulatory compliance of such equipment.

2.3.4 Prevention of unintended and non-compliant modification

Manufacturers can do a lot to guard against the deliberate modification of a device however there will always remain individuals who will see it as a challenge to find ways to circumnavigate the regulations in Europe. Deliberate flouting of regulations remains a risk however to all types of radio communications and is no more or less of an issue for WAS than any other lawful radiocommunications.

The text below contains a number of actions that manufacturers could implement to prevent modification or re-configuration of the equipment resulting in non-compliant operation:

- The configuration of equipment, and as such also the regulatory compliance of it, must never be dependent on the correct selection of the appropriate country of operation or any other setting to be done by the end user. For equipment shipped into the European Union, the operation of the equipment must always be compliant with the EU regulations irrespective of the selection of country of operation or any other setting or configuration available to the end user.
- Prevent equipment from accepting the installation of software which can change the regulatory compliance of that equipment. This means that equipment intended for the EU market shall only accept the installation of new software/firmware which is ensuring the compliance of the equipment with the EU regulations. It must not accept the installation of software/firmware intended for other regulatory domains.
- Prevent equipment from accepting the installation of previous versions of software (downgrading) that does not ensure compliance with the new regulatory requirements or standards currently in force.
- Manufacturers who provide their software/firmware as open source code on the Internet shall prevent modified software from having any impact on the regulatory compliance of the equipment.

- Providing sufficient warnings to end-users on the illegality of any modification (hardware or software) of the equipment, which may impact the compliance of that equipment.

2.3.5 Recent developments

Manufacturers are currently exploring ways by which equipment can detect its location and as such configure itself automatically to the appropriate regulatory domain that applies for the current location of the device. Such location awareness technology could make use of IP address location, GPS coordinates (for outdoor devices) or via a geo-location database. In all these cases, the manufacturer remains the overall responsible person while the end user cannot impact the automatic configuration by the equipment.

2.4 ADCO R&TTE market surveillance campaign

In 2013, ADCO R&TTE has conducted a cross-border market surveillance campaign on WAS/RLAN 5 GHz, involving 21 countries. The main focus of this campaign was not directly on verifying the compliance of the DFS mechanism itself (capability to detect all the various radar signals), but exclusively on the means offered to the user to disable or alter the DFS functionality. It should be emphasised that EN 301 893 states that DFS controls (hardware or software) related to radar detection shall not be accessible to the user.

During the campaign, each participating market surveillance authority investigated different types of equipment from its market. These samples were randomly selected. Subsequently there was an exchange of information amongst authorities to avoid checking of the same product.

It was verified whether the product complies with the user access restrictions contained in the harmonised standard (EN 301 893 V1.5.1, V1.6.1 and V1.7.1) and the manufacturers were requested to present:

- test report demonstrating the compliance of the equipment with the essential requirement;
- descriptions and explanations of the solutions adopted to meet the essential requirement if the manufacturer has not applied or only partly applied the applicable harmonised standard;
- a copy of the opinion issued by an involved notified body where the manufacturer has not applied or only partly applied one of the harmonised standards.

Authorities had to:

- check if the user manual indicates a way on how to disable DFS;
- check if the software included in the packaging allows to disable DFS;
- check if the web page of the manufacturer (on its representative) proposes an updated firmware and/or software which allows to disable DFS;
- check if the manufacturer gives on its web page an indication on how to disable DFS;
- check if requested documents from the technical documentation ensure that the DFS functionality has been built into the equipment.

The report has been presented at the TCAM WG 04 meeting on 22nd November 2013 in Brussels. The following information summarises the results of the campaign. The full report is accessible on the European Commission website (http://ec.europa.eu/enterprise/sectors/rtte/documents/state-of-play/index_en.htm)

Market surveillance authorities conducted investigations on 101 different 5 GHz WAS/WLAN devices taken from the market. 35 of these devices did not have radar detection as they either operated only in frequency bands where DFS is not required or were slave devices with an e.i.r.p. of less or equal 23 dBm which does not require radar detection.

This means that 64 product samples requiring DFS have been investigated. Each participating market surveillance authority had verified for each selected WAS/RLAN device whether it fulfilled the administrative requirements and whether it complied with the "user access restrictions" requirement contained in recent versions of EN 301 893.

- Only about 33% did fully comply with the administrative requirements such as equipment marking, declaration of conformity, part of the technical documentation. The level of compliance with the CE marking requirements was about 88%. 8 devices did not fulfil the formatting requirements (layout and/or height of the CE mark). Whereas for 41 devices the Declarations of Conformity were found compliant, only for 23 devices the technical documentation was compliant.;
- For 3 out of the 64 samples requiring the DFS, DFS was not implemented;
- For 22 out of the 64 samples requiring DFS, DFS could be deactivated by the user. In some cases it was possible for the user to change/update the device firmware with a different version, alternative versions or even old version which allows deactivating the DFS function. This is not in line with the requirement set out in recent versions of the harmonised standard EN 301 893 which prohibits the user to have this possibility. For some devices the information how to deactivate the DFS function was included in the user manual or published on the manufacturer's web site. See also the next bullet point;
- For 7 out of the 64 samples requiring DFS, the manufacturer provided information in the user manual on how to deactivate the DFS, and in 44 cases this information was provided on the manufacturer's website;
- For 38 samples, the DFS function could be indirectly deactivated by changing the device's region or country of use.

.Although EN 301 893 states that DFS controls (hardware or software) related to radar detection shall not be accessible to the user but in 38 out of 64 cases, the region of use could be changed. The campaign did not investigate the impact of the change of region or country of operation on DFS. In future investigations, it should be verified whether the change of the region or country of use does impact the DFS compliance. Amongst the recommendations made by ADCO R&TTE, it is also outlined that the cooperation at national level should be improved between interference management and market surveillance authorities in order to detect more rapidly non-compliant products and to take them off the market.

The results of this ADCO R&TTE campaign confirm the problems identified in this Report. Therefore, market surveillance authorities will continue to investigate such products and take all appropriate measures to ban non compliant products from the market.

2.5 Interference situations in other regions

2.5.1 US

TDWR radars (Terminal Doppler Meteorological radars) are used by the Federal Aviation Administration (FAA) at 45 US airports. TDWRs operate at 5600-5650 MHz. TDWRs have experienced interference from 5 GHz RLANs. The US Federal Communications Commission (FCC) has so far released about 20 notices or orders which provide information on the sources of interference. In those decisions, the interference issues arise from several sources:

1. Several manufacturers of outdoor equipment included capability that allowed users to select an operating mode that disabled DFS;
2. The outdoor equipment in use was returned from a non-DFS band to a DFS band by users in violation of equipment certification;
3. Outdoor users added high gain external antenna that caused the device to operate outside of the emission parameters specified in the device certification. The FCC has said additional cases remain pending.

In response, the FCC has:

1. Tightened its device certification requirements to ensure that DFS cannot be turned off;
2. Worked closely with outdoor user groups to publicize the need for users to operate equipment in a lawful manner;
3. Worked with industry on an industry-established voluntary database to enable outdoor users to register their transmitter sites;
4. Worked with the FAA and the National Telecommunications and Information Administration (NTIA) to revise a portion of the DFS device certification test to better reflect TDWR emissions parameters.

The FCC is expected to propose revised rules for the 5 GHz band in a rulemaking that will launch in 2013, including the newly modified device certification test; in the interim, RLAN/WAS use in 5600-5650 MHz band has been restricted. The NTIA announced in January 2013 an effective outdoor notch for WAS/RLAN use in the band 5600-5650 MHz, stating that: *"...the FCC has allowed outside operation with the following restrictions: ...operations are not allowed in the 5600-5650 MHz band (TDWR frequencies); and U-NII devices within 35 kilometers of a TDWR location shall be separated by at least 30 MHz (center frequency-to-center frequency) from the TDWR operating frequency."*

Significantly, tests conducted by the NTIA during the US government's investigation of this issue at a meteorological radar test facility demonstrated that the functionality of DFS did successfully avoid the meteorological radar channel and did not cause interference to the radar. Government and industry continue to study adjacent channel effects as a potential source of concern.

2.5.2 South Africa

Most South African meteorological radars have experienced interference from non-compliant equipment in the 5600-5650 MHz band, some of them being constantly interfered.

The South African weather services firstly tried to implement specific software filtering to improve the situation but then decided in 2011 to move its meteorological radar network in the 2700-2900 MHz band.

2.6 Possible Solutions and Actions

2.6.1 Guidance to manufacturers and notified bodies

2.6.1.1 Background

In the majority of the interference cases, the interference was caused by non-compliant equipment or non-compliant operation of initially compliant equipment. The feedback to the questionnaire also indicated that in a number of these cases, a Notified Body was involved in the assessment procedure which means that a positive opinion was issued for the equipment which nevertheless later on seems to have caused interference into the meteorological radars.

This guidance has the objective to better educate manufacturers as well as Notified Bodies as to prevent an incorrect or incomplete assessment is made for such equipment.

2.6.1.2 Responsibility

The final responsibility for equipment compliance remains with the manufacturer.

The sharing between a mass market license exempt application such as WAS/RLANs with another primary service like radio determination services (radar) is very challenging as a single non-compliant WAS/RLAN device can cause serious degradation of the radar operations. Therefore the measures to be taken by the manufacturer to prevent incorrect configuration or incorrect operation of his equipment, goes far beyond of what is normally seen as sufficient to ensure coexistence between the two services.

ETSI already recognized the problem in 2006 when it revised EN 301 893 (resulting in version 1.4.1) by including a specific requirement that prevents a manufacturer to provide an end user with a possibility to access any of the DFS related settings.

This guidance document provides a view on how that requirement has to be understood and implemented into the equipment. It goes far beyond of what has been understood before as being sufficient to comply with that requirement as a compliance rate of 99% is still not good enough to ensure interference free operation of meteorological radars.

More than for any other requirement for 5 GHz RLAN, the manufacturer cannot forward any responsibility for DFS compliance to the end user and make the assumption that he will correctly configure his equipment.

2.6.1.3 Requirement

Since EN 301 893 version 1.4.1, DFS controls (hardware or software) related to radar detection shall not be accessible to the user, thus DFS requirements can neither be disabled nor altered.

This end-result of this requirement should be that the user will not have any direct or indirect access to any of the DFS related settings or to a setting where there is any possibility to disable DFS.

Direct access

Direct access is understood as a setting or configuration accessible to the end user and where he can simply disable DFS or change any of the DFS related settings like the DFS threshold level, or settings related to the pulse width, repetition time, etc.

Indirect access

Indirect access is understood as any means for the end user to impact indirectly any of the DFS related settings or even disable DFS. The below provides a list of such means:

- Change the country of operation to a country where different DFS requirements apply or where no DFS applies at all;
- Download software/firmware in the equipment which is not intended for use within the European Union and which will impact the DFS performance or which may even disable DFS completely;
- Equipment for which the manufacturer has published their firmware as open source code on the internet. This code may include the DFS settings and as such any programmer can alter these settings and publish the modified code again on the internet;
- Downgrading the existing firmware to an earlier version resulting in the equipment no longer be compliant with the latest DFS requirements.

In order for the manufacturer to fully comply with the intent of this specific requirement added in EN 301 893 he shall:

- Prevent any direct access which could impact the DFS performance, i.e. that a means to disable or alter the DFS is prohibited;
- Prevent any indirect access which could impact the DFS performance;
 - Where the selection of the country of operation defines the configuration of the equipment, the selection of any country outside the EU (or the selection of a country where a different regulatory regime applies) should be prohibited;
 - The installation of software/firmware not intended for use within the European Union should be prohibited / prevented;
 - In case the manufacturer has published their firmware as open source code, the manufacturer will take measures as to prevent that new or modified firmware will impact the DFS performance of the equipment;

- The manufacturer shall prevent the downgrading of software if such downgrading would impact the DFS performance of the equipment.

In addition, the manufacturer shall provide sufficient warnings to end-users on the illegality of any modification (hardware or software) of the equipment which may impact the compliance of that equipment.

Where the manufacturer decides to involve a Notified Body in the conformity assessment procedure for aspects related to DFS, the Notified Body should do a full assessment of the equipment for all of the above aspects. It should never issue a positive opinion on the basis of statements made by the manufacturer.

2.6.2 Guidance to Enforcement Authorities

2.6.2.1 Background

Enforcement should act in a way to find out the initial source of an interference case and make the interference cease.

However, it is not sufficient to simply remove the interference by changing the WAS/RLAN operating frequency. A detailed investigation need to be done to find out why the WAS/RLAN did cause the interference.

- Was the DFS enabled or disabled?
- If DFS was enabled, and if compliance with EN 301 893 v 1.5.1 (or later versions) was declared, why did it not detect the radar?

If DFS was active, but did not detect the radar, further lab testing may be required to have it confirmed whether or not the equipment complies with the standard to which compliance was declared by the manufacturer.

For all cases considered in this Report, the WAS/RLAN was operating outdoor and in the majority of the cases, the interference was caused by non-compliant equipment or non-compliant operation of initially compliant equipment.. In addition, apart from one case where the WAS/RLAN was operating on the radar image frequency (which the RLAN is authorised to do so), in all other cases the WAS/RLAN was operating co-channel with the radar. It was reported that often the interference was stopped by re-configuring the WAS/RLAN on an operating frequency different from the radar operating frequency or sometimes even by simply re-enabling the DFS.

This document provides a more in depth view on how DFS works, and how it should be implemented in order to solve or prevent interference cases. It further analyses the 3 different means that, according to the feedbacks received, were used to solve the interference cases, but in reality the non-compliance of the equipment was not addressed hence the potential that these equipment would cause interference again at a later stage is real:

- Changing the WAS/RLAN operating frequency away from the radar frequency;
- Enabling DFS;
- Adjusting (reducing) Tx-power.

2.6.2.2 Changing the WAS/RLAN operating frequency

For the interference cases where it was found that the WAS/RLAN equipment was operating co-channel with the radar, it is obvious that re-configuring the WAS/RLAN equipment to a different frequency would stop the interference.

However 2 major observations must be made here:

1. If the DFS mechanism implemented by WAS/RLAN equipment was activated and effective then obviously this would have prevented the WAS/RLAN equipment from operating co-channel with the radar. This leads to the conclusion that the WAS/RLAN equipment is not compliant and should not

be allowed to be placed on the market. No attempt to re-configure the equipment shall be done. Enforcement authorities shall not allow such equipment to remain in use, even if it is not interfering with the radar anymore. Market enforcement and surveillance authorities are also advised to initiate appropriate actions to prevent further that such equipment is placed on the market. It is recommended that the equipment is submitted to a test laboratory to determine why the DFS mechanism is failing.

2. Reconfiguring the WAS/RLAN operating frequency will stop the interference instantaneously, but this could be just temporarily. The random (operating) channel selection, required as part of the DFS requirements, may select the initial radar operating channel again (by coincidence) as the new operating channel for the RLAN. This situation was reported several times.

2.6.2.3 (re-) Enabling DFS

For the interference cases where it was found that the DFS mechanism in the WAS/RLAN equipment was disabled, or where the equipment was configured to the wrong country (a country where DFS is not required), it is obvious that re-enabling DFS, or selecting the correct country of operation, might stop the interference.

However, there remains the risk that the user might alter these settings again which may cause interference to start again. The user should not have any direct or indirect access to settings which may impact DFS as otherwise the equipment cannot be declared compliant with the regulations. Since version 1.4.1. of EN 301 893, it has been made mandatory that none of the DFS related settings should be accessible to the user.

Therefore, in those interference cases where the DFS mechanism in the WAS/RLAN equipment was disabled, or where the equipment could be configured to a country where different or no DFS requirements apply, no effort should be undertaken to resolve the interference case by re-configuring the country of operation or by re-enabling DFS. Market enforcement shall prevent such equipment from being operated.

2.6.2.4 Adjusting Tx-power

Reducing Tx-output power may be efficient to stop a WAS/RLAN equipment, which is operating co-channel with the radar, from causing interference into this radar. However, the fact that interference was caused means that the DFS mechanism of the WAS/RLAN equipment simply does not work as intended.

The equipment is obviously not compliant. It is recommended that the equipment is submitted to a test laboratory to determine why the DFS mechanism is failing. Market enforcement shall not allow operation of such equipment.

2.6.2.5 Conclusion

In those cases where the WAS/RLAN was operating co-channel with the radar and caused interference into the radar, no effort should be made to solve the interference case by

1. re-configuring the WAS/RLAN equipment to a different channel, or by
2. re-enabling DFS again (where it was disabled), or by
3. reducing the Tx-output power.

The equipment is simply not compliant with the regulations. Appropriate action against non-compliant equipment shall be taken. Market enforcement shall not allow such equipment to be operated or remain in use. Market enforcement and surveillance authorities are also advised to initiate appropriate actions to prevent further that such equipment is placed on the market.

In case of a failing DFS mechanism, the enforcement authority are recommended to have lab tests performed to find out why the equipment did not operate as intended.

Enforcement authorities should inform WAS/RLAN users about the consequences of the illegal use of WAS/RLAN equipment, i.e. causing interference to meteorological radars.

It would be desirable to find solutions such that users/ consumers become more aware of the existing problems with non-compliant equipment and get some guidance from authorities.

With regard to guidance provided in this report, France and the Czech Republic have developed a national procedure in order to deal with interference cases between meteorological radars and WAS/RLAN systems. These procedures are detailed in Annex 2 of this report as country cases.

2.6.2.6 Other aspects to be verified by enforcement authorities

1. Possibility to select a country outside the EU or to select a country where no DFS or different DFS requirements apply

Enforcement authorities need to be aware that the manufacturer may only have one single (global) version of the product. The correct configuration of the equipment is supposed to be done by the selection of the country of operation at initial start-up. But the risk is real that by selecting a country outside the EU (or the selection of a country where a different regulatory regime applies) that the DFS in the WAS/RLAN equipment does not operate as required for the actual country of operation, or in worst case, that the DFS is even disabled.

Such an approach is not allowed. It should not be possible that the DFS does not operate as intended by an incorrect setting of the country of operation. Enforcement authorities are advised to take appropriate action to prevent such equipment is further placed on the market.

2. Downloading software/firmware not intended for the EU market

Most WAS/RLAN equipment is designed to support a firmware/software upgrade process. This allows the manufacturer to provide enhancements or to address bug fixes to equipment already placed on the market and installed.

Because of the different regulatory environments, manufacturers are forced to make regional specific products which cannot be altered by the end user. This also means that they have to provide regional specific software/firmware upgrades.

Manufacturers must also prevent equipment that will accept the installation of software which is not intended for this product (wrong region or country) and which might change the regulatory compliance of that equipment. That means that equipment intended for the EU market shall only accept the installation of new software/firmware which ensures compliance of the equipment with the EU regulations. It shall not accept the installation of software/firmware intended for other regulatory domains. Enforcement authorities are advised to take appropriate action against all economic players to prevent such equipment is further placed on the market.

3. Uniform spreading - The avoidance of the band 5600 to 5650 MHz

The manufacturer may decide to permanently block the band 5600 to 5650 MHz in his equipment. Alternatively he can leave that choice to the end-user or the operator by at least providing the option to permanently block these frequencies when configuring the equipment. Such configuration should not be seen as a violation of the Uniform Spreading requirement as according to the ETSI standard EN 301 893, the equipment should only be capable to operate over at least 60% of the total spectrum available. So even if this spectrum is blocked, there is sufficient spectrum left to comply with the uniform spreading requirement.

2.6.3 Additional solutions to improve the situation

The following possibilities have been discussed to improve the current situation:

- Maintain and publish a list of non-compliant equipment

It could be beneficial to maintain and publish a list of non-compliant equipment for which Member States had initiated a safeguard clause in accordance with the R&TTE Directive. Users and retailers are often not aware of the consequences of using non-compliant equipment and therefore such a list may help them.

- Availability of a database with the location of outdoor fixed links using 5 GHz WAS/RLANs

This approach was adopted by FCC as a measure to address the interference from WAS/RLAN to meteorological radars. This database is created and maintained by some RLAN industries and is on a voluntary basis in the USA. This Report does not recommend such an option of creating a database.

- Revision of EN 301 893

Although EN 301 893 prohibits the equipment to provide the user direct access to any of the DFS settings, this Report identifies means which may indirectly impact the DFS mechanism, including potential disablement of DFS (see section 2.6.1.3). Solutions may potentially be found through a further enhancement of the applicable standards. A new work item for the revision of the Harmonised Standard EN 301 893 has already been adopted.

3 CONCLUSIONS

This Report shows that all investigated interference cases relate to outdoor WAS/RLAN fixed installations operating co-channel with the radar, although, due to the lack of information which did not allow concluding on the origin of the interference, some of these cases were not further investigated.

It is also emphasised that short-term interference events have been reported but the short duration of these cases does not give the opportunity for administrations to further investigate the situation and to identify the source of the interference.

The analysis of reported interference cases leads to the following categories:

Intentional illegal use:

- A considerable number of the reported interference cases were caused by equipment where the DFS mechanism was disabled;
- In some cases, higher gain antennas were used resulting in e.i.r.p. levels above the regulatory limits. However, if the DFS mechanism is active and efficient, the use of higher gain antennas should not result in interference towards radars.

Non-compliant equipment

The main reasons for non-compliance are:

- Alteration/ disablement of DFS settings possible by the user (EN 301 893 version 1.4.1 and higher does not allow the user to disable DFS or alter the DFS settings). In some of these cases Notified Bodies had issued a positive opinion to this non-compliant equipment.
- In those interference cases where the DFS mechanism in the WAS/RLAN equipment is disabled, or where the equipment could be configured to a country where different or no DFS requirements apply, market enforcement shall not allow such equipment to be operated or remain in use and no effort should be undertaken to resolve the interference case by re-configuring the country of operation or by re-enabling DFS;
- In some cases, where DFS was disabled, re-enabling DFS did not cause the equipment to detect the radar. The DFS did not function as intended (non-compliant DFS).
- Market enforcement and surveillance authorities are also advised to initiate appropriate actions to prevent further that such equipment is placed on the market. It is also recommended that the equipment is submitted to a test laboratory to determine why the DFS mechanism is failing.

The findings of the present report have been confirmed by the TCAM ADCO market surveillance campaign that shows quite a high percentage of non-compliant equipment among those considered. TCAM/ADCO recommends that market surveillance authorities to increase the amount of inspections on 5GHz WLANs until the situation will have improved.

In those cases where the WAS/RLAN is operating co-channel with the radar and is causing interference into the radar, market enforcement shall not allow such equipment to be operated or remain in use and no effort should be made to solve the interference case by

1. Re-configuring the WAS/RLAN equipment to a different channel, or by
2. Re-enabling DFS again (where it was disabled), or by
3. Reducing the Tx-output power.

The case should be passed to the national responsible market surveillance authority for an action that can end in a safeguard clause procedure to ban the considered equipment from the European market.

Interferences due to equipment placed on the market at an earlier stage (compliant with an earlier standard version) should be dealt with on a case by case basis to solve the interference.

It could be beneficial to maintain and publish a list of non-compliant equipment for which Member States had initiated a safeguard clause in accordance with the R&TTE Directive. It would be desirable to find solutions such that users/ consumers and retailers become more aware of the existing problems with non-compliant equipment and get some guidance from authorities and such a list may help them.

Notified Bodies

Notified Bodies shall not issue a positive opinion for the cases described above where the equipment is clearly non-compliant. Notified Bodies should consider the guidance provided in the present Report when assessing 5 GHz WAS/RLAN equipment.

The development of additional guidance to manufacturers and Notified Bodies is recommended (see section 2.6.1).

Incomplete investigation / inadequate actions by enforcement authorities

Most of the reported interference cases remained ultimately inconclusive because of key information was not collected, the investigations were incomplete or the action was inadequate.

However, despite these incomplete investigations, it can still be concluded that there is a considerable number of cases of intentional illegal use or non-compliant equipment.

Market enforcement authorities should consider the guidance provided in this report and increase their efforts to take appropriate action against non-compliant equipment or non-compliant operation of equipment. There was

- Insufficient or no investigation at all on why DFS did not work as intended;
- No action against non-compliant or illegally used equipment.

A good cooperation and coordination between national market surveillance and market enforcement action is important to solve 5 GHz DFS interference problems.

Enforcement authorities should inform WAS/RLAN users about the consequences of the illegal use of WAS/RLAN equipment, i.e. causing interference to meteorological radars.

Compliance with ETSI standards

Considering investigated interference cases, no issues have been identified with regard to short comings in the specifications of the DFS mechanism itself as specified in the current version of the Harmonised European Standard EN 301 893 (i.e. – v1.5.1 and above). No investigated interference case can be traced back to failure of the DFS mechanism. Therefore, it may be assumed that equipment fully compliant with this standard provides adequate protection to radars.

Although EN 301 893 prohibits the equipment to provide the user direct access to any of the DFS settings, this Report identifies means which may indirectly impact the DFS mechanism, including potential disablement of DFS (see section 2.6.1.3). Solutions may potentially be found through a further enhancement of the applicable standards.

ANNEX 1: ITU-R RESOLUTION 229

Resolution 229 (WRC-03)

Use of the bands 5 150-5 250 MHz, 5 250-5 350 MHz and 5 470-5 725 MHz by the mobile service for the implementation of wireless access systems including radio local area networks

The World Radiocommunication Conference (Geneva, 2003),

considering

- a) that this Conference has allocated the bands 5 150-5 350 MHz and 5 470-5 725 MHz on a primary basis to the mobile service for the implementation of wireless access systems (WAS), including radio local area networks (RLANs);
- b) that this Conference has decided to make an additional primary allocation for the Earth exploration-satellite service (EESS) (active) in the band 5 460-5 570 MHz and space research service (SRS) (active) in the band 5 350-5 570 MHz;
- c) that this Conference has decided to upgrade the radiolocation service to a primary status in the 5 350-5 650 MHz band;
- d) that the band 5 150-5 250 MHz is allocated worldwide on a primary basis to the fixed-satellite service (FSS) (Earth-to-space), this allocation being limited to feeder links of non-geostationary-satellite systems in the mobile-satellite service (No. **5.447A**);
- e) that the band 5 150-5 250 MHz is also allocated to the mobile service, on a primary basis, in some countries (No. **5.447**) subject to agreement obtained under No. **9.21**;
- f) that the band 5 250-5 460 MHz is allocated to the EESS (active) and the band 5 250-5 350 MHz to the SRS (active) on a primary basis;
- g) that the band 5 250-5 725 MHz is allocated on a primary basis to the radiodetermination service;
- h) that there is a need to protect the existing primary services in the 5 150-5 350 MHz and 5 470-5 725 MHz bands;
- i) that results of studies in ITU-R indicate that sharing in the band 5 150-5 250 MHz between WAS, including RLANs, and the FSS is feasible under specified conditions;
- j) that studies have shown that sharing between the radiodetermination and mobile services in the bands 5 250-5 350 MHz and 5 470-5 725 MHz is only possible with the application of mitigation techniques such as dynamic frequency selection;
- k) that there is a need to specify an appropriate e.i.r.p. limit and, where necessary, operational restrictions for WAS, including RLANs, in the mobile service in the bands 5 250-5 350 MHz and 5 470-5 570 MHz in order to protect systems in the EESS (active) and SRS (active);
- l) that the deployment density of WAS, including RLANs, will depend on a number of factors including intrasystem interference and the availability of other competing technologies and services,

further considering

- a) that the interference from a single WAS, including RLANs, complying with the operational restrictions under *resolves* 2 will not on its own cause any unacceptable interference to FSS receivers on board satellites in the band 5 150-5 250 MHz;
- b) that such FSS satellite receivers may experience an unacceptable effect due to the aggregate interference from these WAS, including RLANs, especially in the case of a prolific growth in the number of these systems;
- c) that the aggregate effect on FSS satellite receivers will be due to the global deployment of WAS, including RLANs, and it may not be possible for administrations to determine the location of the source of the interference and the number of WAS, including RLANs, in operation simultaneously,

noting

that, prior to WRC-03, a number of administrations have developed regulations to permit indoor and outdoor WAS, including RLANs, to operate in the various bands under consideration in this Resolution,

recognizing

- a) that in the band 5 600-5 650 MHz, ground-based meteorological radars are extensively deployed and support critical national weather services, according to footnote No. **5.452**;

- b) that the means to measure or calculate the aggregate pfd level at FSS satellite receivers specified in Recommendation ITU-R S.1426 are currently under study;
- c) that certain parameters contained in Recommendation ITU-R M.1454 related to the calculation of the number of RLANs tolerable by FSS satellite receivers operating in the band 5 150-5 250 MHz require further study;
- d) that the performance and interference criteria of spaceborne active sensors in the EESS (active) are given in Recommendation ITU-R SA.1166;
- e) that a mitigation technique to protect radiodetermination systems is given in Recommendation ITU-R M.1652;
- f) that an aggregate pfd level has been developed in Recommendation ITU-R S.1426 for the protection of FSS satellite receivers in the 5 150-5 250 MHz band;
- g) that Recommendation ITU-R SA.1632 identifies a suitable set of constraints for WAS, including RLANs, in order to protect the EESS (active) in the 5 250-5 350 MHz band;
- h) that Recommendation ITU-R M.1653 identifies the conditions for sharing between WAS, including RLANs, and the EESS (active) in the 5 470-5 570 MHz band;
- i) that the stations in the mobile service should also be designed to provide, on average, a near-uniform spread of the loading of the spectrum used by stations across the band or bands in use to improve sharing with satellite services;
- j) that WAS, including RLANs, provide effective broadband solutions;
- k) that there is a need for administrations to ensure that WAS, including RLANs, meet the required mitigation techniques, for example, through equipment or standards compliance procedures,

resolves

- 1 that the use of these bands by the mobile service will be for the implementation of WAS, including RLANs, as described in Recommendation ITU-R M.1450;
- 2 that in the band 5 150-5 250 MHz, stations in the mobile service shall be restricted to indoor use with a maximum mean e.i.r.p.¹ of 200 mW and a maximum mean e.i.r.p. density of 10 mW/MHz in any 1 MHz band or equivalently 0.25 mW/25 kHz in any 25 kHz band;
- 3 that administrations may monitor whether the aggregate pfd levels given in Recommendation ITU-R S.1426² have been, or will be exceeded in the future, in order to enable a future competent conference to take appropriate action;
- 4 that in the band 5 250-5 350 MHz, stations in the mobile service shall be limited to a maximum mean e.i.r.p. of 200 mW and a maximum mean e.i.r.p. density of 10 mW/MHz in any 1 MHz band. Administrations are requested to take appropriate measures that will result in the predominant number of stations in the mobile service being operated in an indoor environment. Furthermore, stations in the mobile service that are permitted to be used either indoors or outdoors may operate up to a maximum mean e.i.r.p. of 1 W and a maximum mean e.i.r.p. density of 50 mW/MHz in any 1 MHz band, and, when operating above a mean e.i.r.p. of 200 mW, these stations shall comply with the following e.i.r.p. elevation angle mask where θ is the angle above the local horizontal plane (of the Earth):

-13 dB(W/MHz)	for $0^\circ \leq \theta < 8^\circ$
$-13 - 0.716(\theta - 8)$ dB(W/MHz)	for $8^\circ \leq \theta < 40^\circ$
$-35.9 - 1.22(\theta - 40)$ dB(W/MHz)	for $40^\circ \leq \theta \leq 45^\circ$
-42 dB(W/MHz)	for $45^\circ < \theta$;

¹ In the context of this Resolution, "mean e.i.r.p." refers to the e.i.r.p. during the transmission burst which corresponds to the highest power, if power control is implemented.

² $-124 - 20 \log_{10}(\text{hSAT} / 1\,414)$ dB(W/(m² · 1 MHz)), or equivalently, $-140 - 20 \log_{10}(\text{hSAT} / 1\,414)$ dB(W/(m² · 25 kHz)), at the FSS satellite orbit, where hSAT is the altitude of the satellite (km).

5 that administrations may exercise some flexibility in adopting other mitigation techniques, provided that they develop national regulations to meet their obligations to achieve an equivalent level of protection to the EESS (active) and the SRS (active) based on their system characteristics and interference criteria as stated in Recommendation ITU-R SA.1632;

6 that in the band 5 470-5 725 MHz, stations in the mobile service shall be restricted to a maximum transmitter power of 250 mW³ with a maximum mean e.i.r.p. of 1 W and a maximum mean e.i.r.p. density of 50 mW/MHz in any 1 MHz band;

7 that in the bands 5 250-5 350 MHz and 5 470-5 725 MHz, systems in the mobile service shall either employ transmitter power control to provide, on average, a mitigation factor of at least 3 dB on the maximum average output power of the systems, or, if transmitter power control is not in use, then the maximum mean e.i.r.p. shall be reduced by 3 dB;

8 that, in the bands 5 250-5 350 MHz and 5 470-5 725 MHz, the mitigation measures found in Annex 1 to Recommendation ITU-R M.1652 shall be implemented by systems in the mobile service to ensure compatible operation with radiodetermination systems,

invites administrations

to adopt appropriate regulation if they intend to permit the operation of stations in the mobile service using the e.i.r.p. elevation angle mask in *resolves* 4, to ensure the equipment is operated in compliance with this mask,

invites ITU-R

1 to continue work on regulatory mechanisms and further mitigation techniques to avoid incompatibilities which may result from aggregate interference into the FSS in the band 5 150-5 250 MHz from a possible prolific growth in the number of WAS, including RLANs;

2 to continue studies on mitigation techniques to provide protection of EESS from stations in the mobile service,

3 to continue studies on suitable test methods and procedures for the implementation of dynamic frequency selection, taking into account practical experience.

³ Administrations with existing regulations prior to this Conference may exercise some flexibility in determining transmitter power limits.

ANNEX 2: COUNTRY CASE IMPLEMENTING GUIDANCES PROVIDED IN THE PRESENT ECC REPORT

France:

The following information is only provided as an example on how the French administration has implemented recommendations from this Report to deal with interference cases from WAS/RLAN devices into meteorological radars. This procedure was recently developed and is subject to further modifications in order to accommodate the described procedures and their applicability.

Three situations are handled:

- a. DFS disabled – equipment compliant with EN 301 893 version 1.4.1 (or above) which is no longer placed on the market;
- b. DFS disabled/enabled – equipment compliant with EN 301 893 version 1.4.1 (or above) which is still placed on the market;
- c. DFS enabled – equipment compliant with EN 301 893 version prior to v1.4.1 and which is no longer placed on the market;

Situation a) : *Analysis*

The DFS functionality should not have been disabled. Nevertheless, such equipment is not any more placed on the market and hence a market surveillance action cannot be envisaged. In this situation the French law offers the possibility to withdraw the equipment/ the network as appropriate from operation by decree signed by the Minister in charge of Electronic Communications.

Procedure

- **A letter** is sent to the manufacturer which includes explanations on non-conformity, requesting the manufacturer to put the non-compliant equipment family in conformity, requesting the manufacturer to inform ANFR (the French relevant public authority for market surveillance) about measures being undertaken, and informing the manufacturer that if no response was received on this letter the Minister in charge of Electronic communications will be legally entitled to publish a decree to withdraw the equipment on a national basis from service;
- **A fine** is applied to the user of the network which caused the interference;
- **A decree** to withdraw from service is published after a contradictory procedure between public relevant authorities and the manufacturer and if there is no cooperation from the manufacturer to put its equipment in conformity.

Situation b) : *Analysis*

A market surveillance action is initiated to perform measurements in order to check the conformity of the equipment and identifying the cause of the interference. Depending on the results of the conformity test and discussions with the manufacturer, a national decree may be published and a safeguard clause procedure may be initiated at the European Level.

Procedure

- **Two devices are seized on the market** to perform conformity tests by an accredited laboratory;
- In case of identified non-conformity, **a letter** is sent to the manufacturer which includes explanations on non-conformity, requesting the manufacturer to put the non-compliant equipment “family” in conformity, inviting the manufacturer to contact its client in order to upgrade its equipment as appropriate, requesting the manufacturer to inform ANFR accordingly on measures being undertaken and informing the manufacturer that in case of non-cooperation from its side, the Minister in charge of Electronic communications will be legally entitled to publish a decree to withdraw the equipment from the market on a national basis and that this measure can then be extended to the whole European Union.
- **A fine** is applied to the user of the network that causes the interference;

- **A national decree** to withdraw from the market the incriminated equipment is published after a contradictory procedure between public relevant authorities and the manufacturer and if there is no cooperation from the manufacturer to put its equipment in conformity.
- **A safeguard clause** will be initiated by France at the EU level.

Situation c) : *Analysis*

On the one hand, the DFS settings could have been made accessible to the user and on the other hand, the DFS requirements were not sufficient to grant protection to radars. In this case, if the date of purchase of the equipment is consistent with the validity date of this version of the standard, then the equipment is compliant. However, if the DFS is disabled so its use is not in accordance with the current regulation which requires the DFS, then the situation and actions are similar to those applied in situation a).

If the DFS is enabled the following procedure is applied.

Procedure

- **A letter** is sent to the user which includes information on current regulation and will invite the user to contact the manufacturer in order to update its equipment;

A fine is applied to the user of the network which causes the interference.

Czech Republic:

Cooperation between the national regulatory authority CTO (Czech Telecommunication Office) and the Czech Hydro Meteorological Institute (CHMI) proved to be necessary for the effective solution of complains.

- CHMI provides clear and unambiguous identification of interfering equipment to CTO (voluntary base, mutual agreement),
- CTO carries out accelerated steps to close down interference (2-3 days),
- Only clear/unique identification of interferer can lead to later legal steps against him (fine, cease the operation).

Identification of interfering equipment is carried out by CHMI. Measurement is made directly at the output of radar dish antenna.

For unambiguous identification of sources it is necessary to measure:

- the MAC address of WAS/RLAN equipment (unique),
- azimuth,
- receiving level, SSID, communication.

The measurements are done during regular radar maintenance, if appropriate also in other cases when the interference is too strong or long-lasting.

The information is compared with a database of WAS/RLAN equipment (outdoor installed WAS/RLAN to be notified to CTO by the users) which is used as much as possible during the interference investigation to see whether the owner is known, measured already earlier, or whether there is no information in the database.

CTO is penalising all cases of harmful interference according to §100 of the Czech telecommunication act – „equipment provider must not cause any interference to other communication means and services’

Example of identification of interference sources at the radar antenna output

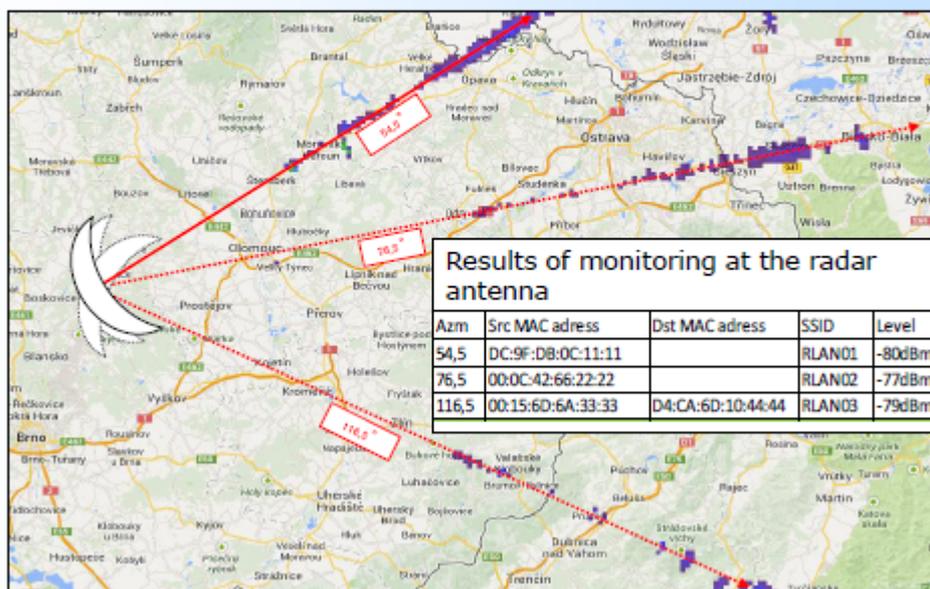


Figure 9: Example of identification of interference sources

More detailed information about the approach is given in document FM22(14)45rev1 [12]

ANNEX 3: LIST OF REFERENCE

- [1] ETSI Harmonised European Standard EN 301 893 for 5 GHz high performance RLAN
- [2] ECC Recommendation (06)04 on the use of the band 5725-5875 MHz by BFWA
- [3] DA 12-459: FCC Enforcement Advisory No. 2012-07- Enforcement Bureau Takes Action to Prevent Interference to FAA-Operated Terminal Doppler Meteorological radars Critical to Flight Safety
- [4] Resolution 229 (WRC-03) Use of the bands 5 150-5 250 MHz, 5 250-5 350 MHz and 5 470-5 725 MHz by the mobile service for the implementation of wireless access systems including radio local area networks
- [5] Recommendation ITU-R M.1652: Dynamic frequency selection in wireless access systems including radio local area networks for the purpose of protecting the radiodetermination service in the 5 GHz band
- [6] ECC Decision (04)08 on the harmonised use of the 5 GHz frequency bands for the implementation of Wireless Access Systems including Radio Local Area Networks (WAS/RLANs)
- [7] EC Decision 2005/513/EC: Commission Decision on the harmonised use of radio spectrum in the 5 GHz frequency band for the implementation of wireless access systems including radio local area networks (WAS/RLANs)
- [8] EC Decision 2007/90/EC: Commission Decision amending Decision 2005/513/EC on the harmonised use of radio spectrum in the 5 GHz frequency band for the implementation of Wireless Access Systems including Radio Local Area Networks (WAS/RLANs)
- [9] Recommendation ITU-R M.1638: Characteristics of and protection criteria for sharing studies for radiolocation, aeronautical radionavigation and meteorological radars operating in the frequency bands between 5 250 and 5 850 MHz
- [10] Directive 1999/5/EC of the European Parliament and the Council on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity
- [11] ETSI Harmonised European Standard EN 302 502 for 5.8 GHz fixed broadband data transmitting systems
- [12] FM22(14)45rev1: Interference of meteorological radar & CTO
- [13] FM(17)177 Annex 5: Summary of discussions based on the replies of CEPT administrations to the questionnaire on interference cases caused by WAS/RLAN in meteorological radars operating in the 5600 - 5650 MHz frequency range