DFS Compliance Criteria, status and prospects

Jan Kruys, Oaktree Wireless

Summary

Recent events taking place in US (the FCC's freezing of outdoor RLAN deployments) and Europe (the EUMETNET concerns over RLAN on board aircraft causing interference into ground-based weather radars) have the effect of casting doubt on the concept of DFS and the capabilities of its implementations. This white paper discusses how the awkward relationship between the DFS real world requirements and the DFS compliance criteria may lead to such concerns – whereas real world conditions assure a properly implemented DFS capability will serve it purpose: protecting radar system from interference.

By proper analysis of the factors involved – including effective beam width of a radar system and the statistics of pulse detection in the presence of other signals – one can determine the essential factors of DFS performance and use them to set compliance criteria that serve the interests of all concerned: the incumbents as well as the Wi-Fi industry and the regulators by avoiding future headaches.

Introduction

The 5GHz band is a prime resource for the RLAN industry and RLAN users, notably in view of the 40MHz channel width introduced by the MIMO capability defined by Amendment "n" of the IEEE 802.11 specification. Using that spectrum requires the implementation of radar detection and avoidance mechanisms usually referred to as "DFS" – Dynamic Frequency Selection. To make sure DFS capable equipment meets its requirements, DFS compliance criteria have been developed in cooperation between industry and frequency regulators.

The successful use of DFS requires that these compliance criteria reflect real life conditions and avoid both under- and over-specification: all relevant radar signals should be detected at the lowest possible cost of RLAN implementation and operation.

Under-specification can cause failure in real life conditions, over- specification leads to unnecessary operational constraints and high costs in development and testing. The current DFS compliance criteria (US -FCC, EU-ETSI, Japan-MIT) are in some ways both under- and over-specified and this leads to risks of spectrum closure demands (see EUMETNET's demands for the 5600-5650MHz band) as well as reduced usage of the highly valuable 5GHz frequencies.

By proper analysis of the factors involved – including effective beam width of a radar system and the statistics of pulse detection in the presence of other signals – one can determine the essential factors of DFS performance and use them to set compliance criteria that serve the interests of all concerned: the incumbents as well as the Wi-Fi industry and the regulators by avoiding future headaches. This white paper provides such an analysis and proposes the development of new criteria, notably for detection probability. Ideally these criteria should be acceptable world-wide so as to avoid the costs of multiple (certification) tests. Working out the details of new criteria as well as the test procedures should be done in cooperation between both all concerned: incumbents, industry and regulators.

The importance of DFS

Increasing use of the2.4GHz band by an ever broader variety of wireless devices will further reduce the Wi-Fi user experience, possibly to the point where people will revert to wired solutions.

With that prospect in mind, the wireless industry sought and obtained a large amount of "extension" spectrum – at 5GHz a total of 455MHz is available in most countries the world over. This process was started in 1997 and took 6 years to yield fruit in 2003 in the form of ITU-R Resolution 229 1] and its attendant Recommendation M.1652 2] which provided the means to assure co-existence between RLANs and the main incumbents of the 5GHz band: high power radar systems.

M.1652 requires the detection and avoidance of co-channel operation with civilian and military radars. This capability is known as DFS –Dynamic Frequency Selection. The basic DFS capability and its associated certification criteria were developed in the preparations for the World Radio Conference of 2003. This document has served as the basis for the DFS requirements in force in the US, in the EU, Canada and Japan.

The core concept of DFS

DFS is based on the fact that radar systems produce highly concentrated RF power pulses that can be detected easily, and therefore reliably, by RLANs so that operating co-channel with a radar system can be avoided. Radars scan their environment in sectors or full revolutions; this scanning results in objects within the radar's range being illuminated for short periods by burst of pulses. The length of such bursts varies with the radar's pulse repetition rate, its rotation rate and its antenna gain pattern. DFS performance is defined in terms of detection probabilities for such bursts.

RLANs need a means to separate radar emissions from packets sent out be nearby RLANs and from environmental RF noise and therefore a minimum number of pulses is necessary, regardless of the pulse rate. This minimum serves as a false alarm threshold [1] only. More pulses provide a better burst detection probability. Detection is also affected by the RLAN's own transmissions and therefore a busy RLAN needs to be illuminated with more pulses in order to assure radar detection but an idle RLAN needs only a few pulses more than the threshold for such assurance.

Essential to the success of DFS in assuring effective co-existence of high powered radars and large numbers of RLANs in the 5GHz band is that radar detection is very efficient so that interference is avoided. Two modes of detection have been defined: the Channel Availability Check performed before the use of a channel and In Service Monitoring performed while the RLAN is operating on a channel.

The DFS compliance criteria define detection probabilities for different burst lengths and different pulse rates for RLANs that are idle (required during the Channel Availability Check) and that are operating at 50% load (during the In Service Monitoring).

The importance of DFS Compliance Criteria

The purpose of the DFS compliance criteria is to determine whether equipment is able to effectively protect radar systems by reliably detecting their emissions. These criteria should correspond in some sense to reality and take into account radar signal propagation and detector properties. If such factors are ignored the consequences are largely negative, in one way or another.

[1] The threshold depends to some degree on the design of the detector: if the interval between pulses is the only criterion, at least three pulses are needed to detect a constant pulse repetition radar, if the pulse rate is staggered on a pulse by pulse basis and has two frequencies, at least 4 pulses are needed. For three such frequencies, at least 5 pulses are needed. Other pulse properties may be taken into consideration as well.

Under-Specification: If the criteria are easier to meet than real life conditions, the risk is that vendors will put equipment on the market that will cause interference when market penetration increases. If that is the case, regulators may be forced to deny further use of the 5GHz band by RLANs.

Over-Specification: If the criteria are tough to meet, vendors will shy away from using the 5GHz frequencies because of the costs of compliance testing and the risk of failing to meet these criteria. Although this will "protect" the radar systems in this band, it wastes the precious resource of 455 MHz of largely unpolluted spectrum that is ideal for use by wide channel MIMO equipment.

Because of the above considerations, it is necessary that the DFS compliance criteria reflect real life conditions and avoid the pitfalls of both under-specification and over-specification.

Problems with the current DFS Compliance Criteria

The ITU-R work on DFS focussed on the setting of the DFS threshold such that all relevant radars (which excluded low power radars) would be detectable. Detection probability was not considered and Recommendation M.1652 does not specify it in any way but extensive simulations were performed by NTIA experts to determine the threshold setting, given a certain rate of detection.

This Recommendation was the basis for DFS compliance criteria that could be applied to real devices. In the further work of the FCC 3] and ETSI 4], the need for a false alarm threshold was recognized but the mathematics of pulse detection by operating RLANs were largely ignored. Instead, detection probabilities for certain "radar types" were arrived at by negotiation[2]. Because of the industry's concerns about complexity and cost, the outcome of this work was an **under-specification**, notably in the case of the ETSI DFS specification which did not address the requirements of weather radars [3] although these were addressed in some detail in the ITU-R work on DFS.

Note: a detailed analysis of the differences between the FCC and the ETSI DFS compliance criteria is given in the Appendix.

The result of this **under-specification** was that, following the inevitable interference cases caused by non-compliant products and non-RLAN gear such as military radars early in the deployment of 5GHz RLANs, EUMETNET – the EU's meteorological radar network – pushed for and obtained much tighter detection protection criteria for weather radars. These tighter requirements – which include a 99.99% detection probability for the Channel Availability Check - is a clear case of **over-specification** which serves the purpose of EUMETNET to keep "their" band clean. It *appears* difficult to achieve and it is time consuming to validate in testing. ETSI attempted to compensate this with a relaxed test method – which is another case of **under-specification.**

The result is that the latest version (1.5.1) of the ETSI DFS test specification defines compliance criteria that appear stringent but the tests are relatively easy to meet. The consequences include that, if some equipment –regardless of its certification– causes interference, incumbent spectrum users will point consider such interference as evidence of that DFS does not protect their systems and demand that RLANs are denied access to some or all of the 5GHz band above 5250MHz. The EUMETNET demand to close part of the band to airborne RLANs is a case in point.

[2] Both the FCC and the initial ETSI work ignored the impact of staggered pulse patterns on the burst detection probability.

[3] Weather radars typically use staggered pulse patterns and have extended, typically helical scan cycles that last up to 10 minutes. Since detection of the radar is not possible while it is looking away from an RLAN, it was assumed that interference would occur whenever the radar would point at such an RLAN. No attempt was made to quantify this interference in terms of probability or signal power.

How to improve the DFS Compliance Criteria

Many regulators, incumbents and industry members confuse the DFS test compliance test criteria[4] with actual DFS behaviour – and it is the *latter* that counts in spectrum sharing and co-existence. The former serves as means to verify that the equipment is capable of DFS behaviour. To limit testing cost, the compliance criteria focus on small set of test cases but leave much of the actual behaviour untested.

In order to eliminate the risk of future compatibility issues, the DFS compliance criteria must be given a sound technical basis that recognizes the effects of the radar waveform statistics as well as the effects of radar antenna pattern and radar signal propagation on the DFS detection probability.

Secondly, there is no technical reason to have different criteria by country or region: instead a single set of criteria that covers the radars to be protected world-wide would save the WFA membership significant costs in development, the compliance testing, whether done in-house or in a certified test lab, and in product distribution.

Understanding radar detection statistics

The cornerstone of DFS is the practical detection efficiency. This is determined first of all by the statistics of the pulse patterns and secondly by operational conditions such as the RLAN busy level. Implementation plays a limited role The **detection statistics** of pulse patterns follow a cumulative binomial distribution function 5]: it determines how the detection probability *p* for individual pulses affects the overall burst detection probability *P* for *n* such pulses, given a minimum (false alarm threshold) of *k* pulses.

$$P_{(k \text{ out of } n)} = \frac{n!}{k!(n-k)!}(p^k)(q^{n-k})$$

where
k = the false alarm threshold,
n = the number of pulses in a burst,
p = the detection probability for a single pulse,
q = the probability that a pulse will not be detected.

In this case, q = 1-p because the detection and non-detection are complementary.
This formula ignores aspect of how to relate each detected pulse to the other pulses – that is an implementation matter. The figure below shows how detection probability varies with the number of pulses per burst and with the detection probability for individual pulses.

[4] See Appendix.

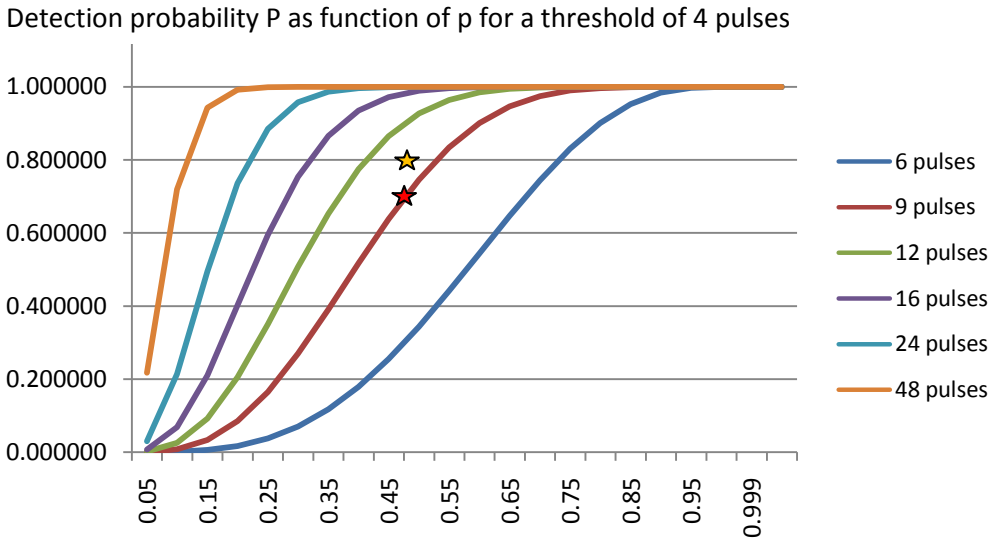


Figure 1: Typical detection probability variation with pulse count, given a 4 pulse false alarm threshold

The stars in the figure correspond to the current FCC compliance criteria (which are more stringent than ETSI's): the yellow star is for fixed frequency radars[5], the red star is for frequency hopping radars. As the recent work on DFS for RLANs on-board aircraft has shown, the actual detection conditions are vastly different from these test criteria and therefore radars are much better protected than suggested by the DFS compliance criteria. Much of the recent upheaval about the risk of (airborne) RLAN interference in the weather radar band was unnecessary and could have been avoided.

The effectiveness of DFS rests on its ability to quickly detect various radar types under different conditions. DFS detectors should be designed to cover most if not all of the "space" covered by the graphs (not just the few points shown above) but the current compliance criteria do not address that coverage. This has become apparent in some reported interference cases which, upon analysis showed that the detector had been designed to detect particular pulse patterns.

Understanding the impact of the DFS threshold on the observed burst length

In the work of the ITU-R as well as in the work of the FCC and ETSI, the impact of the DFS threshold on radar detectability were ignored; instead the DFS requirements were based on the (hidden) assumption that RLANs would see only the pulses that correspond to the radar's nominal beam width. This lack of understanding has caused the industry to be overly conservative with detection criteria and this conservatism has led to the **under-specification** identified earlier. However, both theory and practice show that the hidden assumption is wrong: for most radars, the DFS threshold is set far lower than is needed to assure detection in case interference could be caused. The implication is that DFS detectors see a far wider radar beam than the nominal beam width suggests. Even for a highly sensitive radar and a protection level of I/N = -10dB, the link budget difference is large.

The general formula is:

$$P_{rad}+(G_{rad}+G_{rlan})-PL-T_{DFS} \geq P_{rlan}+(G_{rlan}+G_{rad})-R_{BW}-PL-T_{rad}$$

Filling in the values for a weather radar and a 100mW RLAN gives:

[5] The 80% requirement applies over 4 different pulse patterns of different lengths, the minimum detection probability for each is 60%. For all, p ~ 50%

84 +(44) – PL+62 ≥ 20 + (44)– PL -12.2+121

146 ≥ 128.8 ~ 17.2dB

See the figure below. The actual values depend on the radar power and antenna gain, the bandwidth ratio R_{bw} and the interference threshold of the radar (T_{rad}).

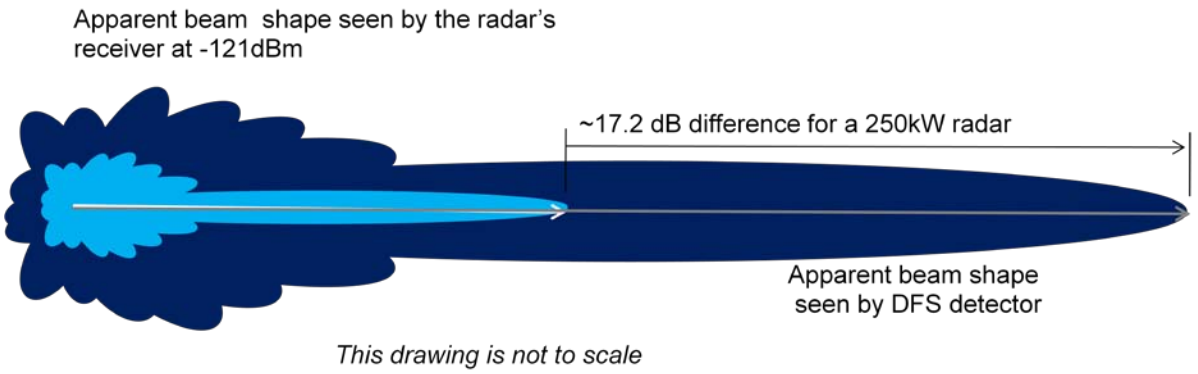


Figure 2: Apparent radar beam dimensions as seen by a DFS detector and the radar's receiver

As indicated by this picture, both the length and width of the radar beam as seen by the DFS receiver far exceed the effective beam shape as seen by the radar's receiver. In other words, DFS will detect the radar at azimuths and distances at which no interference is possible [6].

The most important effects of the above are that the RLAN sees many more pulses than indicated by nominal beam width and that this difference grows with a decrease in distance between the radar and the RLAN. Thus, as the impact of interference increases with decreasing distance, the probability of interference occurring at all decreases even faster, mostly due to the side lobes of the radar antenna.

These effects are very large: a case in point is given by these data from a modern Dutch weather radar: the nominal beam width is .9° but at a distance of 13km (~8 mi) the beam width observed by a DFS detector is almost 2.2° at a peak signal strength of -46dBm. At 3 RPM and a staggered PRF7 of 450/600Hz, the DFS detector sees ~ 60 pulses and detection probability for this radar is de facto 100%. The 13km distance is near the edge of the radar's susceptibility zone where the potential interference is so low as to be difficult to notice in the weather radar's data products. At shorter ranges, the pulse count will be even higher. As shown in the Appendix, at 16 pulses, the DFS detection efficiency in ISM mode is more than 98% and at 24 pulses it exceeds 99.9%. This means that first hit detection is assured under all conditions and that in most cases – as the radar beam sweeps over the RLAN – detection will occur before the RLAN becomes visible to the radar – regardless of the distance8. This "mode" of detection could be called lateral detection.

[6] It might be countered that some excess range is necessary to assure that large numbers of RLANS just outside the detection range will not cause interference. In free space propagation conditions this is true but large numbers of RLANs are only found on the ground and in buildings and here earth's curvature and near ground propagation losses – which easily leads to path loss exponents of 5 and more – assure that such large numbers will always be well outside the radar's susceptibility footprint.

[7] This particular radar uses packet staggering with two pulse repetition intervals: each packet is at least 16 pulses long. Range ambiguity is resolved at the packet level – the 16 pulses per packet improve the SNR by some 12dB over a single pulse.

[8] Some weather radars use a "silent scan" at a high elevation to establish a background noise level for signal processing. Due to the high elevation, terrestrial RLANs will not affect the results of such silent scans.

Since most modern weather radars have similar properties9, DFS is in practice adequate to protect weather radars, even in real time, on its operating channel. In fact, the onerous Channel Availability Check is unnecessary for all but a few types older of weather radar that combine high rotation speed and low pulse rate. This argument easily extends to military radars.

Finally, the high detection probabilities (lateral as well as full beam) associated with nearly all radars makes the complexity of implementing and testing the ETSI "Off channel CAC" unnecessary.

Improved DFS Compliance Criteria

The current DFS compliance criteria address both radar detection (probabilities) and RLAN response behaviour. The latter can be reduced or changed in view of the high detection probabilities noted above.

Further, as the RLAN industry matures and the applications of RLAN expand, different regimes of compliance and compliance assessment become necessary, e.g. for RLAN used in transportation systems.

The main requirement for new compliance criteria is to increase the coverage the criteria over a wider range of detection parameters that correspond better to real world conditions. In addition, some modifications can be applied to the DFS behaviour to reduce complexity and remove unnecessary operational constraints.

The figure below shows how detection probability varies with the number of pulses per burst and with the detection probability for individual pulses. The stars mark the FCC's current criteria. The red star marks the position of the frequency hopper test criteria, the green star marks the maximum requirement for the types 1-4 radars and the orange star marks the long pulse radar requirement. The white star marks the Channel Availability Check condition: near detection of each individual pulse because there is no RLAN traffic to interfere with detection. In fact, the graphs show that even 5% of loss of individual pulses does not affect the overall detection probability. In other words, Channel Availability Check detection is quite robust, regardless of the pulse count. However, the compliance criteria for this mode of detection are the same as for ISM mode detection.

The picture clarifies the degree of under-specification of the compliance test criteria: most of the detection space is not covered and therefore the behaviour of a given implementation outside of the criteria is not assessed.

[9] In all information systems, the information bandwidth varies with signal to noise ratio. In case of radar systems the information bandwidth equates to the ability to detect small targets and small movements of such targets. The signal to noise ratio of radar signals improves with the number of pulses returned by the target. Therefore, modern radars use high pulse rates and are thus easier to detect than old, low pulse rate radars.

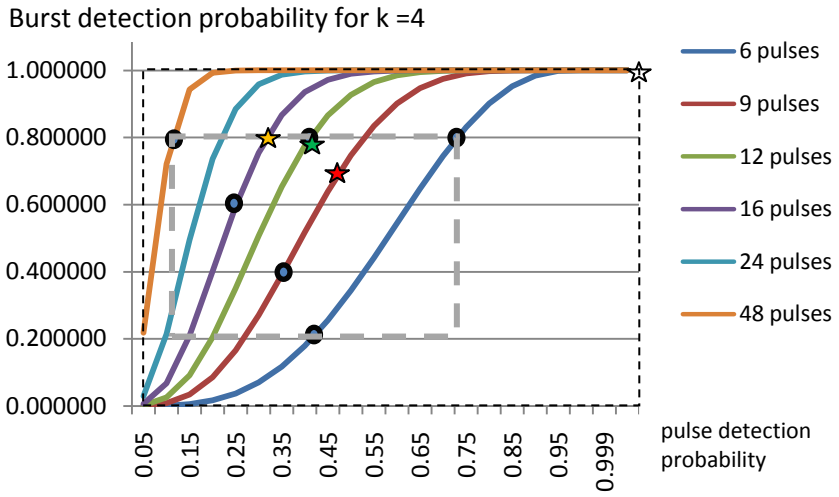


Figure 3: Burst detection probability variation with RLAN busy level and for different burst lengths

The gray dashed rectangle indicates the parameter values that *together* determine the ability of a DFS detector. Therefore, the DFS compliance test criteria should be spread over a major part of that parameter space. In practice, the test "burden" need not be affected significantly: the test points need not be many and there is little need to test with many different pulse rates. The black dots suggest 6 test points that together test a detector over its performance with different burst lengths and with different RLAN channel busy ratios. A detector that shows this behaviour will also perform according to these curves at the very high detection probabilities that are too time consuming and therefore too costly to test exhaustively. Therefore, limiting the compliance criteria to the gray square is adequate.

Tests to validate compliance can easily be automated, notably with assistance of testability features in the products to be tested, e.g. disabling the channel switch for and reporting the time, pulse count and pulse spacing of the detected bursts.

This white paper proposes the development of new criteria, notably for detection probability. Ideally these criteria should be acceptable world-wide so as to avoid the costs of multiple (certification) tests. Working out the details of the criteria as well as the test procedures should be done in cooperation between both all concerned: incumbents, industry and regulators.

Appendix B provides more considerations and detail for deriving improved and harmonised detection criteria for DFS. These harmonised criteria could be applied by any Administration – completely or partially as necessary to protect the radars systems operating in the 5GHz.

Finally, some of the DFS operational requirements may need fine tuning to improve their effectiveness and to reduce the burden of implementation and testing. This too is subject for further work by industry experts.

References:

1] ITU-R Resolution 229, 2003: www.itu.int/ITU-R/study-roups/was/.../resolution229e.doc

2] ITU-R Recommendation M.1652: Dynamic frequency selection (DFS) in wireless access systems including radio local area networks for the purpose of protecting the radio-determination service in the 5 GHz band

3] FCC Memorandum & Order 06-96A1: Revision of Parts 2 and 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) devices in the 5 GHz band

4] ETSI EN 301-893-v1.5.1: Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive

5] Binomial function: http://faculty.vassar.edu/lowry/binomialX.html

Author's biographical data:

Jan Kruys recently joined Oaktree Wireless after retiring from Cisco. His technical expertise includes RF signal propagation analysis, spectrum sharing methods and techniques, protocols for RLANs and wireless mesh systems. Jan has more than 20 years of experience in spectrum regulations, technology analysis, systems engineering and standardization at NCR, Lucent Technologies, Agere Systems and Cisco. His recent work included chairing and assisting regulatory teams in the Wi-Fi Alliance, the WiMAX Forum and ETSI. His earlier participation in ETSI and a number CEPT project teams as well as in the ITU-R preparations for WRC 2003 resulted in the allocation of 455 MHz of license exempt spectrum for RLANs.

Appendix A: Details of the FCC and ETSI DFS Compliance Criteria

Common to both sets of DFS requirements are the DFS detection thresholds for indoor (max -62dBm for 200mW) and outdoor (-64dBm for 1000mW) RLANs.

Differences are:

1) The pulse statistics (see below)
2) When to perform a Channel Availability Check (FCC: always before start of usage of a channel, ETSI only at power up of the RLAN device or network)
3) The duration of the Channel Availability Check (FCC: 60 seconds only, ETSI = 10minutes for the 5600-5650 MHz band)
4) The duration of the Channel Closing Transmission time (FCC = 260msec, ETSI = 1 second)
5) The option to do a "off-channel Channel Availability Check" (ETSI only)

FCC DFS Test Waveforms

The following is a summary of the FCC's DFS criteria with regard to pulse statistics.

"Generic" radars are modelled with the following "short pulse waveforms" for radar types 1 through 4; for each a detection requirement is given. Over all waveforms, the detection probability should exceed 80%.

The absence of staggered waveforms is noteworthy. It may be based on the assumption that there is little difference in detectability between the staggered and non-staggered pulse patterns. This is true only for staggering by "packet".

Type	Pulse Width (µsec) Minimum	PRI (µsec)	Number of Pulses	Percentage of Successful Detection	Minimum Number of Trials
1	1	1428	18	60%	30
2	1 - 5	150 - 230	23 - 29	60%	30
3	6 -10	200 - 500	16 - 18	60%	30
4	11 – 20	200 - 500	12 - 16	60%	30
			Over all types	80%	

Table A1: Basic DFS test waveforms of the FCC's Part15 rules

The most stringent requirement of this set is the last one: it has the lowest number of pulses per burst (12).

Long pulse radars are modelled with this waveform (radar type 5) which has to be detected with a probability of 80% over a detection period of 12seconds:

Pulse Width (µsec)	Chirp Width (MHz)	PRI (µsec)	Number of Pulses	Number of *Bursts*	Percentage of Successful Detection	Minimum Number of Trials
50 - 100	5 - 20	1000-2000	1 - 3	8-20	80%	30

Table A2: DFS detection requirement for "long pulse" waveforms of the FCC's Part 15 rules

This detection requirement is effectively determined by the statistics of the pulse distribution over the average of 14 bursts which have 2 pulses per burst on average. This is roughly equivalent to 14 pulse pairs with constant intra-pair spacing. Since the pulse pattern is determined by the transmitter's algorithm, there are no RF propagation effects that improve the detectability of this radar waveform.

Frequency hopping radars (type 6) are modelled with this waveform:

Pulse Width (μsec)	PRI (μsec)	Pulses per hop	Hopping rate (kHz)	Hopping Sequence Length (msec)	Percentage of Successful Detection	Minimum Number of Trials
1	333	9	.333	300	70%	30

Table A3: DFS detection requirement for frequency hopping waveforms of the FCC's Part 15 rules

Here the determinant is the number of pulses per hop: 9

ETSI DFS Test signals

The ETSI EN 301-893-v1.5.1 specifies the following test signals and success criteria:

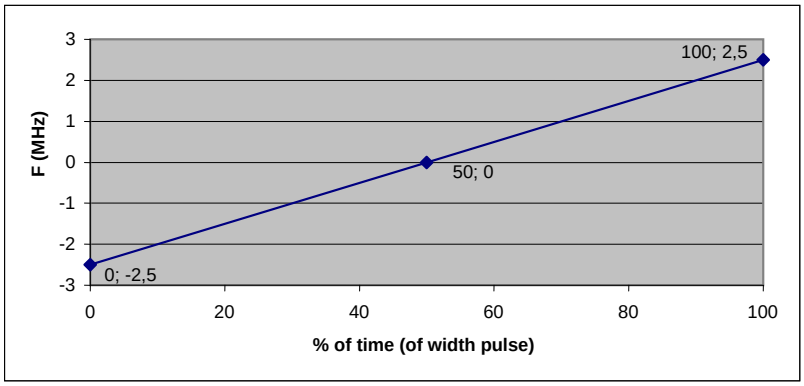
Parameter	Detection Probability (P_d)	
	Channels whose nominal bandwidth falls partly or completely within the 5600 – 5650 MHz band	**Other channels**
CAC, Off-Channel CAC	99.99 %	60%
In-Service Monitoring	60 %	60%
NOTE: Pd gives the probability of detection per simulated radar burst and represents a minimum level of detection performance under defined conditions. Therefore Pd does not represent the overall detection probability for any particular radar under real life conditions.		

Table A4: Required Detection probabilities per EN 301-893-v1.5.1

Radar test signal # (see notes 1 to 3)	Pulse width W [µs]		Pulse repetition frequency PRF (PPS)		Number of different PRFs	Pulses per burst for each PRF (PPB) (see note 5)
	Min	Max	Min	Max		
1	0.8	5	200	1000	1	10 (see note 6)
2	0.8	15	200	1600	1	15 (see note 6)
3	0.8	15	2 300	4000	1	25
4	20	30	2 000	4000	1	20
5	0.8	2	300	400	2/3	10 (see note 6)
6	0.8	2	400	1200	2/3	15 (see note 6)

NOTE 1: Radar test signals 1 to 4 are constant PRF based signals. See figure D.1. These radar test signals are intended to simulate also radars using a packet based Staggered PRF. See figure D.2.

NOTE 2: Radar test signal 4 is a modulated radar test signal. The modulation to be used is a chirp modulation with a ±2,5MHz frequency deviation which is described below.



NOTE 3: Radar test signals 5 and 6 are single pulse based Staggered PRF radar test signals using 2 or 3 different PRF values. For radar test signal 5, the difference between the PRF values chosen shall be between 20 and 50 pps. For radar test signal 6, the difference between the PRF values chosen shall be between 80 and 400 pps. See figure D.3

NOTE 4: Apart for the *Off-Channel CAC* testing, the radar test signals above shall only contain a single burst of pulses. See figure D.1, D.2 and D.3.
For the *Off-Channel CAC* testing, repetitive bursts shall be used for the total duration of the test. See figure D.4. See also clause 4.7.2.2.

NOTE 5: The total number of pulses in a burst is equal to the number of pulses for a single PRF multiplied by the number of different PRFs used.

NOTE 6: For the CAC and Off-Channel CAC requirements, the minimum number of pulses (for each PRF) for any of the radar test signals to be detected in the band 5600 to 5650 MHz shall be 18.

Table A5: DFS test signals per EN 301-893-v1.5.1

Analysis

From the viewpoint of detection statistics, the most stringent requirement of all of the above is the FCC's requirement for the detection of frequency hopping signals: over 30 trials, bursts of only 9 pulses have to be detected with a probability of 70% or better. Since the burst length is determined by the transmitter's frequency hopping algorithm[10], there are no RF propagation effects that improve the detectability of this radar waveform. For ISM detection at 50% load, the 70% requirement is near the theoretical limit.

[10] The converse is that military radars can control their detectability RLANs through changing their hopping pattern or hopping rate.

For the Channel Availability Check, this is requirement is easily met: assuming absence of interferers on the RLAN channel that could affect detection, 4 pulses are enough to assure detection and to meet the minimum false alarm threshold.

Of the ETSI specification, Test signal type 1 is the tightest but it is easily met: 10 pulses at 60% detection probability. Also, the ETSI specification does not demand to 80% overall detection probability of the FCC's requirements: this is a degree of **under-specification** that is actually harmful because it suggests that DFS is not very good at radar detection – "it gets only 60%" .

The following table gives the theoretical [11] burst detection probability for 6, 9, 10, 12, 16 and 24 pulses for a false alarm threshold of 4 pulses.

		Pulses per burst					
RLAN busy factor	False alarm threshold	6	**9**	10	12	16	24
50%	4	0.343750	0.746093	0.818125	0.927002	0.989365	0.999229

Since all of the other waveforms provide far more pulses per burst, their detection probability will easily exceed the requirement of the 80% average over radar types 1 through 4 required by the FCC. Case in point: the 4th FCC radar type gives 12-16 pulses per burst: these give 0.927002 to 0.989365 detection probability in ISM mode and 100% in CAC mode.

Both specifications ignore the vast difference in detection probability between the RLAN being silent (i.e. during the Channel Availability Check) and the RLAN being active (i.e. during In Service Monitoring), notably when the radar "bursts" are short. This is clearly shown in Figure B1: for a burst of only 6 pulses, detection probability varies from 100%, when the RLAN is silent, to 20% when the RLAN is busy for 60% of the time.

Similarly, the physics of radar signal propagation and detection were ignored; instead the DFS requirements were based on the (hidden) assumption that RLANs would see only the pulses that correspond to the radar's nominal beam width. See "Understanding the impact of the DFS threshold on the observed burst length" in the body of this paper.

[11] Detection efficiency varies with the amount of activity of other RLANs and the presence of electro-magnetic noise that is strong enough to cause RLAN receiver de-sensitisation and frequent enough to cause masking of radar pulses. Only the former is a real factor in practice but even this is marginal since the interfering signal comes from another uncoordinated RLAN. The CSMA/CA PHY protocol assures that such signals, if they occur at all, far below the DFS threshold.

Appendix B: Details of improved DFS Compliance Criteria

Improving DFS compliance criteria should take the following into account:

1) Radar pulse patterns vary significantly and include constant, packet staggered and pulse staggered pulse repetition intervals. In practice, the latter requires different detection procedures and a higher false alarm threshold. In practice two or three pulse repetition intervals are used.
2) Detection probability varies non-linearly with the RLAN's busy level. This property requires a departure from the current criteria which consider only two such levels: 0% and 50%.
3) In fixed applications, RLANs should perform a Channel Availability check only upon start-up so to assure the channel is not already in use by a radar system. This requirement reduces the (remote) possibility that many RLANs start on the same channel – e.g. after a power failure.
4) For RLANs used in transportation systems[12], including airborne applications, a Channel Availability Check serves no purpose and should not be required.
5) Similarly the non-use period of 30 minutes after detection serves no purpose and should not be required in transportation applications of RLANs.
6) Upon detection, the RLAN should remain silent for at least 100msec to allow the radar's beam to pass before the RLAN starts its Channel Move Time transmissions.
7) The DFS detector will generally see a large number of pulses and multiple instances of different pulse repetition intervals.
8) Radars using (coded) pulse compression use longer pulse durations compared to non compressed pulse types. However, pulse duration does not affect the detection statistics to the extent that the peak power levels concerned are comparable to those of non-compressed pulse types.
9) During testing of DFS behaviour, environmental factors such as EMI from third sources are not present but in practice they are; these have the same effect as a (slight) increase in RLAN busy level.
10) Last but not least: care should be taken with detailing and implementing changes in the DFS compliance criteria so as to assure a stable result.

The test procedures for the above should take the following into account:

1) Since the detection process is statistical in nature, the test methods used to assess compliance should assure that the test outcome itself has a high probability of being correct.
2) Test complexity and test time are major contributors to testing cost and both should be kept low.
3) Test automation, possibly assisted by test support functions in the unit under test, would be highly beneficial, both for assuring reliable test outcomes and for reducing test time and test cost.

[12] It should be noted that RLANs in transportation systems (aircraft, trains, buses, cars) are not consumer products but installed by experts under controlled circumstances. The "no CAC" requirement should not apply to over-the-counter equipment.

Improved DFS Detection Criteria

Considering the large variation in detection conditions and the resulting detection probabilities a different approach to test definition is needed. The current criteria focus on signals to be detected but do little to validate overall detector performance. Taking into account the statistics of the detection process suggests that there is no need to validate detection performance at very high levels of probability. Instead, detector behaviour at high probabilities can be derived from its behaviour at lower probabilities. In the figures below, the gray blocks represent an area of behaviour that can be verified quickly and at low cost – the first for constant pulse rates and packet staggered pulse rates, the second for (triple) staggered pulse rates. The red dots correspond to test cases that together validate that the detector behaviour is adequate over a wide range of conditions. The dot with the blue square represents the current test case for frequency hopping radars in the FCC's Part 15 rules.

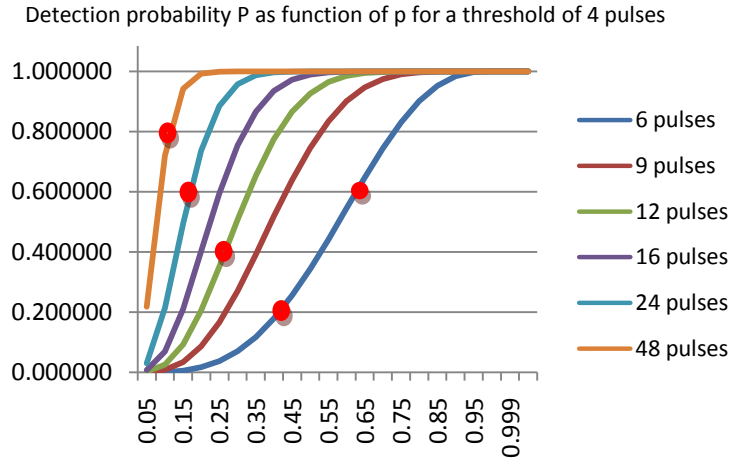


Figure B1: Compliance Test cases for constant rate and packet staggered radar signals

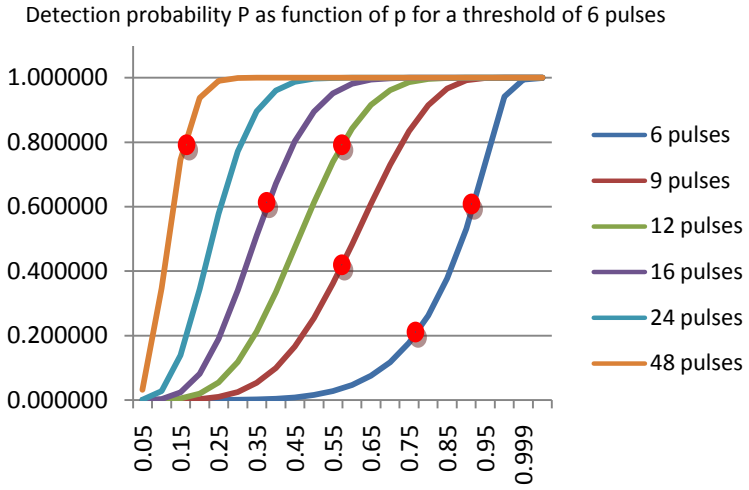


Figure B2: Compliance Test cases for constant rate and packet staggered radar signals

Note that the above criteria do not include a pulse rate; this has to be added but only to verify the range of pulse rates that the detector under test will support.

Converted to a list the above test requirements look as follows:

Test	Pulse rates,	Staggering	Burst	Channel	# of	# of	Success

case	Hz		length	busy	bursts	trials	rate
1	250	None or packet	6	60%	10	5<x<10	20%
2	4000	None or packet	6	60%	10	5<x<10	20%
3	500	None or packet	6	30%	30	10<x<20	80%
3	500	None or packet	9	50%	20	10<x<20	70%
4	500	None or packet	12	70%	30	5<x<10	40%
5	500	None or packet	24	80%	20	10<x<20	60%
6	500	None or packet	48	90%	30	10<x<20	80%
7	250/300	Dual pulse	6	20%	10	5<x<10	20%
8	250/300	Dual pulse	6	10%	20	10<x<20	60%
8a	2500/3000	Dual pulse	9	40%	10	5<x<10	40%
9	300/350/400	Triple pulse	9	40%	10	10<x<20	40%
10	300/350/400	Triple pulse	12	40%	30	10<x<20	80%
11	400/500	Dual pulse	16	60%	20	10<x<20	60%
12	400/500	Dual pulse	48	80%	30	10<x<20	80%

Table B1: Set of detection criteria that cover most of the detector operating conditions

The required pulse width can vary from case to case between the limits of .5 and 30usec but a constraint might added that at least 3 of the second set of tests must be run with .5usec pulse width.

Finally it must be noted that the above success rates are close to the theoretical values. In practice, radar signals will be much easier to detect to the larger burst lengths. Therefore, the above results minus some “implementation margin” would provide designers with some implementation margin without detracting from practical performance. The value of this implementation margin requires further work.

To this list must be added the “bin 5” criteria of the FCC for long pulse compression radars (which already contains the implementation margin):

Test case	Pulse Width (µsec)	Chirp Width (MHz)	Pulse rate Hz	Pulses per burst	Number of *Bursts*	Minimum # of Trials	Percentage of Successful Detection
13	50 - 100	5 - 20	500/1000	1 - 3	8-20	30	80%

Taken together, the tests validate the detector performance over a wide range of conditions. The tests can easily be automated. Such automation is facilitated if the equipment under test is able to a) disable its “channel move function” and b) report the observed radar signals and their detection.