R&TTE Market Surveillance Campaign on WLAN 5GHz

Background

- Terrestrial radars are operating in the 5250-5350 MHz and 5470-5725 MHz frequency bands
- 5150-5350 MHz and 5470-5725 MHz were allocated to WAS/RLANs 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)**."
- Resolution 229 (WRC-03) specifies tha this allocation was made under the condition that mitigation techniques such as DFS shall be used to enable sharing with terrestrial radars.

DFS requirements (Master devices)

- 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, master device shall :
  - stop normal operation on this channel
  - 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.

DFS requirements (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.

Interference cases (see also ECC REPORT 192)

- Interference management authorities reported many cases where terrestrial radars (metrological radars) were interfered.
- The analysis of reported interference cases leads to the following categories:
  - Intentional illegal use
    - equipment where the DFS mechanism was disabled
    - higher gain antennas were used resulting in e.i.r.p. levels above the regulatory limits
  - Non compliant equipment
    - Alteration/ disablement of DFS settings possible by the user or DFS can be deactivated by changing the country setting
    - The DFS did not function as intended (non-compliant DFS)

Aim of the campaign

- Target on WLAN 5 GHz on the market
- Assess compliance with DFS specific requirement
- Determine the compliance rate on DFS specific requirement
- Remove all non compliant equipment from market
- Subsequent measures in case of non-compliance was at the discretion of participating market surveillance authorities (MSA)
- 21 MSA participated

Samples

Participating MSA had to

- take at least 5 WLAN 5 GHz on their market.
- take the samples randomly on their market to have a correct picture of the situation on the market.
- avoid checking of the same product

Harmonised Standards and other regulations

- ETSI EN 301 893 – Broadband Radio Access Networks (BRAN);5 GHz high performance RLAN;,
- ETSI EN 302 502 - Broadband Radio Access Networks (BRAN); 5,8 GHz fixed broadband data transmitting systems;
- ETSI TR 102 651 - Guide to the implementation of Dynamic Frequency Selection (DFS),
- ECC/DEC/(04)08 - ECC Decision of 09 July 2004 on the harmonised use of the 5 GHz frequency bands for the implementation (WAS/RLANs),

Type of samples

Scope of samples taken from the market			
Group of samples	**Radar detection required**	**Number of samples**	**Percentage**
Devices operate only in 5150-5250 MHz	No	35	34,65%
Devices operate in 5 GHz band only in slave mode with maximum e.i.r.p of less than 23dBm	No	2	1,98%
Other 5 GHz devices	Yes	64	63,37%
All taken devices	**101**		**100,00%**

Compliance of products

Participating MSA have checked if each chosen WLAN fulfill administrative requirements and the "user access restrictions" requirement according to the applicable harmonised standard (EN 301 893)

Compliance with assessed requirements		
Number checked	**Number compliant**	**Compliance [%]**
64	18	28,13%

Administrative compliance (1)

Compliance with CE marking requirements				
Number assessed	Not fulfil CE mark layout	Not fulfil CE mark height	Overall CE marking compliance	Overall CE marking compliance [%]
64	1	8	56	87,50%

Compliance with DoC requirements				
Number assessed	DoC available*	DoC available [%]	DoC compliance	DoC compliance [%]
64	48	75%	41	64,06%
* Note: Complete form and short form.				

Administrative compliance (2)

Compliance with TD requirements				
Number assessed	TD available	TD available [%]	TD compliance	TD compliance [%]
47	40	85,11%	23	48,94%

Compliance with administrative requirements		
Number checked	Number compliant	Compliance [%]
64	21	32,81%

Dynamic Frequency Selection

Dynamic Frequency Selection is a mechanism that allows WLANs devices to operate in 5250-5350 MHz and 5470-5850MHz bands without causing harmful interferences to maritime and weather radars which have a priority right to use that band. Terms of DFS implementation are described in harmonized standard EN 301 893 and EN 302 502

Implementation of DFS		
Number checked	DFS not implemented	DFS not implemented [%]
64	3	4,69%

Dynamic Frequency Selection - deactivation

High occupancy and penetration of 5GHz band causes that WLANs users try to directly or indirectly deactivate DFS functionality.

In about 35% of tested devices (about 1 of 3), firmware allowed the end-user to switch off DFS function

Deactivation of DFS		
Number checked	DFS can by deactivated	DFS can by deactivated [%]
64	22	34,38%

Dynamic Frequency Selection - deactivation

In some cases it is necessary for user to update device firmware with the new version, alternative version or even old version which allows to deactivate DFS function. Detailed information about ways to deactivate DFS function can be found in user manual or manufacture's web page.

Ways of DFS deactivation				
Number checked	User manual indicates how to deactivate DFS	Firmware/software allows to deactivate DFS	Web site suggests a firmware update to deactivate DFS	Web site indicates how to deactivate DFS
22	7	20	5	4

Dynamic Frequency Selection - deactivation

EN 301 893 states that DFS controls (hardware or software) related to radar detection shall not be accessible to the user so that the DFS requirements described in clauses 4.7.2.1 to 4.7.2.6 can neither be disabled nor altered.

Setting of "Region of use"		
Number checked	Region of use can be changed	Region of use can be changed [%]
64	38	59,38%

Conclusions (1)

- 35 of 101 (35%) WLANs avoided frequency bands where DFS is mandatory.
- Almost all WLANs (95%) which are using frequency bands where the DFS system is mandatory have the DFS function implemented.
- 22 of 64 (34%) WLANs can have DFS deactivated by the user, in 91% cases by using WLANs' original or provided on manufacturer's web site firmware.
- 38 of 64 (59%) WLANs give the possibility to the user to change the "Region of use".

Conclusions (2)

- The availability of the TD (85%) is not satisfactory.
- The overall level of compliance of TD is low (49%).
- Low overall compliance with the assessed requirements (28%)
  [even if the level of compliance of the CE marking (88%) and compliance of DoC (64%) is higher than in previous MSC under the R&TTE directive].

Conclusions (3)

- The firmware can have an important and a deliberate impact on the compliance to the essential requirements of a state of the art radio equipment.

- This campaign confirmed the problem identified by interference management people and contained in the ECC liaison statement.

- Number of participating MSA (21) in campaign is satisfactory and showed a good level of cooperation between MSAs.

Recommendations (1)

- MSA should continue to check such products and take all appropriate measures to ban non compliant product from the market.

- It should be ensured that the change of the “Region of use” do not alter or disable the DFS functionality.

- In a general way it should be ensured that changes of “Region of use” cannot alter the compliance against the essential requirements.

Recommendations (2)

- All relevant firmware release numbers that may alter the compliance to the essential requirements, shall be considered during the evaluation of the conformity of a radio equipment.

- For reproducibility reasons the manufacturer shall indicate in the test report, a part of the technical documentation, all relevant firmware release numbers.

Recommendations (3)

- ADCO R&TTE discussed the results with ECC, ETSI and industry the possibilities to solve the problem and increase the level of conformity of 5 GHz WLAN on the market.

- The cooperation at national level between interference management and market surveillance authorities should be improved to detect rapidly non compliant products as possible sources of interferences and to take them off the market.

Recommendations (4)

- Due to high influence of non-compliant WLANs on radiolocation systems and ground-based meteorological radars MSAs were asked to increase the amount of inspections on 5GHz WLANs until the situation has improved. MSA should regularly report to ADCO R&TTE.


MERCI!
THANK YOU!
FRAPAR.

Contact

Lucio Cocciantelli
ADCO R&TTE Chairman
Head of section
Federal Department of the Environment,
Transport, Energy and Communication DETEC
Federal Office of Communications OFCOM
Section Market access and conformity
Zukunftstrasse 44, CH 2501 Biel
Phone +41 58 460 55 59 (direct)
Fax +41 58 460 55 55
mailto:lucio.cocciantelli@bakom.admin.ch
www.ofcom.admin.ch