

# **Lessons Learned from the Development and Deployment of 5 GHz Unlicensed National Information Infrastructure (U-NII) Dynamic Frequency Selection (DFS) Devices**

**Frank H. Sanders  
Edward F. Drocella  
Robert L. Sole  
John E. Carroll**



***report series***

# **Lessons Learned from the Development and Deployment of 5 GHz Unlicensed National Information Infrastructure (U-NII) Dynamic Frequency Selection (DFS) Devices**

**Frank H. Sanders  
Edward F. Drocella  
Robert L. Sole  
John E. Carroll**



**U.S. DEPARTMENT OF COMMERCE**

December 2019



## **DISCLAIMER**

Certain commercial equipment and materials are identified in this report to specify adequately the technical aspects of the reported results. In no case does such identification imply recommendation or endorsement by the National Telecommunications and Information Administration, nor does it imply that the material or equipment identified is the best available for this purpose.

## PREFACE

The National Telecommunications and Information Administration (NTIA) Institute for Telecommunication Sciences (ITS) and Office of Spectrum Management (OSM) have performed a case study that describes the development of 5 GHz Dynamic Frequency Selection (DFS) from multiple perspectives. One perspective is a historically linear, timeline-based description of the technology's development and deployment. A second perspective is provided as a timeline description that focuses on the technical issues and hurdles that were encountered and solved in the course of development and deployment. Subsequent report sections describe the technology as it was finally developed. Issues, problems, and challenges that were encountered after commercial deployment began are described in succeeding sections.

This report offers a perspective of the experiences associated with the development and deployment of 5 GHz DFS unlicensed national information infrastructure (U-NII) devices. In particular, it puts focus on harmful interference interactions with respect to Terminal Doppler Weather Radars (TDWRs) that have been attributed to some DFS-enabled 5 GHz U-NII devices, some of which were determined to have been non-compliant with the applicable FCC regulations. It also describes unexpected harmful interference that has been experienced on an ongoing basis to tracking radars used at U.S. government rocket test and space launch ranges on the east and west coasts.

The report summarizes the most likely explanations for these interference incidents, along with actions already implemented in an attempt to mitigate both the existing and future interference potential, based upon the technical information derived from investigations into the underlying causes of these interference interactions. Lessons Learned are introduced as this report's narrative progresses. Ultimately, eleven such Lessons Learned are presented. This narrative, with the associated Lessons Learned, provides guidance that may be applied to, and perhaps may be used to modify, similar spectrum-sharing approaches in other spectrum bands, with other radio systems, in the future.

## NOTE ON REFERENCES

In this report, references for major documents and reports (e.g., the *Manual of Regulations and Procedures for Federal Radio Frequency Management*) are provided as bracketed links (e.g., [1]) in the main text. Because of the sheer number of total references, and because the bulk of those references are minor documents, references to minor documents are placed as footnotes on report pages.

This report contains numerous references to sections of Title 47 of the Code of Federal Regulations. As of the date of publication, all 47 CFR sections are available on-line at <https://www.fcc.gov/wireless/bureau-divisions/technologies-systems-and-innovation-division/rules-regulations-title-47>.

There are also numerous references to Federal Communication Commission Dockets, including those that pertain to Notices of Proposed Rulemaking and Report and Orders. These are available via a search function at <https://www.fcc.gov/edocs>.

# CONTENTS

Preface .....	iv
Figures .....	ix
Tables .....	x
Abbreviations/Acronyms.....	xi
Executive Summary .....	xiii
1. Introduction.....	1
1.1 Report Organization.....	3
1.2 Gradual Introduction of Lessons Learned as the Report Progresses .....	4
2. Narrative Review of DFS Spectrum Sharing Technology Development.....	5
2.1 Historical Development of Spectrum Sharing Arrangements and Management Approaches.....	5
2.2 Historical U.S. Radar Band Usage and a New Idea for Overlay Sharing.....	6
2.3 Historical Narrative of WAS at 5 GHz: A Decade of Development .....	7
2.3.1 Initial FCC Rulemaking Efforts.....	7
2.3.2 International Developments and FCC Rulemakings Between 2000 and 2003.....	10
2.3.3 Development of Adequate Testing Procedures and FCC Decisions Between 2003 and 2006.....	14
3. Technical Review of DFS Spectrum Sharing Technology Development.....	18
3.1 DFS: Highlights of a Novel Spectrum Sharing Concept .....	18
3.2 Uniqueness of the DFS Concept in Real-World Spectrum Sharing .....	19
3.3 Technical DFS Developments Starting in 1996 .....	19
3.3.1 DFS Introductory Efforts, 1996 .....	20
3.3.2 Technical Parameters in the Initial FCC R&O and MO&O, 1997–1998.....	20
3.3.3 Technical Parameters from WRC-03 and Recommendation M.1652.....	21
3.3.4 Determination of Technical Protection Criteria, Late 1990s through Mid-2000s.....	21
3.4 First Technical Implementation Steps in the U.S., 2003–2004.....	22
3.5 Certification Testbed Technical Development, 2005–2006.....	22
3.6 Technical Certification Requirements Development, 2005–2006.....	23
3.7 DFS Compliance Testbed Constructed at ITS, 2005–2006 .....	24
3.8 Early DFS Testing at the ITS Boulder Laboratory and Testing Transition to the FCC, 2005–2006.....	25
3.9 Initial DFS Deployment Experience and TDWR Interference, 2006–2009 .....	27
3.10 Brief Summary of Ongoing DFS Deployment, 2010 to 2015.....	27
3.11 CSMAC Impetus for this Report, 2015.....	29
4. DFS Principles and Implementation .....	30
4.1 The Basic DFS Concept .....	30
4.1.1 DFS Architecture Within U-NII Systems.....	30

4.1.2 DFS Parameter Space: Note on Frequency-Shift (Channel-Move) Protocols.....	32
4.2 Theoretical Difficulties with DFS.....	32
4.2.1 Assumption: Radars Can Be Detected While U-NII Message Traffic is Running .....	33
4.2.2 Assumption: Detection of Radar Signals by APs Protects Radars from All Network Transmissions .....	34
4.2.3 Assumption: Radar-Detection Thresholds are Adequate to Protect Radars from Harmful Interference.....	34
4.2.4 Assumption: Radar Waveform Testing is Sufficiently Robust.....	35
4.2.5 Assumption: Firmware Updates Installed in DFS Units After Initial Certification Will Not Cause DFS to be Impaired or Disabled .....	36
4.2.6 Assumption: DFS-Equipped U-NIIs will be Properly Installed and Operated.....	37
4.2.7 Assumption: Introduction of DFS to a Previously Unshared Band Will Not Encourage Illegal Introduction of Non-DFS-Equipped Devices Into the Band .....	38
4.3 Ongoing Need for Enforcement Actions in DFS Bands .....	39
4.4 Lessons Learned from DFS Principles and Implementation.....	41
5. DFS Challenges for Manufacturers and Vendors .....	44
5.1 Challenges to U-NII Device Manufacturers Understanding of Radar Systems .....	44
5.2 Difficulty of Detecting General, As Opposed to Specific, Radar Waveforms.....	45
5.3 Lack of Industry Testbeds for DFS.....	46
5.4 Development of the NTIA DFS Testbed and Its Use by Industry and FCC .....	46
5.5 Laboratory and Field Tests of DFS with Industry Participation .....	47
6. Challenges for Government Development of DFS Testing and Certification Protocols .....	49
6.1 The Difficulty of Designing DFS Protocols for Non-Existent Radio Systems .....	49
6.2 Advantages of Working on a Blank Slate .....	49
6.3 Disadvantages of Having Areas of Developmental Doubt and Uncertainty.....	50
7. Early DFS Deployments: First Successes and Failures in the Field .....	52
7.1 San Juan, Puerto Rico and New York City Harmful Interference Events Review.....	52
7.2 Identification of Interfering DFS-Equipped Devices at San Juan .....	52
7.3 NTIA-FAA-FCC Cooperative Efforts at Field Locations.....	53
8. Harmful Interference at U.S. Rocket Test and Space Launch Ranges.....	55
8.1 Overview of 5 GHz Range Instrumentation Radars .....	55
8.2 RIR Missions .....	57
8.3 Range Safety and 5 GHz RIR Tracking.....	57
8.4 RIR Spectrum Shared with U-NII Transmitters.....	60
8.5 Example U-NII-to-RIR Interference Case Histories at Cape Canaveral .....	61
8.5.1 Interference in the DFS-Required U-NII-2C Band.....	61
8.5.2 Interference in the Non-DFS U-NII-3 Band.....	63
8.5.3 Interference Case Summary for Cape Canaveral.....	63
8.5.4 Interference Analysis.....	64
9. Ongoing DFS Spectrum Sharing Support .....	66
9.1 Continuing Monitoring of Legal FCC-Certified DFS Devices .....	66



9.2 Illegal (Non-DFS-Equipped) Device Imports .....	66
9.3 Accommodating More Complex Future Radar Waveforms .....	66
9.4 Accommodating Changing U-NII Device Technology .....	67
10. Summary of Lessons Learned for Future Dynamic Spectrum Sharing Technologies.....	68
11. References.....	70
Acknowledgements.....	71
Appendix A How DFS Detection Thresholds Are Computed and Why DFS Detection Does Not Require Radar Mainbeam Coupling to Work .....	72
Appendix B Technical Characteristics of Range Instrumentation Radars.....	76
Appendix C Range Instrumentation Radar Tracking Techniques .....	78
C.1 Monopulse Technique for RIR Tracking.....	78
C.2 Monopulse Skin Tracking with RIRs at Launch Facilities.....	80
C.3 Monopulse Beacon Tracking .....	81
C.4 Metric-Tracking GPS Beacons.....	82
Appendix D Interference from U-NII Transmitters to 5 GHz Range Radars .....	83
D.1 Effect of RF Interference on Monopulse Radar Tracking.....	83
D.2 Other Possible Effects of RF Interference on RIR Receivers .....	84
D.3 Interference Coupling from U-NII Transmitters to RIR Receivers .....	84
Appendix E Current DFS PRF Certification Testing Limits.....	87

**FIGURES**

Figure 1. DFS performance-testing system developed by NTIA and transferred to FCC. ....25

Figure 2. Early DFS radar-pulse detection result with a prototype DFS U-NII provided by industry, circa 2005. Time is in seconds.....26

Figure 3. Typical 5 GHz DFS-equipped U-NII network as usually deployed by WISPs.....30

Figure 4. DFS algorithm flowchart.....31

Figure 5. A RIR antenna (8.8 m diameter). Note three strut support points for an earlier-generation RF feed. Circular aperture at right is for a co-axial telescopic camera. ....56

Figure 6. Example of multiple-RIR deployment at a single range. ....56

Figure 7. Schematic diagram of a booster being skin tracked while flying both possible beacons.....59

Figure 8. The 5 GHz spectrum that is shared between RIRs and U-NIIs, with Eastern Range frequencies used as an example case. U-NII Band 3 shares spectrum with radars, including some RIR frequencies, but has never had any DFS requirement. ....60

Figure 9. Sketch of a RIR receiver diagnostic display where operators can see interference during radar operations (drawn from the lead author’s *in situ* notes at a Cape Canaveral radar station). ....62

## **TABLES**

Table 1. DFS Technical Protocol Summary .....	24
Table 2. Summary of FCC DFS-Related Enforcement Actions from 2007 to 2019 .....	40
Table 3. Overview of Criteria for Launch Vehicle Tracking Selections .....	58

## ABBREVIATIONS/ACRONYMS

<b>AP</b>	access point
<b>CFR</b>	Code of Federal Regulations
<b>CPM</b>	Conference Preparatory Meeting
<b>CSMAC</b>	Commerce Spectrum Management Advisory Committee
<b>dB</b>	decibel
<b>dB<sub>i</sub></b>	decibels relative to isotropic
<b>dB<sub>m</sub></b>	decibels relative to a milliwatt
<b>DoD</b>	Department of Defense
<b>DFS</b>	dynamic frequency selection
<b>EI</b>	electronic intelligence
<b>EW</b>	electronic warfare
<b>EIRP</b>	effective isotropic radiated power
<b>EMC</b>	electromagnetic compatibility
<b>FAA</b>	Federal Aviation Administration
<b>FCC</b>	Federal Communications Commission
<b>FDR</b>	frequency dependent rejection
<b>FNPRM</b>	Further Notice of Proposed Rulemaking
<b>Gbit/s</b>	gigabits per second
<b>GPS</b>	Global Positioning System
<b>HIPERLAN</b>	high performance radio local area network
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IF</b>	intermediate frequency
<b>IRAC</b>	Interdepartment Radio Advisory Committee
<b>ITAC-R</b>	International Telecommunication Advisory Committee, Radiocommunication
<b>ITS</b>	Institute for Telecommunication Sciences (NTIA)
<b>ITU-R</b>	International Telecommunication Union, Radiocommunication Sector
<b>JRG</b>	Joint Rapporteur's Group
<b>KDB</b>	Knowledge Database
<b>LNA</b>	low noise amplifier
<b>LPA</b>	log periodic antenna
<b>LV</b>	launch vehicle
<b>Mbit/s</b>	megabits per second
<b>MIMO</b>	multiple input, multiple output
<b>MIPIR</b>	Missile Precision Instrumentation Radar
<b>MO&amp;O</b>	Memorandum Opinion and Order
<b>MPEG</b>	Moving Picture Experts Group
<b>NPRM</b>	Notice of Proposed Rulemaking

<b>NTIA</b>	National Telecommunications and Information Administration
<b>OET</b>	Office of Engineering Technology (FCC)
<b>OoB</b>	out of band
<b>OSM</b>	Office of Spectrum Management (NTIA)
<b>PRF</b>	pulse repetition frequency
<b>PRI</b>	pulse repetition interval
<b>PRR</b>	pulse repetition rate
<b>R&amp;O</b>	Report and Order
<b>RF</b>	radiofrequency
<b>RLAN</b>	radio local area network
<b>RIR</b>	Range Instrumentation Radar
<b>ROSA</b>	radar open system architecture
<b>RSO</b>	range safety officer
<b>SDR</b>	software defined radio
<b>SSID</b>	service set identifier
<b>SUPERNet</b>	shared unlicensed personal radio network
<b>TDWR</b>	Terminal Doppler Weather Radar
<b>U-NII</b>	unlicensed national information infrastructure
<b>US&amp;P</b>	United States and Possessions
<b>VSA</b>	vector signal analyzer
<b>WAS</b>	wireless access system
<b>VSG</b>	vector signal generator
<b>WInnForum</b>	Wireless Innovation Forum
<b>WISP</b>	wireless internet service provider
<b>WISPA</b>	Wireless Internet Service Providers Association
<b>WP</b>	Working Party
<b>WP-8B</b>	Working Party 8B
<b>WRC</b>	World Radio Conference

## EXECUTIVE SUMMARY

Part 15 of Federal Communications Commission (FCC, the Commission) rules permits the operation of radio frequency (RF) devices without issuance of individual licenses to device operators. The Commission's Part 15 rules are designed to prevent harmful interference to assignments and licensees. Typically, unlicensed devices operate at low power over relatively short distances. They sometimes use techniques such as dynamic spectrum access or listen-before-talk protocols to reduce interference risk to other Part 15 operators as well as themselves. However, the primary operating condition for unlicensed devices is that their operators must accept any received interference and must immediately correct any harmful interference caused by their devices or else cease operation.<sup>1</sup>

In 1997, the Commission made available 300 megahertz of spectrum at 5.15-5.25 GHz, 5.25-5.35 GHz, and 5.725-5.825 GHz for use by a new category of unlicensed equipment regulated under Part 15, Subpart E of the Commission's rules, called unlicensed national information infrastructure (U-NII) devices. In 2003, the Commission made an additional 255 megahertz of spectrum available across 5.47–5.725 GHz.<sup>2</sup> These actions aligned the frequency bands used by U-NII devices in the United States with the frequency bands used by U-NII devices in other parts of the world, thus decreasing development and manufacturing costs by allowing the same products to be used in most parts of the globe.

Within the 5.47–5.725 GHz U-NII band, incumbent radio systems that would need to share spectrum with the new U-NII devices included Federal Aviation Administration (FAA) Terminal Doppler Weather Radars (TDWRs) that provide detection and alerts for wind shears at airports within the 5.60–5.65 GHz band. Additional types of federal radars also operated as incumbents in that spectrum. To facilitate spectrum sharing between U-NIIs and radars including TDWRs, a new detect-and-avoid technology called dynamic frequency selection (DFS) was jointly developed between government and industry. As a pre-condition of operation in the U.S. U-NII systems implemented DFS, causing U-NIIs in selected 5 GHz spectrum bands to detect the presence of radar signals and then avoid those radar frequencies.

In early 2009, after commercial deployment of DFS-equipped U-NIIs had begun in the U.S. and Possessions (US&P), the FAA reported interference to TDWRs at multiple locations in US&P. Early field studies performed by the National Telecommunications and Information Administration's (NTIA's) Institute for Telecommunications Sciences (ITS) and FAA engineering staff, with FCC support, indicated the interference sources were U-NII devices that incorporated DFS. The U-NII devices all operated in the same frequency band as the TDWRs and were from more than one manufacturer. Subsequent interference cases occurred involving radars at U.S. rocket test and launch ranges on the west and east coasts.

It was determined that most of these interference interactions resulted from either of two problems. One cause was unauthorized modification of certified U-NII devices (e.g., incorrect country code selection and/or usage of non-certified transmit antennae) by U-NII operators, resulting in U-NII non-response to radar signals. The other problem was U-NII non-detection of

---

<sup>1</sup> See 47 Code of Federal Regulations 15.5(b).

<sup>2</sup> The final (current) set of U-NII bands eventually became: 5.15–5.25 GHz (U-NII-1); 5.25–5.35 GHz (U-NII-2A); 5.470–5.725 GHz (U-NII-2C); 5.725–5.850 GHz (U-NII-3); and 5.850–5.925 GHz (provisionally U-NII-4).

radars because of insufficient data on radar characteristics such as pulse repetition frequency (PRF) that had been used to originally develop DFS.

This report documents the approach that was used to develop and deploy DFS enabled U-NII devices, the radar interference cases that followed, and the reasons that the interference occurred. It identifies the following Lessons Learned and corollaries that can be applied to future implementation dynamic spectrum sharing technologies in other frequency bands:

**Lesson 1:** The development time for dynamic spectrum technologies, even when government and industry work closely and cooperatively together on the necessary technical and regulatory framework, can be something on the order of a decade. This is because innovation requires considerable advance work in the absence of existing implementations. The more innovative and technically challenging the new sharing scheme, the longer the advance-work timeline can be expected to be.

**Lesson 2:** The use of dynamically based spectrum sharing technologies requires permanent, ongoing government expenditures for testing facilities and maintenance of trained, competent engineering staff for permanent ongoing surveillance of such devices. This state must continue for as long as any given class of dynamic spectrum-sharing devices continues to be sold and used in markets. Dynamic spectrum sharing is associated with ongoing post-certification compliance auditing<sup>3</sup> costs. This is not to say that the expenditures are not worth the advantages that society gains from more and better spectrum sharing; it is to say that such sharing has recurring technology-opportunity costs. The need for adequate ongoing technical auditing resources needs to be recognized.

**Corollary to Lesson 2:** Technical analysis and measurements will have to be performed to assess the impact of changing U-NII device technology on incumbent federal radar systems.

**Lesson 3:** Any non-trivial, innovative, dynamic spectrum sharing technology introduction, no matter how carefully it is initially devised, may result in some elevated interference potential when it is initially deployed. The more complicated or innovative the technology, the more likely it is that some unanticipated field-deployment situation may result in an increase in the potential for interference.

**Corollary to Lesson 3:** When new, innovative dynamic spectrum sharing technologies are introduced, resources should be set aside in advance to accommodate and resolve the inevitable initial harmful interference cases that may be expected to occur.

**Lesson 4:** Post-certification compliance auditing may be necessary to identify spectrum sharing devices that have been illegally sold without proper regulatory certification.

**Lesson 5:** If installers and operators are physically able to illegally modify spectrum sharing devices to disable spectrum-sharing features, some will do so even knowing that they will be fined by regulators when they are eventually caught.

---

<sup>3</sup> Such auditing, when done by NTIA, is done on DFS-equipped U-NII devices that NTIA purchases off-the-shelf from commercial vendors.

**Corollary 1 to Lesson 5:** Manufacturers need to restrict the ability to disable or modify their devices' spectrum sharing functionality as much as is physically possible. Regulatory entities need to thoroughly examine all of a spectrum-sharing device's set-up and control sub-menus.

**Corollary 2 to Lesson 5:** Introducing legitimate, legal spectrum sharing devices to a band can have the unintended consequence of encouraging the proliferation of illegal devices in the same band. This is especially true if the band is used worldwide for such functions, but does not have the same spectrum sharing rules internationally as the U.S. has domestically.<sup>4</sup>

**Lesson 6:** There is no substitute for person-to-person interchanges of critically important design information about technical requirements and needs for spectrum sharing systems. These human interchanges (as opposed to non-human interactions such as database sharing) must be between and among multiple government agencies (including regulatory agencies and agencies operating incumbent radio systems), industry that is developing new devices, and private sector companies that will eventually buy and operate the devices.

**Lesson 7:** Development and implementation of a dedicated operational testbed might be well-advised, prior to widespread introduction of a new spectrum sharing technology. But testbeds consume time and resources to build and operate. They tend to run counter to the desire to develop and deploy new technologies as quickly and inexpensively as possible

**Lesson 8:** Some technical spectrum sharing parameters cannot be known until after spectrum-sharing devices have been built and possibly deployed. This lack of knowledge can result in flaws in spectrum sharing device certification testing.

**Lesson 9:** Shortcomings in certification testing (such as initially inadequate radar waveform characterization for DFS) may only be discovered after a variety of devices (multiple models marketed by numerous manufacturers) have already been tested, certified, and deployed.

**Corollary to Lesson 9:** In hindsight, it would have been well advised for commercially produced 5 GHz DFS-equipped U-NII devices to have been initially introduced at a limited number of pre-identified field sites in close proximity to TDWRs (and other 5 GHz radars). Their operations at those sites could have been evaluated, with corrections to certification testing, prior to full-scale certification and deployment of such devices in open markets.

**Lesson 10:** Certification testing requirements for spectrum sharing devices need to be as technically robust as possible. Manufacturers may have concerns that some certification testing might be difficult to pass. But experience has shown that if devices are allowed to pass testing with less-than-robust protocols, their developers tend to build devices that only meet the reduced requirements. Such devices may then tend, disproportionately, to cause harmful interference to incumbent systems when they are deployed at field locations.

---

<sup>4</sup> Another possible explanation for this phenomenon is the fact that software defined radio (SDR) technology, which introduced the ability to tailor devices to applicable requirements in any country of anticipated operation, was developing coincident with DFS. As such, instances where the wrong country code was selected may have occurred even in the absence of the DFS arrangement.



**Lesson 11:** Some technical modifications or additions may need to be made to develop new or improved spectrum sharing technology subsequent to initial market introduction.

It should be noted that as a result of lessons learned from the limited interference incidents described in this report, the FCC has already implemented changes and modifications to technical requirements that are applicable to DFS-equipped U-NII devices applying for FCC certification. These changes include: 1) a new requirement to lock down the country code setting to preclude manipulation by third party installers and/or users; 2) an increase in the required DFS detection bandwidth; and 3) an effective reduction in the unwanted emissions limit through a change in measurement procedure.

It should also be noted that as a result of lessons learned by the DFS industry, improved self-policing has also been introduced, in large part to avoid a repeat of having DFS certification suspended as it was for nearly three years while these incidents were under investigation.

# LESSONS LEARNED FROM THE DEVELOPMENT AND DEPLOYMENT OF 5 GHZ UNLICENSED NATIONAL INFORMATION INFRASTRUCTURE (U-NII) DYNAMIC FREQUENCY SELECTION (DFS) DEVICES

Frank H. Sanders,<sup>5</sup> Edward F. Drocella,<sup>6</sup> Robert L. Sole,<sup>6</sup> John E. Carroll<sup>5</sup>

This report is a case-history of the development, deployment, and operational experiences associated with 5 GHz unlicensed national information infrastructure (U-NII) devices that incorporate a detect-and-avoid approach to spectrum sharing. Such dynamic frequency selection (DFS) technology was authorized by the Federal Communications Commission (FCC) to accommodate co-band operation of U-NII transmitters among other incumbent radio systems, specifically radars. DFS-equipped U-NII systems are designed to detect frequencies occupied by radar transmissions and then command their own transmitters to avoid operation on those occupied frequencies. Examining the historical and technical aspects of the development and deployment of 5 GHz DFS-equipped U-NIIs, this report focuses on issues encountered with the deployment of this nascent DFS technology, particularly with respect to two government radar systems that have experienced harmful interference: Terminal Doppler Weather Radars (TDWRs) and Range Instrumentation Radars (RIRs). These interference interactions and the likely underlying causes are described, along with steps that have already been taken in an effort to mitigate existing and potential future interference interactions. This report's narrative summarizes the DFS experience and shares the Lessons Learned from these experiences that may be applied to future similar spectrum-sharing approaches.

**Keywords:** 5 GHz band; access point (AP); band sharing; detect and avoid; Dynamic Frequency Selection (DFS); electromagnetic compatibility (EMC); emission limits; out-of-band (OOB) emissions; radar; radio interference; Range Instrumentation Radar (RIR); Terminal Doppler Weather Radar (TDWR); spectrum measurement; spectrum sharing; spurious emissions; unlicensed national information infrastructure (U-NII)

## 1. INTRODUCTION

Dynamic frequency selection (DFS) is a technique for sharing spectrum at 5 GHz between incumbent radars (which are primarily federal government systems) and a subset of wireless access systems (WASs) called unlicensed national information infrastructure (U-NII). As of the date of this report, DFS-equipped systems are routinely used at locations across the United

---

<sup>5</sup> The author is with the Institute for Telecommunication Sciences, National Telecommunications and Information Administration, U.S. Department of Commerce, Boulder, CO 80305.

<sup>6</sup> The author is with the Office of Spectrum Management, National Telecommunications and Information Administration, U.S. Department of Commerce, Washington DC 20230.

States. DFS can now be considered to be a mature technology. But based on ongoing experience with the technology as deployed, some incremental improvements can still be made, such as changes to the radar waveforms that are used for certification testing of new DFS-equipped systems.

Many 5 GHz radars are legacy systems, but DFS is designed to accommodate new, future radar systems as well. The parameter space (pulse widths, pulse repetition rates, and chirp characteristics) of radar waveforms used for DFS certification testing is supposed to be large enough to accommodate future radar systems that may eventually be introduced at 5 GHz.

DFS-equipped U-NII data communication systems are typically operated by private sector operators for last-mile radio connectivity between wireless Internet service providers (WISPs) and their customers. DFS is a detect-and-avoid spectrum sharing technology that is implemented entirely in the U-NII systems; radars sharing the same spectrum are not re-engineered or otherwise modified under the DFS scheme.

The FCC does not specify a technology for the U-NII bands. Commonly used technologies in DFS-equipped systems are based on Institute for Electrical and Electronic Engineers (IEEE) 802.11 standards.<sup>7</sup> DFS-enabled non-802.11 technologies include WiMAX communication links, video surveillance data links, low data rate inventory control devices, and wireless speakers.<sup>8</sup> For all DFS-equipped systems, U-NIIs monitor their own operational frequencies for radar signals within time slots that are themselves placed in between system data-packet exchanges. When a radar signal is detected by a U-NII receiver above a defined power threshold,<sup>9</sup> the U-NII system coordinates a new frequency among its individual nodes (transmitters and receivers called access points (APs) and clients). An AP and its clients then simultaneously switch their operations to the new, non-conflicting frequency. (If an AP tries to use a new frequency in a DFS mandated U-NII band, the AP must check the new channel for radar activity for one minute before transmitting.) All of this occurs within a defined time interval. No attempt is made to re-use the first frequency for 30 minutes.<sup>10</sup>

This report provides an overview and summary of experience that government and industry have gained in the course of 5 GHz DFS development, deployment, and operations. The sum total of the experience gained is encapsulated in eleven Lessons Learned that can be applied to the development and introduction of other spectrum sharing schemes in other bands and with other systems in the future.

---

<sup>7</sup> 802.11h is the IEEE standard that incorporated DFS support into the 802.11 series to expand the available channels for 802.11a from 12 to 23 non-overlapping channels in the 5 GHz band. 802.11b is a legacy 2.4 GHz exclusive standard. It has been replaced, for the most part, by 802.11g in the 2.4 GHz band. 802.11n adds multiple input, multiple output (MIMO) support and combines 802.11a and 802.11g to provide dual 2.4 GHz and 5 GHz support. 802.11a/c is an expansion of 802.11a/n in the 5 GHz band to support increased data rates via enhanced MIMO, wider bandwidths, and higher density modulation.

<sup>8</sup> NTIA has worked with the FCC to apply specialized DFS performance testing procedures for non-802.11 devices.

<sup>9</sup> The threshold is defined in terms of spectral power density, a certain amount of power per unit bandwidth. This is -62 dBm/MHz or -64 dBm/MHz, depending on DFS system characteristics.

<sup>10</sup> When (or if) use of the original frequency is re-attempted, that frequency is first re-monitored for any radar signal presence.

The authors were involved, along with many other people in multiple agencies and industry (see Acknowledgements) in all phases of DFS development, deployment, and post-deployment. They have worked for years on interference analysis and mitigation, dating from the 1990s to ongoing present work. While dozens of documents are referenced in this report, the authors' own, direct experience with DFS, especially testing DFS devices and troubleshooting interference problems, is provided without referenceable documentation (where only personal notes and recollections exist) so that their experience can be added to the formal record.

## 1.1 Report Organization

The remainder of this report is structured as follows. Section 2 describes the historical timeline of the development of DFS, mentioning DFS technical details only in passing. The decade-long effort that it recounts demonstrates the extensive work that had to be accomplished among multiple international and domestic standards bodies and regulators, both industry and government, to make DFS a reality. This section shows that spectrum sharing schemes inherently involve many complexly interlocking organizations (on the people side) and multiple radio systems (on the hardware side).

Section 3 looks again at DFS historical development, but focuses on the technical *minutiae*. The bifurcation of Sections 2 and 3 is required by the need to describe both forks of DFS development (i.e., the human narrative versus the technical narrative).

Section 4 describes DFS technical principles and implementation as finally agreed and defined between government and industry. It includes rules and requirements for DFS.

Section 5 describes challenges that DFS has posed for U-NII manufacturers and vendors. It lists enforcement actions that have been taken by the government against some U-NII operators for violations of DFS regulations.

Section 6 describes the challenges that DFS has posed for the government in its development and testing. These include the difficulty of needing to define rules and requirements for these radio systems before they were designed or built.

Section 7 recounts the successes and failures that occurred when DFS was first deployed in commercially available packages. This narrative leverages earlier NTIA reports to describe interference that occurred after initial commercial deployment in the New York City and San Juan, Puerto Rico, areas.

Section 8 describes interference that has occurred to radars at rocket test and launch ranges on the U.S. east and west coasts. It reinforces the Lessons Learned from the Terminal Doppler Weather Radar (TDWR) experience.

Section 9 describes the ongoing support that has been required of the government in the decade and a half that has elapsed since DFS was originally commercially deployed.

Section 10 summarizes the Lessons Learned from the entire DFS experience.

## **1.2 Gradual Introduction of Lessons Learned as the Report Progresses**

The eleven Lessons Learned and corollaries from the DFS experience are introduced sequentially as the report progresses. Each Lesson Learned is stated at the conclusion of the part of the report that led to it. Thus the reader learns, from reading the text preceding each Lesson Learned, how each one originated.

## 2. NARRATIVE REVIEW OF DFS SPECTRUM SHARING TECHNOLOGY DEVELOPMENT

This section describes the historical timeline for the development of DFS at 5 GHz. It does not focus on DFS technical details. Section 3 looks again at DFS historical development, but with focus on the technical *minutiae* of DFS. This bifurcation is required by the need to describe both forks of DFS development, and by the great complexity of both of those forks. A take-away lesson from reading these two sections should be that development and implementation of DFS was immensely complex, both administratively and technically.

### 2.1 Historical Development of Spectrum Sharing Arrangements and Management Approaches

Conventional spectrum management practices developed largely because of interference problems resulting from uncoordinated broadcasting and long-distance (so-called high frequency, below about 30 MHz) transmissions that were common during the first two decades of the 20<sup>th</sup> century. As radio spectrum became more crowded, spectrum managers controlled interference among the growing volume of users by delineating radiofrequency spectrum bands. Users were grouped by radio services (e.g., fixed, mobile, and broadcasting) and authorized to operate on specific frequencies in bands related to those services. Specific technical rules set parameters such as maximum operating power, maximum antenna gain, overall maximum power output, and sometimes even specific modulation and bandwidth requirements.<sup>11</sup>

As demand for radio spectrum continued to grow, spectrum authorities began to allow static sharing arrangements between different radio services. In such cases, users from different radio services were required to meet strict technical requirements limiting operating power, unwanted emissions, antenna gain, etc., and, in some instances, operational restrictions (e.g., antenna directionality and time of day). In many cases, “shared” bands have been sub-divided in terms of distinctive but compatible service use. Incumbents have been given “priority rights” to a band where sharing users are restricted by operational rules developed to protect the incumbent users. This type of sharing, with designations for primary and secondary users and services in the U.S. and international tables of spectrum allocations [1], has provided some opportunity to accommodate additional users in shared bands, while also limiting potential harmful interference between the incumbents’ and sharing users’ operations.<sup>12</sup>

Market pressures to accommodate more radio spectrum users and the recognized need to increase efficient use of spectrum led industry to develop two types of opportunistic sharing arrangements referred to as “underlay” and “overlay.” The “underlay” concept refers to cases where transmitters operate basically beneath the noise floor of other services. There may be some increase in the overall noise floor for a primary service, but technical and operational limits are established for the opportunistic service to ensure that harmful interference is not received by the incumbent. Unlicensed devices employing this kind of sharing are still subject to the requirements that they should not cause harmful interference and can claim no protection from harmful interference, as specified in §15.5 of the FCC rules. This type of arrangement limits the

---

<sup>11</sup> FCC Radio Broadcast Services, 47 CFR § 73.

<sup>12</sup> FCC Frequency Allocations and Radio Treaty Matters; General Rules and Regulations, 47 CFR § 2.100-8.

type of sharing operation because the technical and operational limits are based on allowing simultaneous transmissions by incumbent systems and the opportunistic systems. The FCC General Part 15 rules are based on this concept and require that opportunistic systems meet specific testing requirements in order to operate with existing incumbent systems.<sup>13</sup> Such sharing arrangements provide no operational assurance for underlay systems. As such, they are rarely used for critical communication applications, but instead are primarily used for very short range consumer devices, such as garage door openers, car access remote controls, etc.

The “overlay” concept, embodied in a variety of WASs, allows new users to transmit during quiet periods when incumbent users are not transmitting on their assigned bands.<sup>14</sup> This type of arrangement recognizes that spectrum must be available for incumbent services as needed, but allows the new, innovative systems to utilize spectrum resources in periods, however brief, when the assigned frequencies are not being used by incumbents.<sup>15</sup> By using detection and avoidance techniques the WAS devices can access spectrum, at any particular point in time and for a given location, when the spectrum is not being used by incumbent users.<sup>16</sup> One WAS scheme, which is the focus of this report and operates in the 5 GHz part of the spectrum, is DFS.

As a greater number of services utilize opportunistic sharing techniques that use adaptive, cognitive or software defined radio (SDR)<sup>17</sup> techniques, it would be short-sighted to conduct interference analysis and planning based solely on conventional spectrum management techniques that rely purely on limiting the technical parameters of transmitters and receivers. For systems using opportunistic capabilities, like DFS capability at 5 GHz, sharing partners and spectrum managers need to develop minimum operational requirements that define a system’s ability to detect and avoid incumbent systems that have spectrum “rights” to a particular frequency band.<sup>18</sup> This spectrum management approach can give industry a degree of flexibility not found in prior sharing arrangements and will allow opportunistic sharing opportunities to develop and grow in the future.

## **2.2 Historical U.S. Radar Band Usage and a New Idea for Overlay Sharing**

Although many radio spectrum bands have historically been shared between distinct services, the radiolocation service (called “radar” in this report) has for the most part not shared its bands with other services. That is, radar bands have tended to be exclusive to that service. U.S.-allocated radar bands are relatively wide. From ultra-high frequency (UHF) to 18 GHz, they are 420-450 MHz, 1215-1390 MHz, 2700-3650 MHz, 5250-5925 MHz, 8.5-10.5 GHz, and

---

<sup>13</sup> FCC Radio Frequency Devices, 47 CFR § 15.

<sup>14</sup> FCC Radio Frequency Devices, 47 CFR § 15.

<sup>15</sup> The Defense Advanced Research Projects Agency (DARPA) XG program has experimented with similar detect-and-avoid operational ideas. Also, in FCC ET Docket No. 04-186, the FCC considers the operation of non-television radio devices in “TV white spaces,” where locally unassigned television broadcast channels may be used for low-power non-television systems. This proceeding also involves a test program to examine the ability of prototype devices to detect and avoid occupied broadcast television channels (somewhat like DFS), and study the interference potential of such devices.

<sup>16</sup> FCC Radio Frequency Devices, 47 CFR § 15.

<sup>17</sup> SDRs use software, rather than hardware, to control a radio’s operational characteristics, allowing dynamic changes to a radio’s operating characteristics.

<sup>18</sup> FCC Radio Frequency Devices, 47 CFR § 15.

15.7-17.7 GHz.<sup>19</sup> These bands' widths are respectively 7%, 13%, 31%, 11%, 22% and 12% of the band center frequencies, the average being about 13%. Thus these radar bands represent significant portions of the spectrum between UHF and 18 GHz.

By the 1990s, as described below, demands for more spectrum for new systems led to interest in increased sharing between radars and other systems. The interest was not confined to spectrum use in the United States; several Administrations in the International Telecommunication Union Radiocommunication Sector (ITU-R) expressed interest in sharing between radars and other services.

By the late 1990s, industry groups in the U.S. and abroad began to circulate a new WAS concept for sharing between radars and other systems. Called unlicensed national information infrastructure (U-NII), this WAS idea was inspired by the perception that some spectrum being used by incumbent radar systems might be relatively underutilized in time and space (based on the relatively low operational duty cycles of radar waveforms and the relative sparsity of radars in space) and could be used by new, unlicensed radio systems without adversely impacting the operations of the radar incumbents. Incumbent systems that were identified as being possibly able to share with new systems were using spectrum between 5 to 6 GHz. In the U.S., the spectrum that became a candidate for this sharing was a segment inside the 5250-5925 MHz band.

The idea of 5 GHz spectrum-sharing U-NII development eventually gained support in the ITU-R. No other administration, however, has the amount of radar infrastructure that the U.S. administration has, both military and civilian. Other administrations therefore arguably had less at risk in the development of radar spectrum sharing with WAS than did the U.S.

## **2.3 Historical Narrative of WAS at 5 GHz: A Decade of Development**

In 1995, telecommunications firms began to crystallize plans to develop the 5 GHz band for WAS. WAS designs were aimed primarily for wireless networking, requiring broad bandwidths to meet data transfer requirements, in contrast to advanced cellular systems that were providing traditional voice and narrow bandwidth data communications. Initial plans called for these devices to operate principally indoors and at fairly low power levels.<sup>20</sup>

### **2.3.1 Initial FCC Rulemaking Efforts**

Early industry efforts in Europe led to an initial designation of two bands at 5 GHz (5150-5350 MHz and 5470-5725 MHz) for providing wireless networking, based on the high performance radio local area network (HIPERLAN) standard. With a clear interest in developing a more global market, the industry petitioned the FCC to create rules for a domestic WAS.<sup>21</sup>

---

<sup>19</sup> There are amateur secondary allocations in 420-450 MHz; 1240-1300 MHz; 3300-3500 MHz; and 5650-5925 MHz.

<sup>20</sup> FCC ET Docket 96-102.

<sup>21</sup> These efforts did not provide complete harmonization with European efforts, since the FCC selected the 5.15-5.35 GHz and 5.725-5.825 GHz bands initially for service development.



Apple Computer, Inc. became the early U.S. industry leader by petitioning the FCC for a rulemaking to designate an unlicensed national information infrastructure (U-NII) band for what later would develop into a WAS.<sup>22</sup> This petition, together with an earlier petition by an industry consortium, the Wireless Innovation Forum (WInnForum), proposed to harmonize U.S. and European spectrum planning efforts at 5 GHz.<sup>23</sup>

These petitions raised important initial questions, including the manner in which U-NII devices could share the proposed frequency bands with incumbent radar systems, if at all. In response to these petitions, on January 9, 1997, the FCC adopted an underlay scheme for sharing three bands of 100 MHz each at 5.15-5.25 GHz, 5.25-5.35 GHz and 5.725-5.825 GHz.<sup>24</sup> The FCC's decision required specific power limits, emission limits, and other technical rules appropriate for unlicensed Part 15 operations, based on sharing conditions for each of the three designated 5 GHz bands. Consistent with Part 15 operating rules, these devices were required to protect incumbent federal systems and operate at low power levels.<sup>25</sup> The FCC also believed that authorization under Part 15 rules would be sufficient to address interference concerns since unlicensed devices are required to cease operation when they cause interference and must accept interference from authorized systems.<sup>26</sup>

Throughout the eighteen months that preceded the FCC's January 1997 decision, and until June 1998 when the FCC adopted an Order addressing reconsideration petitions,<sup>27</sup> the interested parties were handicapped by incomplete technical information, skepticism about the viability of sharing in this band, and worries about technical and operational constraints applied to the potential sharing partners. Initial industry proposals lacked specific technical and operational

---

<sup>22</sup> Apple petitioned the FCC on May 24, 1995 for a rulemaking for "the creation of a new band of frequencies for high capacity, unlicensed wireless data – the NII Band." Apple wanted to promote technology development and harmonize frequencies between Europe and the United States by promoting common 5.15-5.35 GHz and 5.725-5.850 GHz bands. Apple also asked the FCC to establish new Part 16 rules to give these devices some operating protection from other unlicensed devices. See Apple Petition for Rulemaking, *supra* note 20 at pages 5-6.

<sup>23</sup> In a May 15, 1995 petition to the FCC, the WInnForum advanced the idea that "the high speed SUPERNet is the next generation of wireless information transmission systems." WInnForum sought allocation of the 5.10-5.35 GHz band, chosen because it would maintain compatibility with the European HIPERLAN developments. This petition provided information that complemented the Apple petition. See WInnForum Petition for Rulemaking, *supra* note 20 at 21.

<sup>24</sup> U-NII Report and Order in ET Docket No. 96-102 *Amendment of the Commission's Rules to Provide for Operation of Unlicensed NII Devices in the 5 GHz Frequency Range*, (January 9, 1997), [https://transition.fcc.gov/Bureaus/Engineering\\_Technology/Orders/1997/fcc97005.pdf](https://transition.fcc.gov/Bureaus/Engineering_Technology/Orders/1997/fcc97005.pdf).

<sup>25</sup> U-NII Memorandum Opinion and Order in ET Docket No. 96-102 *Amendment of the Commission's Rules to Provide for Operation of Unlicensed NII Devices in the 5 GHz Frequency Range*, (June 17, 1998), [https://transition.fcc.gov/Bureaus/Engineering\\_Technology/Orders/1998/fcc98121.txt](https://transition.fcc.gov/Bureaus/Engineering_Technology/Orders/1998/fcc98121.txt)

<sup>26</sup> CFR 47 Part 15.407.

<sup>27</sup> Petition for Reconsideration in ET Docket No. 96-102, *Amendment of the Commission's Rules to Provide for Operation of Unlicensed NII Devices in the 5 GHz Frequency Range*, (March 3, 1997); Petition for Reconsideration in ET Docket No. 96-102, *Amendment of the Commission's Rules to Provide for Operation of Unlicensed NII Devices in the 5 GHz Frequency Range*, (March 3, 1997); Wireless Information Networks Forum Petition for Reconsideration in ET Docket No. 96-102, *Amendment of the Commission's Rules to Provide for Operation of Unlicensed NII Devices in the 5 GHz Frequency Range*, (March 3, 1997).

details needed for a comprehensive electromagnetic compatibility (EMC) analysis to ensure that U-NII devices would be compatible with existing federal systems.<sup>28</sup>

Using the available technical and operational data for U-NII devices and information regarding the technical characteristics of incumbent federal systems and how they were deployed, NTIA performed an analysis that the FCC used to establish the technical parameters for U-NII devices.<sup>29</sup> Based on the information available at the time, the analysis assumed that U-NII devices would be used primarily indoors. Incumbent military radar systems were typically used only on military facilities located beyond heavily populated areas where U-NII device deployment was expected to be extensive. The assumptions underlying NTIA's analysis were coordinated with the federal agency representatives on the Interdepartment Radio Advisory Committee (IRAC). NTIA recognized that if the assumptions regarding deployment of the U-NII devices and incumbent radar systems changed, there could be potential problems. NTIA recommended that channel monitoring protocols be used in conjunction with dynamic channel selection to protect federal users.<sup>30</sup> The FCC did not adopt NTIA's proposal to require channel monitoring and dynamic channel selection.

The FCC's January 1997 Order brought reconsideration petitions from industry.<sup>31</sup> WinnForum, Apple, and the Hewlett Packard Company asked for higher power operations and higher gain antenna allowances in all three designated bands.<sup>32</sup> Concerned about the additional interference potential suggested by the petitions, NTIA opposed the proposed Part 15 modifications and urged the FCC to limit the use of both mobile and fixed devices near military bases and test ranges because of likely interference to such devices from high-power federal radar systems.<sup>33</sup>

On June 17, 1998, the FCC amended its rules to permit higher power fixed, outdoor point-to-point U-NII devices in the 5.725-5.825 GHz band. It denied industry requests for higher power and increased antenna gain in the 5.15-5.25 GHz and 5.25-5.35 GHz bands.<sup>34</sup> In this decision, the FCC attempted to balance industry's desire for more flexible operational characteristics with protection of federal systems.

Between 1998 and 2000 several key factors changed the electromagnetic compatibility picture between the U-NII devices and federal radar systems. In its original analysis, NTIA initially characterized U-NII devices as operating primarily indoors. However, new applications subsequently included the use of the technology to support Internet backhaul communications.

---

<sup>28</sup> *Report of the First Meeting*, Radiocommunication Study Groups of International Telecommunication Union, Joint Rapporteur Group 8A-9B, Doc. 8A-9B/27-E at 94 (October 19, 2000); *Report of Second Meeting*, Radiocommunication Study Groups of International Telecommunication Union, Joint Rapporteur Group 8A-9B, Doc. 8A-9B/55-E at 144 (March 27, 2001).

<sup>29</sup> Reply Comments of the National Telecommunications and Information Administration in ET Doc. No. 96-102, *Amendment of the Commission's Rules to Provide for Unlicensed NII/SUPERNet Operations in the 5 GHz Frequency Range*, (August 16, 1996).

<sup>30</sup> *Id.* at page 11.

<sup>31</sup> See U-NII Petitions for Reconsideration, *supra* note 27 at page 11.

<sup>32</sup> *Id.* at page 6.

<sup>33</sup> Letter to Mr. Richard Smith, Chief, Office of Engineering and Technology, Federal Communications Commission, from Dr. Richard D. Parlow, Associate Administrator, Office of Spectrum Management, National Telecommunications and Information Administration, in ET Docket No. 96-102 (April 18, 1997).

<sup>34</sup> See June 1998 U-NII Device Order, *supra* note 25.

This condition can cause U-NII signal interaction with federal radars over unobstructed signal propagation paths, effectively increasing the interference potential.

Other than some weather radars, many radars at 5 GHz were initially assumed by the U.S. government and private industry to be limited to operating on or near military installations for testing and training. However, this usage pattern was based on practices prior to the terrorist attacks of September 11, 2001. One area of concern in assessing interference to military radars from U-NII systems involved wider possible future radar deployments and an expanded domestic role for military radars in support of homeland defense. Changing usage requirements could result in a need to deploy military radars in and near cities and close to highways where U-NII devices would be expected to have their highest usage. Such changes in usage patterns needed to be considered in the development of 5 GHz U-NII service rules that would be effective in protecting federal radar systems.

### **2.3.2 International Developments and FCC Rulemakings Between 2000 and 2003**

Substantial development occurred between 2000 and 2003.<sup>35</sup> By 2000, manufacturers began to push for world-wide allocations for WAS. The idea was to take advantage of massive potential economies of scale in being able to sell the same devices in many countries with few or no variations from one country to the next. Based on U.S. and European proposals to the 2000 World Radiocommunication Conference (WRC-2000), three separate spectrum bands were delineated for consideration within an agenda item for WRC-03.<sup>36</sup> These were 5.15-5.25 GHz, 5.25-5.35 GHz, and 5.47-5.725 GHz. The last band was based solely on European input and provided an additional 255 MHz of spectrum not previously considered for WAS operations within the United States.<sup>37</sup>

Following up on its initial skepticism about the viability of sharing with existing radar operations in the 5 GHz band, NTIA had suggested, as early as 1996, that channel monitoring protocols, used in conjunction with dynamic channel selection capabilities, could be effective in

---

<sup>35</sup> The international proceedings for development of treaty text were considered in the International Telecommunication Union (ITU), Radiocommunication Sector (ITU-R), Study Groups (SG). More information on the ITU and its structure can be found at [www.itu.int](http://www.itu.int). Various Working Parties (WP) of individual SGs were involved in development of the technical and regulatory work associated with the ultimate treaty text that was completed related to WASs, including RLANs at 5 GHz. This work was liaised between the contributing WPs, and for purposes of this case study the summary discussions found in the Chairman's Reports for the Joint Rapporteurs Group 8A-9B (JRG 8A-9B) (a combined effort between WP's 8A and 9B under the respective SG 8 and SG 9 responsibilities) which was developed specifically to address WASs is used for cites to the international work. The Chairman's Reports of JRG 8A-9B provide an overall summary of the discussions related to many input contributions to each meeting and summarize the appropriate output documents that were developed in support of the World Radiocommunication Conference (WRC) held in 2003 (WRC-03) where treaty text was developed for the 5 GHz WASs, including RLANs. This includes liaison activity from other contributing groups within the ITU-R SG structure. This treaty text is related to the U.S. 5 GHz UNII CFR 47, Part 15 rules that were developed and also referenced in this case study. Access to the documents developed in the ITU-R SG structure is limited to individuals with access to the ITU-R document center (TIES Account). All documents from the ITU referenced in this case study are available from the author.

<sup>36</sup> *Resolution 800, Agenda for the 2003 World Radiocommunication Conference*, World Radiocommunication Conference, International Radiocommunication Union (March 25, 2000) [hereinafter *Agenda for 2003 WRC*].

<sup>37</sup> *European Common Proposals for the Work of the Conference*, World Radiocommunication Conference, International Telecommunication Union. Addendum 8 to Doc. 13-E at 6 (March 25, 2000).

minimizing interference. NTIA recommended that the FCC mandate receiver standards and that industry incorporate adaptive capabilities in the new 5 GHz devices.<sup>38</sup> These recommendations were not adopted by the FCC in its 1997 and 1998 Orders,<sup>39</sup> the preference being to allow such receiver standards to be developed within industry-participation standards groups such as the IEEE 802.11 Wi-Fi® standards body.

This innovative approach gained no traction domestically as the international and U.S. industry shifted their focus to 5 GHz proposals in European venues. But by 2000, driven by strong interest shown by European regulators in adaptive radio system capabilities, the industry began working to define DFS spectrum etiquette protocol that would require 5 GHz devices to dynamically reassign channels based on detection and avoidance of incumbent signals.<sup>40</sup>

Meanwhile, efforts to find an initial U.S. consensus position on developing a world-wide allocation for WAS were slowed by several factors, including sparse participation in U.S. preparatory processes for WRC-03, inadequate technical information and changing technical criteria. U.S. government representatives remained pessimistic about the feasibility of sharing with a wide variety of radar systems operating in the 5 GHz band (particularly in the specific bands 5250-5350 MHz and 5470-5725 MHz). U.S. delegates to meetings of the International Telecommunication Union Radiocommunication Sector (ITU-R) preparing technical material for WRC-03 lacked adequate information from which to develop detailed, workable sharing arrangements that sufficiently addressed their interference concerns. Lacking detailed information on WAS device design and operational characteristics of incumbent military systems, U.S. representatives to these meetings used a “best guess” approach to develop proposed alternative technical rules for WAS devices.<sup>41</sup> Industry representatives strongly objected to the resulting proposed rules as unworkable, asserting that such constraints would not lead to marketable products.<sup>42</sup> This led to a virtual stalemate between industry and government interests working on the 5 GHz issue.

Another factor related to the technical work involved a shift from the HIPERLAN standard, developed earlier by the European standards body, to more recent IEEE standards work related to its Wi-Fi and 802.11 development activities.<sup>43</sup> While this shift complicated efforts to define a reasonable sharing situation, caused some delay, and invalidated some earlier technical work, the IEEE work was eventually widely accepted and adopted as the technical basis for all subsequent work globally.<sup>44</sup>

---

<sup>38</sup> See NTIA Reply Comments Aug. 16, 1996, *supra* note 29 at pages 3-4.

<sup>39</sup> See January 1997 U-NII Device Order, *supra* note 24; June 1998 U-NII Device Order, *supra* note 25.

<sup>40</sup> *Report of the Third Meeting*, Radiocommunication Study Groups of International Telecommunication Union, Joint Rapporteur Group 8A-9B, Doc. 8A-9B/98-E at 144 (December 6, 2001).

<sup>41</sup> *Id.* at 101., See ITU-R Report of First Meeting, *supra* note 28 at 94; ITU-R Report of Second Meeting, *supra* note 28 at 144.

<sup>42</sup> *Report of the Fourth Meeting*, Radiocommunication Study Groups of International Telecommunication Union, Joint Rapporteur Group 8A-9B, Doc. 8A-9B/132-E at 6 (May 8, 2002).

<sup>43</sup> *Id.*

<sup>44</sup> *Report of Sixth Meeting*, Radiocommunication Study Group of International Telecommunications Union, Joint Rapporteur Group 8A-9B, at 2.1 (February 4, 2003); *Changes to Agenda Item*, Radiocommunication Sector of International Telecommunication Union, Conference Preparatory Meeting for WRC-03, United States, Doc. CPM02-2/141-E (November 11, 2002).

Internationally, the U.S. delegations to ITU-R meetings continued to press for several conditions to address ongoing concerns about the potential for interference to radar receivers. First, since earlier analyses indicated that conventional spectrum management practices, such as power limits, would not alone be sufficient to provide the required protection, the United States advanced a proposal within the ITU-R to mandate operational requirements instead of more conventional power and antenna gain limitations.<sup>45</sup> Second, the U.S. Department of Defense (DoD) was asked by NTIA and the FCC to supply details regarding its radar operations in order to develop more realistic sharing analyses.<sup>46</sup> The United States also sought inclusion of detect-and-avoid measures in international agreements related to operational requirements.<sup>47</sup>

By October 2001, international agreement was reached to define operational requirements as a regulatory mechanism.<sup>48</sup> International agreements also called for definition of the minimum detect-and-avoid requirements in terms of: 1) a power detection threshold built into WAS to trigger WAS channel moves away from frequencies occupied locally by radars; 2) a time limit to be allowed for these channel moves; and 3) in-service WAS spectrum monitoring for radar signals, expressed as a defined listening period to be repeated continually at set intervals of time.<sup>49</sup>

While progress was being made in defining rudimentary DFS parameters, the emerging U.S. position in preparation for WRC-03 called for “no change” in existing allocations at 5 GHz, due in part to sparse industry participation in U.S. preparatory processes and continuing potential interference concerns in the 5.25-5.35 GHz band.<sup>50</sup> Faced with the prospect of no allocation for WAS at 5 GHz, a major shift in industry participation occurred in 2002. At this point, industry representatives offered to work actively on U.S. preparations to WRC-03 and lobbied NTIA and DoD for a change in the U.S. position.<sup>51</sup> In response to this high level of industry interest in developing WAS at 5 GHz, the State Department’s International Technical Advisory Committee for Radiocommunications (ITAC-R) created a specific project team to collaborate in developing an accurate picture of likely sharing conditions and to exchange key information about WAS device global market requirements and technical and operational specifications.<sup>52</sup>

Participants also learned more about incumbent system operational details. Based on this information, NTIA, FCC, and DoD worked with industry to develop computer models and detailed sharing scenarios that would be the basis for more realistic EMC analyses.<sup>53</sup> This specialized ITAC-R project team played a key role in creating an information flow and a

---

<sup>45</sup> *Report of the Fifth Meeting*, Radiocommunication Study Groups of International Telecommunication Union, Joint Rapporteur Group 8A-9B, Doc. 8A-9B/161-E at 6 (October 23, 2004).

<sup>46</sup> *Chairman’s Report Of Sharing Analysis*, International Telecommunications Advisory Committee for Radiocommunications, 5 GHz DFS Project Team, at page 4, (November 5, 2002).

<sup>47</sup> See ITU-R Report of Fifth Meeting *supra*, note 45 at 7.

<sup>48</sup> *Id.* at 109.

<sup>49</sup> *Id.* at 114.

<sup>50</sup> *Final list of participants*, Radiocommunication Study Group of International Telecommunications Union, Joint Rapporteur Group 8A-9B, at page 3 (January 23, 2003).

<sup>51</sup> See CPM Changes to Agenda Item *supra*, note 44.

<sup>52</sup> *ITAC-R 5 GHz Project Team Chairman’s Report*, International Telecommunications Advisory Committee for Radiocommunications, 5 GHz DFS Project Team, at page 1, (February 2, 2006).

<sup>53</sup> *Supra* note at pages 1-4.

collaborative process to reach a productive result that allowed the United States to eventually support a WAS allocation at 5 GHz.

The ITAC-R Project Team completed a large volume of work in less than six months. This consensus work had wide support from manufacturers; the group's work products were introduced and used at subsequent international meetings.<sup>54</sup> The U.S. position began to gain traction internationally, as more manufacturers shifted their focus from European venues to the U.S. domestic process. This collaboration quickly became the defining work for subsequent international studies. With the needs of both government and industry met, work progressed rapidly in the ITAC-R toward a shared goal of endorsing a WAS allocation at 5 GHz at WRC-03.

ITAC-R participants reached two important conclusions. First, traditional spectrum management planning practices would not be sufficient to address innovative radio systems that used adaptive functions based on SDR technology. Second, a detailed conformance test procedure and methodology would need to be developed to support spectrum management efforts. Rather than using the conventional spectrum management approach of setting static technical parameters such as power and antenna gain limits, the group agreed to specify a set of minimum operational requirements to ensure that radio systems employing adaptive functions could share spectrum with incumbent users. This approach would demand rigorous conformance test procedures while alleviating the need to review software changes which could occur frequently in a product lifecycle. This approach also simplified spectrum management requirements for multiple regulatory authorities. Devices operating under specific domestic rules could be approved based on conformance testing, without requiring reviews of literally millions of lines of programming code.<sup>55</sup>

The collaborative work also showed that sharing possibilities depended on adequate planning for likely aggregate interference to military radar systems. As a result, subsequent work focused on deployment scenarios involving urban, suburban, and rural population densities. This work showed that previous assumptions of what would constitute a worst-case scenario were not appropriate. Through the work of the ITAC-R project team, government and industry representatives created realistic deployment scenarios for the radar systems and developed estimates of WAS devices based on representative population density levels found in local markets. The ITAC-R had once again provided a venue for detailed technical discussions, exchange of information, and compromises that resulted in common agreement concerning an appropriate EMC analysis by all parties.

Consistent with this spirit of cooperation, DoD performed a detailed review of its operational requirements, revisiting the possibility of new sharing arrangements at 5 GHz. Based on this review, DoD subsequently suggested that airborne radars were not relevant to ongoing sharing

---

<sup>54</sup> See ITU-R Report of Sixth Meeting *supra*, note 44.

<sup>55</sup> Report and Order in ET Docket No. 03-287, 18 FCC Rcd 24484 (32), *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* (November 18, 2003), <https://www.fcc.gov/document/revision-parts-2-and-15-commissions-rules-permit-unlicensed-2>; and Memorandum Opinion and Order in ET Docket No. 03-122 *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*, (June 30, 2006), <https://www.fcc.gov/document/revision-parts-2-and-15-commissions-rules-permit-unlicensed>.

discussions because these systems did not operate where WAS devices would likely operate in large numbers.<sup>56</sup> This important concession allowed the group to move forward with viable sharing rules for the 5.25-5.35 GHz band.

Buoyed by the progress made domestically and as the international preparatory work wrapped up in anticipation of WRC-03, the FCC began a new rulemaking on May 15, 2003 to address all aspects of the international work developed up to this point.<sup>57</sup> This review of existing U.S. rules and consideration of new rules for the 5 GHz band was necessary to incorporate agreements and compromises reached both domestically and internationally to establish global rules.

WRC-2003 established a mobile allocation for WAS in the 5.15-5.25 GHz, 5.25-5.35 GHz, and 5.47-5.725 GHz bands and set detect-and-avoid DFS as a requirement for the 5.25-5.35 GHz and 5.47-5.725 GHz bands. WRC-2003 also established power limits and technical requirements for DFS, based on U.S. contributions proposing limits for detection threshold, channel move time, and in-service monitoring. Some disagreement internationally on further operational limits for the 5.25-5.35 GHz band led to the specification of “options” for WAS operation in this band.<sup>58</sup>

On November 18, 2003, the FCC adopted a Report and Order (R&O) that added 255 MHz of spectrum from the 5.47-5.725 GHz band to the Part 15 rules and established rules consistent with the agreements reached domestically between the regulators, industry, and federal agencies.<sup>59</sup> The FCC required the use of DFS and transmitter power control in the 5.25-5.35 GHz and 5.47-5.725 GHz bands, established interim procedures for conformance testing, and gave its Office of Engineering and Technology the authority to develop final conformance test procedures, based on continuing work by the ITAC-R Project Team. These FCC actions were largely consistent with international agreements reached at WRC-03.

### **2.3.3 Development of Adequate Testing Procedures and FCC Decisions Between 2003 and 2006**

Much had been accomplished by the ITAC-R in the preceding period. Through timely exchange of information and active collaboration, the group found consensus on sharing scenarios based on realistic assumptions, and agreement concerning the technical analysis methodology to be employed. The group also completed a rigorous modeling activity, involving the construction and execution of multiple models to validate and verify the accuracy of technical assumptions.

The group next needed to reach agreement about final compliance measurement procedures. These test measurement procedures were vital to ensure that equipment produced would in fact “overlay” existing systems in such a way as to not cause harmful interference. To ensure this result, NTIA performed tests using prototype devices to validate the test procedures under development. This was accomplished in two phases: bench testing against simulated radar signals and field testing against real radar systems, including against military radars at a

---

<sup>56</sup> See ITAC-R Report of Sharing Analysis *supra* note 46 at page 3.

<sup>57</sup> Revision of Parts 2 and 15 of the Commission’s Rules to Permit Unlicensed National Infrastructure (U-NII) Devices in the 5 GHz Band, ET Docket 03-122, Notice of Proposed Rulemaking, 18 FCC Rcd. 11,581 (May 15, 2003).

<sup>58</sup> International Telecommunications Union, Radio Regulations, *Frequency Allocations*, § 5.441, RR5-83 (2004).

<sup>59</sup> See footnote 55.

southwestern desert test range. These activities allowed the regulators to determine the specific test procedures required to ensure that any device authorized under the test procedures would in fact detect and avoid real radar systems.

Two rounds of bench testing in the spring of 2004 led to the discovery that the WAS devices could not employ power threshold detection as the sole means of triggering a channel move.<sup>60</sup> The first bench test was performed on three manufacturers' devices and noted their inability to detect the test radar signals. Federal government representatives concluded that most of the algorithms under development detected only specific, individual radar signals identified in the draft conformance test procedures. Federal government representatives also noted that the WAS devices appeared to employ a radar detection algorithm instead of a power detection mechanism to initiate channel moves for their devices. In a series of meetings held between April and May 2004, parties agreed that a second round of bench testing should be performed to alleviate federal government concerns and to allow industry to use the lessons learned from the first test to change their equipment configurations to more reliably detect test signals. Based on federal government requirements, the second test included randomized test signals that simulated a wide range of radars operated in the 5 GHz bands and required a complete overhaul of the compliance test procedures and development of pass/fail criteria. While industry opposed the randomization requirement, federal officials developed an initial set of randomized test signals.

After an additional round of bench testing conducted between May and June of 2004 confirmed that threshold detection alone could not be used to trigger a channel move, the group collaborated closely to find a solution to this problem. Eventually, a compromise was reached in the ITAC-R process, leading parties to agree that industry could employ algorithms that used features of the radar signals to ensure protection of the federal systems. This agreement led to the development of pass/fail criteria in the compliance measurement procedures for each operational requirement and also led to the use of test signals that randomized key radar signal parameters. WAS devices could detect a very wide range of radar systems (current and potential future systems) in sufficient time to minimize harmful interference. From this important ITAC-R work, final operational values for the applicable radar test signals and pass/fail criteria were developed by the 5 GHz Project Team and ultimately accepted by the FCC.<sup>61</sup>

The ITAC-R Project Team pressed on with its work, generating the required substantial modification of compliance test procedures and development of new pass/fail criteria. These very specialized DFS compliance test procedures extended well beyond the typical procedures required to demonstrate compliance with respect to other existing FCC Part 15 rules. Since the radar signal parameters were randomized, pass/fail criteria were needed to account for the statistical nature of radar signal detection. The ITAC-R Project Team also developed a new set of

---

<sup>60</sup> Up to this point, power threshold detection was intended to trigger a channel move by a WAS device. Two separate procedures were defined. A start-up radar detection procedure was initiated when a WAS device initially powered up. A subsequent in-service radar detection procedure occurred after the initial start-up. Both procedures required a move time, defined as the amount of time acceptable for clearing operations on a particular channel once the radar pulse detection threshold was exceeded, as well as a non-occupancy period to ensure that WAS devices did not prematurely return to channels occupied by radar systems. With this specification, ITAC-R work focused on determining the operational values formally identified as Detection Threshold, Channel Availability Check, Channel Closing Transmission Time, Channel Move Time, and a subsequent minimum Channel Non-Occupancy Period.

<sup>61</sup> See footnote 55.



test signals representing a wide range of radar functions to ensure that DFS detection algorithms and the associated compliance test procedures would protect existing as well as future federal radar users operating in the 5 GHz band.

The ITAC-R worked rapidly between May and June of 2004 to produce a revised compliance test procedure and test plan. Technical representatives from NTIA and DoD developed new test procedures designed to increase their confidence that the WAS devices could avoid interfering with incumbent radar systems. These procedures included pass/fail requirements based on percentages of successful detections. The ITAC-R Project Team meanwhile reached agreement on a new test plan and additional radar test signals with long pulse widths. As a proof of concept, the project team agreed to use these compliance test procedures for baseline bench testing, to be followed by field testing using actual radar signals. In response to industry attempts to remove the long-pulse signal detection requirement, federal officials compromised by delaying final agreement on compliance procedures until both bench and field testing were completed.

In September 2005, NTIA released the baseline bench test report to provide specific test data useful for further ITAC-R discussions.<sup>62</sup> To alleviate continuing industry concerns over the long-pulse width radar signals, DoD agreed to allow industry personnel with the appropriate security clearances to receive a classified briefing on the radar operations to verify federal government requirements. This action by DoD removed a very significant roadblock during this phase of testing. Based on a new understanding of federal government testing requirements, industry agreed to comply with pass/fail criteria for all required signals, including those tests involving long-pulse radar signals.

Despite more than two years of effort by the ITAC-R to support development of WAS service rules for both international and domestic markets, the FCC realized that WAS rules could not be completed as planned by January 2005. On February 23, 2005, the FCC extended the transition period for the 5.25-5.35 GHz band by one year.<sup>63</sup> Without consensus on final conformance test procedures, no devices could be certified under the new rules. The extension period was required to allow devices to continue to be made and sold under the previous rules for the 5.25-5.35 GHz band.

Based on the work performed within the ITAC-R, in December 2005, NTIA completed the field testing that validated the new test procedures. Based on field tests of DoD radar systems, final adjustments were made to the pass/fail criteria. The baseline bench testing and field testing gave federal agencies a higher degree of confidence that incumbent radar systems could be protected. NTIA's field testing demonstrated that the conformance test procedures were valid and capable of producing WAS devices that would protect incumbent radar systems.<sup>64</sup>

---

<sup>62</sup> *ITAC-R DFS Project Team Test Report for 5 GHz U-NII Devices Equipped with Dynamic Frequency Selection With Radar Waveforms*, International Telecommunications Advisory Committee for Radiocommunications, 5 GHz DFS Project Team, Performed by NTIA at the Institute of Telecommunication Sciences Boulder, Colorado in September 2005 (available from the authors).

<sup>63</sup> Revision of Parts 2 and 15 of the Commission's Rules to Permit Unlicensed National Infrastructure (U-NII) devices in the 5 GHz band, ET Docket 03-122, Order, 20 FCC Rcd. 4883 (February 23, 2005).

<sup>64</sup> *Radar/U-NII Device DFS Field Test Results*, International Telecommunications Advisory Committee for Radiocommunications, 5 GHz DFS Project Team, Performed by NTIA at the U.S. Army McGregor Range, Ft. Bliss, Texas from November 28 to December 9, 2005, (December 21, 2005) (available from the authors).

With this common understanding of final compliance measurement procedures, the ITAC-R began work on detailed procedures that would be required by FCC-certified compliance testing facilities. By May 2006, all parties agreed that any industry requests for device certification would contain laboratory results documenting their device's ability to pass compliance measurement requirements established by FCC.

All that remained was for the FCC to finalize its 5 GHz DFS rules and to address petitions for reconsideration raised since its November 2003 decision. In June 2006, the FCC finalized its 5 GHz DFS rules by adopting an Order, dismissing previous petitions, and establishing final compliance measurement procedures in full accordance with the agreements reached by the ITAC-R Project Team.<sup>65</sup>

As is customary with new compliance measurement procedures, FCC gathers the measurements necessary to certify WAS devices. Once the FCC has confidence that the compliance measurement procedures are well understood, they permit Telecommunication Certification Bodies to certify DFS equipped devices. As part of their equipment certification process, the FCC can obtain off-the-shelf samples of the commercially available systems to verify their operational compliance with the rules.

The complex nature of the compliance measurement procedure for DFS equipped devices also led NTIA to establish a program to measure off-the-shelf devices to verify that they comply with the FCC rules. Early tests of several DFS equipped devices revealed minor problems of noncompliance with the FCC rules. NTIA has worked with the FCC and equipment manufacturers to resolve these problems before the devices have been widely deployed. Given the importance of DFS functionality in protecting the military and civilian radar systems, verifying compliance with the FCC rules is a critical factor for successful deployment of 5 GHz U-NII devices.

---

<sup>65</sup> See June 2006 U-NII Device Order, *supra* note 61.

### 3. TECHNICAL REVIEW OF DFS SPECTRUM SHARING TECHNOLOGY DEVELOPMENT

This looks again at DFS historical development, but with a focus on the technical *minutiae* of DFS development. The bifurcation between this section and the preceding section is required by the need to describe both forks of DFS development (i.e., the human narrative versus the technical narrative), and by the length and complexity of both of those forks.

#### 3.1 DFS: Highlights of a Novel Spectrum Sharing Concept

The original technical ideas behind 5 GHz spectrum-sharing U-NII devices were (and still are):

- The basic sharing concept was that U-NII receivers (associated with U-NII transmitters but not necessarily co-located) would detect local, incumbent radar signals and not operate on those locally used radar frequencies. The amount of off-tuning required to protect radar receivers from interference would need to be determined.
- The radar signal power detection threshold would be adjusted so that radar receivers would not see U-NII signal power above a pre-identified, critical interference,  $I$ , to noise,  $N$ , level of  $I/N = -6$  dB in those receivers when the U-NII monitoring circuitry was triggered. This concept of triggering the receiver side of a potentially interfering transmitter to activate frequency avoidance when it sees a critical transmitted power level from a victim system with a susceptible receiver is a clever part of the DFS scheme.<sup>66</sup> A full explanation of how and why it works requires a lengthy technical discussion that is presented in Appendix A of this report.
- Radars, as pre-existing incumbents in the bands, would have primary allocation status over the new spectrum-sharing systems. The new U-NII devices would operate on the same non-interference basis as defined in FCC CFR 47 §15.5 for all Part 15 applications. The U-NII systems would be operated on a not-to-interfere basis with radar systems at 5 GHz, even if existing radars were eventually modified or if entirely new radar systems were developed after the U-NII spectrum-sharing systems were already deployed.
- Radar receivers' *noise-limited performance* (as described further below) would become the *technical limiting factor* for the new spectrum sharing.
- Prior to commencing operation at any location, a U-NII system would verify that no radar signals were present on a candidate U-NII frequency. Subsequently, if a U-NII system using a frequency in the 5 GHz band detected a co-channel local radar signal, all associated U-NII transmitter(s) would be commanded to vacate the local radar frequency; the associated

---

<sup>66</sup> Doing all sensing and triggering with the interfering system inverts what would otherwise be a more straightforward relationship of having a victim receiver sense, and then trigger the response of, the interfering transmitter. This inverted arrangement results from the DFS requirement that incumbent radar systems with victim receivers are not to be modified and that all detection and responses must therefore be generated by the potentially interfering U-NII systems themselves.

receiver(s) would re-tune accordingly. All of these sensing, detection and avoidance operations were to occur in timeframes that would eventually be specified.

In detecting and avoiding the frequencies used locally by radars, the 5 GHz U-NII systems would need to have available, and make use of, alternative frequencies on an *ad hoc* basis. Thus this dynamic approach to detection and interference mitigation by switching to a new frequency when a protected system was sensed would become the newly developed technology of DFS.

### **3.2 Uniqueness of the DFS Concept in Real-World Spectrum Sharing**

The idea of identifying frequencies used locally by one system and then making use of other, unused frequencies in a band (or even in an entirely different band) was not entirely new. SDR system designers had been working with that concept for some years. SDR development work had typically assumed that a single type of service (frequency-channelized communications) would share a band with the same type of service. Within that service, there would be two types of radios: conventional sets that were fixed-tuned by human operators based on pre-existing band assignments<sup>67</sup> and newer SDRs that would find unused interstices in the local frequency assignments and opportunistically make use of those slots. The basic technical problem for an SDR that was trying to enter a band would be to identify and occupy locally unused channels without causing interference to pre-existing radios.

But the idea of developing a fully automated detect-and-avoid functionality for sharing spectrum between communication systems and radars was entirely new. For the first time, automated sharing was being proposed for two different services in a single band. Moreover, one of those services (radar) would continue to function with no change in its operations (no modifications to the radar hardware or software) while the new service would literally work its way into the radar band without producing any harmful interference to the radar receivers.

### **3.3 Technical DFS Developments Starting in 1996**

Development of DFS was an inherently international undertaking. Administrations that had particular interest in the concept and that actively participated in the idea's development included the U.S., the United Kingdom (UK), France and Germany. This was likely due to these administrations having significant pre-existing radar assets to protect in the 5 GHz band that had been proposed for DFS.

---

<sup>67</sup> A note on terminology: *Allocations* specify the *types of systems or services* that are allowed to operate in radio bands. *Assignments* are permissions for *individual radios to use particular frequencies* within designated bands at designated locations. Thus a band allocation may be 162–174 MHz for the land mobile radio (LMR) *service*, while an LMR band assignment is for a *particular radio transmitter* (e.g., for an individual NOAA Weather Radio broadcast station to specifically operate on 162.55 MHz at a designated latitude and longitude within New York City).

### **3.3.1 DFS Introductory Efforts, 1996**

The 5 GHz DFS U-NII development began in the late 1990s with industry proposals to the FCC for authorization of new types of radio devices that would be used for unlicensed wireless data networks, as already described above. The FCC began a rulemaking process that led to the DFS-technology requirement for detection and avoidance of incumbent radar signals by unlicensed wireless devices in designated U-NII bands. (In the ITU-R, WRC-03 would eventually enable a corresponding allocation on a worldwide basis.)

The May 6, 1996 FCC Notice of Proposed Rulemaking (NPRM) for U-NII devices proposed to make available spectrum at 5.15-5.25 GHz and 5.725-5.875 GHz for use by unlicensed NII shared unlicensed personal radio network (SUPERNet) devices for the purpose of short range wireless local area networks (WLANs). Among the proposed rules were:

- 1) a modification to Part 15 of the FCC rules to allow for U-NII device operations in the identified frequency bands;
- 2) a minimum set of technical standards to allow technical flexibility in designs;
- 3) a minimum attenuation of 50 dB by the unlicensed devices for all emissions outside the identified frequency bands or in accordance with 47 CFR 15.209 (whichever is lower);
- 4) no channeling plan, opting instead to allow the industry standards bodies to develop that;
- 5) a “listen before talk” spectrum sharing etiquette; and
- 6) spectrum sharing criteria for incumbent and proposed 5 GHz systems to prevent interference.

The last clause directly related to the later requirement and implementation of DFS.

### **3.3.2 Technical Parameters in the Initial FCC R&O and MO&O, 1997–1998**

The January 9, 1997, FCC R&O on U-NII devices set the allowable band to include 5.15-5.35 GHz and 5.725-5.825 GHz. This document stated some potential conflicts with mobile satellite service (MSS) devices and addressed public concerns from amateur radio and other vendors and agencies that had plans for use of the spectrum allocated for U-NII. There was no mention in this R&O of potential conflicts with radar systems or of a need for DFS.

The June 17, 1998, FCC Memorandum Opinion and Order (MO&O) limited U-NII devices to a peak power of one watt and directional antennas of up to 23 dBi gain. Furthermore, it addressed the original industry petition, accepting some recommendations and rejecting others. Most notably, this MO&O addressed for the first time the potential susceptibility of U-NII devices to high power government radar systems. But it did not address the possibility of interference to radar receivers from U-NII devices. There was still no mention of DFS technology.

### **3.3.3 Technical Parameters from WRC-03 and Recommendation M.1652**

At WRC-03 the U.S. administration actively promoted the allocation proposal for the bands 5250-5350 and 5475-5725 MHz for a new mobile unlicensed service under the condition that the new service had to use a DFS approach to protect radar operations. NTIA, along with the U.S. DoD and industry, developed computer models used in inputs to the Joint Rapporteur Group (JRG) 7-8-9 in Working Party 8B (WP-8B) prior to the WRC, demonstrating that radar operations would be protected under very specific guidelines.

NTIA's Office of Spectrum Management (OSM) and Institute for Telecommunication Sciences (ITS) modeled various types of radar systems, including ground and ship based navigation, and weather and military tactical, to determine the limits on U-NII device emissions that would protect radars. Airborne radar systems were not considered. The model results generally agreed with each other on the U-NII detection thresholds that would protect radar operations. The models considered radars with scanning and rotating antennas. A summary of these studies was included in the Conference Preparatory Meeting (CPM) report.

The United States was successful in obtaining the new allocation under the DFS provision at the conclusion of WRC-03. A new ITU-R Recommendation was also developed that roughly outlined the guidelines, limits, and operating procedures for the U-NII devices. This was ITU-R Recommendation 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*" [2].

ITU-R M.1652 provided:

- Representative 5 GHz radar system characteristics derived from OSM-ITS radar data sets.
- Detection thresholds for radar signals based on OSM-ITS data.
- Requirements for determining channel availability prior to data transmissions based on OSM-ITS data and studies.
- Speed requirements for vacating DFS channels when radar signals are detected.

At this point, no prototype U-NII devices had been tested nor had the DFS approach been proven in any laboratory to reliably detect radar signals and vacate channels.

### **3.3.4 Determination of Technical Protection Criteria, Late 1990s through Mid-2000s**

DFS rules were based on a multi-year fundamental research program by ITS and OSM engineers into the levels at which interference causes radars to lose targets. That NTIA engineering work began in the late 1990s when the DFS concept was first floated, and continued into the mid-2000s. The results of the work were published in a comprehensive technical summary [3]. Significant results included:

- Radar receivers begin to lose desired targets (experience harmful interference) when interference levels are 6 dB *below* the radar's own receiver noise.
- Substantial loss of radar performance (harmful interference) occurs when an interference level is *equal* to the radar receiver noise level.
- Performance degradation (harmful interference) occurs in both radar antenna main-beam and sidelobe coupling; it depends only on coupled interference power, not on direction from the radar antenna (Appendix A).

### **3.4 First Technical Implementation Steps in the U.S., 2003–2004**

With the frequency allocation in place and the domestic rulemaking process started, the domestic rules and procedures for permitting these devices to operate under the CFR were begun. The FCC initiated a rulemaking in 2003 under Docket 03-122 for gathering information on using the bands 5250-5350 and 5475-5725 MHz for U-NII devices.

This process was quite involved and included representatives from NTIA, FCC, DoD and industry having many meetings to review presentations, documents, and filings. Industry was represented by various Fortune 500 companies, but during negotiations acted as one entity.

By the spring of 2004 three companies (Cisco, Motorola, and Atheros) had developed prototype U-NII devices that they submitted to the ITS laboratory in Boulder, Colorado, for initial tests to determine if the devices could detect radar signals and perform the required actions to change their operating frequencies.

The initial set of tests was based on a limited number of radar testing waveforms. ITS engineers spent considerable time and effort to develop the first system that would generate radar signals while also monitoring the U-NII responses to see if they detected the radar signals and vacated the operating channel within the required time intervals. Other test certification laboratories were also involved in the process and offered their comments and guidance on how to develop a DFS-capable U-NII test system.

### **3.5 Certification Testbed Technical Development, 2005–2006**

In 2005–06 bench tests with prototype DFS devices from multiple manufacturers took place at the ITS Laboratories in Boulder, Colorado, followed by field tests against some actual radars at the U.S. Army's McGregor Test Range in New Mexico. These tests included a fully operational air defense radar that tracked commercial air traffic at short and long ranges while interference was injected into its receiver, and further tests in which DFS systems were used to try to detect the presence of this defense radar while it was operating normally. Thus testing began nine years after the initial FCC NPRM for U-NII at 5 GHz, and two years after Recommendation M.1652 [2] described DFS.

The bench tests utilized a laboratory radar transmitter, specially built by ITS engineers, that replicated radar waveforms defined in Recommendation M.1652. Some difficulties with DFS

detection of radar waveforms were encountered in these initial rounds of testing. DFS device performance was better during a second round of testing. The FCC and the U.S. Army participated in both rounds of testing.

ITS engineers also designed and built a system to monitor and record U-NII device responses to the radar pulses. There were at that time no commercial off-the-shelf systems that could perform that function to the degree required by the ITU-R Recommendation and FCC rules.

These initial tests accomplished two goals: they showed that DFS devices could actually detect representative radar waveforms, and they validated a test-and-measurement setup that could be used by the FCC and independent certification labs for certification of DFS devices.<sup>68</sup>

NTIA passed on the DFS certification hardware design and its associated custom-written test-and-measurement software needed for certification testing to the FCC's Columbia, Maryland, laboratory in 2005-06. The FCC then began to actually test and certify the U-NII devices. ITS did not perform that function, but it did buy some devices off-the-shelf and tested them independently. ITS test results were presented to federal agencies and the FCC.<sup>69</sup>

### 3.6 Technical Certification Requirements Development, 2005–2006

DFS rules for the U.S. were codified in CFR 47, Part 15.407.<sup>70</sup> These included:

- *Power-on Test*: Verify that the device monitors the initial channel for one minute after it completes the power-on cycle and that it does not transmit during that time.
- *Initial Detection Tests*: The device must detect a radar signal within the first six seconds and last six seconds of the initial channel check and not transmit.
- *In-Service Monitoring Test*: This is the most comprehensive test, in which DFS U-NII devices must detect six different waveform categories *representative* of six *types* of radars operating in 5 GHz bands. *Operational radar waveforms are not exactly replicated.* Hundreds of radar-detection trials are run for the certification of each device.
- *30 Minute Non-Occupancy Test*: When a previously used DFS channel has been occupied by a radar signal, the U-NII device must be verified as not attempting to use it again for at least the next 30 minutes.

Table 1 summarizes the DFS technical protocols as finally implemented.

---

<sup>68</sup> As a federal research and development laboratory, ITS does not perform routine certification testing. Instead, it develops certification testing approaches and systems and then transfers them to other agencies and to industry.

<sup>69</sup> The FCC has a similar process, but does not buy devices off-the-shelf. Instead, it requests that manufacturers provide devices for testing. ITS's process ensures that devices being tested are the same as devices being bought by consumers.

<sup>70</sup> <https://www.gpo.gov/fdsys/pkg/CFR-2004-title47-vol1/pdf/CFR-2004-title47-vol1-sec15-407.pdf>.



Table 1. DFS Technical Protocol Summary

DFS Technical Parameter	DFS Requirement
Radar Signal Detection Threshold in DFS receivers	-62 or -64 dBm in 1 MHz bandwidth <sup>71</sup>
Channel availability-check interval before any channel can be used	60 seconds
Channel non-occupancy period after radar detection	30 minutes
Maximum interval allowed for channel move after radar detection	10 seconds
Maximum intervals allowed for housekeeping transmissions during a channel move	200 milliseconds plus approximately 60 milliseconds over the remaining 10 second period

### 3.7 DFS Compliance Testbed Constructed at ITS, 2005–2006

The DFS compliance testbed that ITS and OSM engineers developed and built at the ITS Boulder laboratory between 2005 and 2006 included these features:

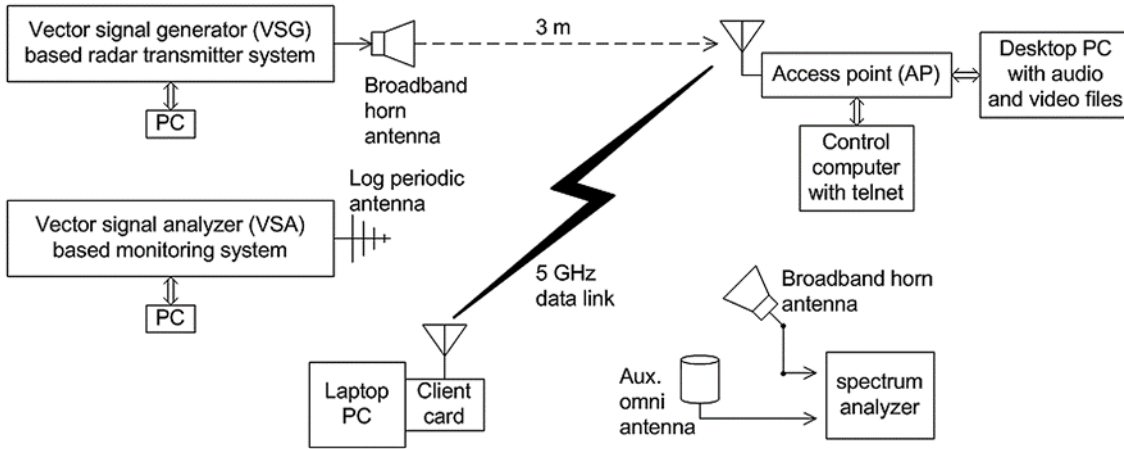
- A radar signal generator (itself a complicated undertaking) and RF signal synthesizer.
- Capability to produce bursts of un-modulated, frequency modulated (“chirped”), and frequency-hopping pulses in all 5 GHz DFS bands.
- Variable and user selectable capability for RF frequencies, number of pulses per test-burst, pulse width, pulse repetition interval (pri) and chirp bandwidth.
- Power control of RF radar pulses.
- Use of a programmable vector signal generator (VSG) for pulse production.
- A radar pulse timing measurement system.
- Monitoring capability for RF activity on U-NII channels.
- Use of a vector signal analyzer (VSA) and spectrum analyzer for fine and coarse measurement of the RF emissions of U-NII AP and client transmissions over 12 seconds.
- Development of a customized MATLAB® routine for analysis of all collected data.
- Implementation of two systems that are synchronized so that a press of a button starts an in-service test and collects data for 12 or 24 seconds.
- For in-service tests, a Moving Picture Experts Group (MPEG) formatted file was streamed from one computer to another using a DFS AP and client to load the RF channel. Then and

---

<sup>71</sup> Depending on whether the U-NII transmitter power exceeds 200 milliwatts. See Appendix A.

now, APs in the U.S. *must* have DFS functions built-in, with radar detection capabilities being optional for clients. European rules are different.<sup>72</sup>

The performance testing system that was developed by NTIA is shown in Figure 1.



Figure

1

Figure 1. DFS performance-testing system developed by NTIA and transferred to FCC.

The certification hardware and software were transferred from NTIA to the FCC by 2006. Overall this development effort required several engineer-years of effort; the timeline for the effort was over a year.

### 3.8 Early DFS Testing at the ITS Boulder Laboratory and Testing Transition to the FCC, 2005–2006

Starting in August 2005 NTIA engineers began testing prototype DFS devices that were provided by industry. These tests used an early version of the DFS testbed and test methods developed by ITS. The tests helped NTIA to better develop the testbed and helped industry by providing feed-back on how well the early DFS devices functioned against simulated radar pulses. An example of an early DFS test output is shown in Figure 2.

In this figure, measured received power in the testbed is shown as a function of elapsed time. At 0.75 seconds (elapsed time from an arbitrary starting point), a wireless AP transmits a data burst. At 0.83 seconds the AP transmits a second data burst. At a randomized time of 0.82 seconds elapsed, at the end of the second AP data burst, the testbed fired a burst of radar pulses. The pulses partially overlapped the very end of the second AP data burst. Subsequent to the radar pulse burst, the AP halted its ordinary data bursts. Instead, it transitioned to sending a set of four beacon packets. The packets alerted the AP's clients that they would have to stop operating on

<sup>72</sup> MPEG files have now been replaced by a channel loader/emulator in the testing process. This allows precise control of how much data is sent over a link during testing. In 2003 such devices were costly. The FCC wanted to keep costs lower and not require testing companies to unnecessarily procure costly equipment. Using MPEG files to load each communication system's RF channel during streaming from an AP to a client was a compromise.

the current frequency and transition to a different frequency. At 1.25 seconds the last of the beacon transmissions occurred.

The AP then went silent on the previously used frequency. After the radar burst concluded, the MATLAB<sup>®</sup> program would then read the total “on” time of the RF pulses as the VSA digitized and stored the RF activity on the channel over the 12 seconds. That total on-time was then compared to the standard. This kind of test verified that subject U-NII systems were correctly implementing DFS detect-and-avoid technology, vacating the channel with the time allotted and not exceeding the allowed “on” time within that time period. These types of tests and measurements had never previously been done by any test house or company.

In the 2005-06 period, NTIA transferred its knowledge of DFS certification testing techniques to the FCC. NTIA and the FCC worked jointly to establish a DFS certification testbed at the FCC’s laboratory at Columbia, Maryland. The transfer involved acquisition by the FCC of dedicated testing equipment, including a VSA and a VSG (see Figure 1), and transfer from NTIA to FCC of custom-written testing software.

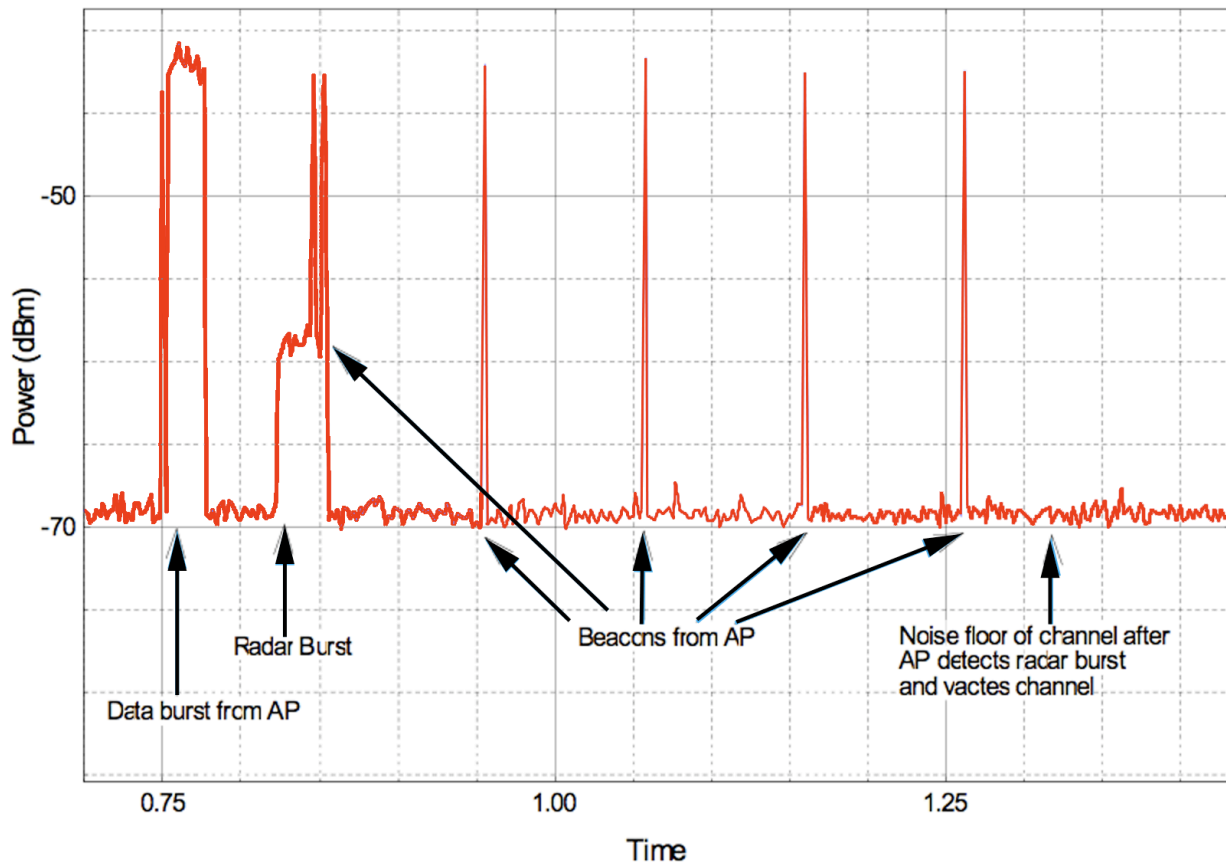


Figure 2. Early DFS radar-pulse detection result with a prototype DFS U-NII provided by industry, circa 2005. Time is in seconds.

### 3.9 Initial DFS Deployment Experience and TDWR Interference, 2006–2009

DFS-enabled U-NII devices were available to consumers by July 2006, three years after WRC-03 and 10 years after initial FCC R&O for U-NII. A wide variety of DFS-enabled 5 GHz U-NII devices were soon certified by the FCC and were sold by several manufacturers. Both frame-based and 802.11 devices were marketed; other types were certified including low data-rate and hand-held devices. The devices were primarily marketed to WISPs for use as radio backhaul links between remote locations and central stations with wireline connections to the Internet.

NTIA later undertook random off-the-shelf spot-checks of commercially available products to verify their DFS performance. In 2008, a certified product was found by NTIA and FCC to not be detecting radar signals; post-certification changes to the device's firmware were the cause. The changes were not supposed to disable DFS, but did. Ongoing NTIA and FCC spot-checks identified additional issues with some FCC certified devices.

In early 2009 the FAA reported interference to its 5 GHz microburst-warning TDWRs. The interference was found to be caused by DFS-capable 5 GHz U-NII transmitters, as described at length in Section 7. Major interference areas included the San Juan area in Puerto Rico and the area around New York City.

Subsequent studies conducted by NTIA, FAA, and FCC, with assistance and cooperation from industry, identified cases in which some devices did not adequately detect TDWR radar signals in the field, even though they had passed DFS type-certification tests. One cause was U-NII DFS software that allowed operators to change their units' software-assigned country code from USA to other administrations (e.g., Brazil). Operators who did this disabled DFS functionality, as most countries did not have DFS rules. The devices, unhindered by DFS software operation, would then operate across local radar frequencies and cause interference to local radars. These included the safety-of-life-mission TDWR.<sup>73</sup> Additional factors also played a role, including radar testing waveforms that were not sufficiently robust to ensure detection of radar signals at field locations by devices that had nevertheless performed adequately in lab testing. These factors are discussed in greater detail in Section 7.

### 3.10 Brief Summary of Ongoing DFS Deployment, 2010 to 2015

Government and industry worked together to improve certification-testing parameters to resolve these problems. Notable results included development and implementation of more robust DFS testing protocols and elimination of the user-accessible country code option in DFS software. On July 27, 2010, the FCC issued a Memorandum, "*Elimination of Interference to Terminal Doppler Weather Radar (TDWR)*" from the FCC Office of Engineering Technology (OET) and the Enforcement Division. The memorandum summarized information about 5 GHz U-NII interference to TDWR receivers. Its contents were based on multi-agency inputs including previous OSM-ITS troubleshooting results with these systems. The memo encouraged WISPs to

---

<sup>73</sup> TDWRs are one of a number of tools that detect potentially deadly microbursts at airports and route air traffic around them. A major original impetus for microburst-warning technology development was the August 1985 crash, with 137 fatalities, of Delta Flight 191 while attempting to land through a microburst at the Dallas Ft. Worth airport.

use good practices in the deployment and use of DFS-enabled U-NII systems, including an on-line database developed by government and industry to better coordinate the use of DFS-capable U-NIIs in areas near TDWR installations.

However, an ongoing problem with DFS U-NIIs is that some authorized<sup>74</sup> firmware updates have caused unintentional failures in DFS functionality. Since DFS U-NIIs do not undergo re-testing after initial FCC certification, it is possible for firmware updates that are sent to FCC-certificated devices to accidentally (that is, unintentionally) disable those devices' DFS operations. Devices that receive such updates may begin to cause interference to TDWR receivers even though they have had a long previous track record of interference-free operation. What to do about this problem remains an open question.

In 2013, the Commission issued the Notice of Proposed Rule Making with the goal of supporting the growing needs of businesses and consumers for fixed and mobile broadband communications using U-NII devices in the 5.15-5.35 GHz and 5.47-5.850 GHz bands.<sup>75</sup> At the same time, it recognized the need to modify its rules to better ensure that these devices do not cause harmful interference to authorized federal and non-federal users in these bands.<sup>76</sup>

As a result of the 2013 NPRM, the FCC issued a Report and Order<sup>77</sup> that increased the utility of the 5 GHz band where U-NII devices are currently permitted to operate, and modified certain U-NII rules and testing procedures to ensure that U-NII devices do not cause harmful interference to authorized users of these bands. Specifically:

- The FCC removed the indoor-only restriction for U-NII devices in the 5.15-5.25 GHz band and increased the permitted power, thus increasing the utility of spectrum and accommodating the next generation of Wi-Fi technology.
- The FCC extended the upper edge of the 5.725-5.825 GHz band to 5.85 GHz and consolidated the Part 15 rules applicable to all digitally modulated devices operating across this 125 megahertz of spectrum to ensure that all such devices comply with U-NII requirements intended to protect authorized users from harmful interference.

---

<sup>74</sup> Some unauthorized firmware files have been provided by third parties to intentionally make devices that are FCC compliant operate in an unauthorized manner.

<sup>75</sup> See, Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, Notice of Proposed Rule Making, ET Docket No. 13-49, 28 FCC Rcd. 1749, (2013) (NPRM); 47 CFR Part 15 Subpart E—Unlicensed National Information Infrastructure Devices. This First Report & Order does not address the use of U-NII devices into the 5.35-5.47 GHz and 5.85-5.925 GHz bands, pending additional technical analyses of those bands. See NPRM at paras. 75-112. These bands are the subject of further study and will be addressed in a separate future order. See also Department of Commerce, "Evaluation of the 5350-5470 MHz and 5850-5925 MHz Bands Pursuant to Section 6406(b) of the Middle Class Tax Relief and Job Creation Act of 2012," available at [http://www.ntia.doc.gov/files/ntia/publications/ntia\\_5\\_ghz\\_report\\_01-25-2013.pdf](http://www.ntia.doc.gov/files/ntia/publications/ntia_5_ghz_report_01-25-2013.pdf). A copy of this report has been placed in the Docket of this proceeding.

<sup>76</sup> See 47 CFR § 15.403(s).

<sup>77</sup> Report and Order in ET Docket 13-49, 29 FCC Rcd 4127 (5), *Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band* (April 1, 2014), <https://www.fcc.gov/document/5-ghz-u-nii-ro>.

- The FCC required that all U-NII device software be secured to prevent its modification to ensure that the devices will operate as authorized by the Commission, thus reducing the potential for harmful interference to authorized users.
- The FCC further protected TDWR systems and other radar systems operating in the 5.250-5.350 GHz and 5.470-5.725 GHz bands from harmful interference by modifying certain technical rules and compliance measurement procedures for U-NII devices operating in these bands. For example, the measurement procedure to demonstrate compliance to the applicable out-of-band and spurious emissions limits was modified to require the use of a positive peak detector with maximum hold instead of an RMS power averaging detector with trace averaging, effectively making the limit approximately 10 dB more conservative.

### 3.11 CSMAC Impetus for this Report, 2015

In 2015 the Commerce Spectrum Management Advisory Committee (CSMAC) recommended that NTIA consider a study of potential mechanisms that could lead to the more effective policing of the radio spectrum. In response to the CSMAC recommendation NTIA's OSM has performed this case study on harmful interference to TDWR caused by DFS-enabled 5 GHz U-NIIs. Examining the historical and technical aspects of the development and deployment of 5 GHz DFS, this study describes the strengths and weaknesses of DFS related to the major government systems, TDWR, which share the spectrum with DFS-enabled U-NII devices in the 5 GHz part of the spectrum. This narrative summarizes the DFS experience and shares lessons learned that may be applied to, and perhaps may be used to modify, similar spectrum-sharing approaches in other spectrum bands, with other radio systems, in the future.

Looking back on the history of DFS design, development, and deployment (Section 2 and this section) brings us to the first Lesson Learned from the DFS experience:

**Lesson 1:** The development time for dynamic spectrum sharing technologies, even when government and industry work closely and cooperatively together on the necessary technical and regulatory framework, can be something on the order of a decade. This is because innovation requires considerable advance work in the absence of existing implementations. The more innovative and technically challenging the new sharing scheme, the longer the advance-work timeline can be expected to be.

## 4. DFS PRINCIPLES AND IMPLEMENTATION

### 4.1 The Basic DFS Concept

This section describes the technical details of DFS. DFS is an integrated, on-board detect-and-avoid system for protection of radar receivers from harmful interference from 5 GHz U-NII transmitters that would otherwise operate on those radars' frequencies.<sup>78</sup> DFS is meant to run completely autonomously, having no interactions with nor inputs from human operators. When DFS functions properly, it should be nearly invisible to operators; radars do not receive harmful interference and U-NII devices use non-conflicting frequencies that have been self-selected by the U-NII DFS control system to avoid the radar frequencies. U-NII operators may, however, notice a halt in data flow if their system attempts to change channels to a new one that still must use DFS, as the one-minute non-transmit initial channel check is mandatory. If the new channel is in a non-DFS band, they should not see such an interruption. DFS equipped U-NII devices may also “look ahead” while they are operating on their current channel and be prepared to switch to a new channel, as long as that channel has already been checked for radar activity.

#### 4.1.1 DFS Architecture Within U-NII Systems

U-NII devices at 5 GHz are primarily used by WISPs to route backhaul traffic from remote locations to central stations that have wireline Internet connections. As such, a typical U-NII network consists of a single controller station, called an AP, which communicates with one or more remote-location stations called clients. The network topology is a star configuration with the AP at the center of the network, as shown in Figure 3.

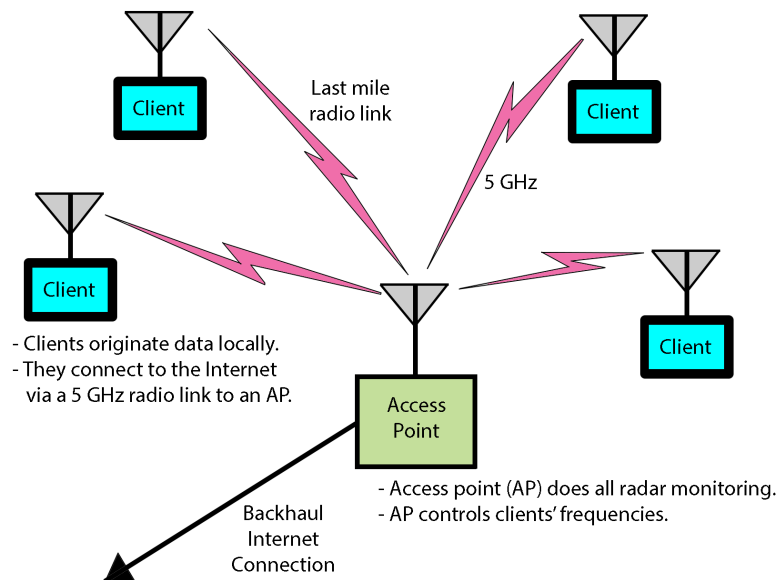


Figure 3. Typical 5 GHz DFS-equipped U-NII network as usually deployed by WISPs.

<sup>78</sup> More broadly, DFS types of approaches can be used to protect other receiver systems in other bands from other transmitters.

Early in DFS development it became apparent that practical and affordable U-NII networks could not be expected to incorporate radar-sensing technology in their nominally low-cost client units. The alternative, which has been implemented in every system of which the authors are aware, is to implement radar-sensing technology only in the AP units. Since the AP units perform all command and control functions for clients, the implementation of radar-sensing capabilities in these units alone also makes sense from a network-operations standpoint. Figure 4 flowcharts the DFS algorithm. In some non-U.S. administrations, clients must also have DFS functionality.

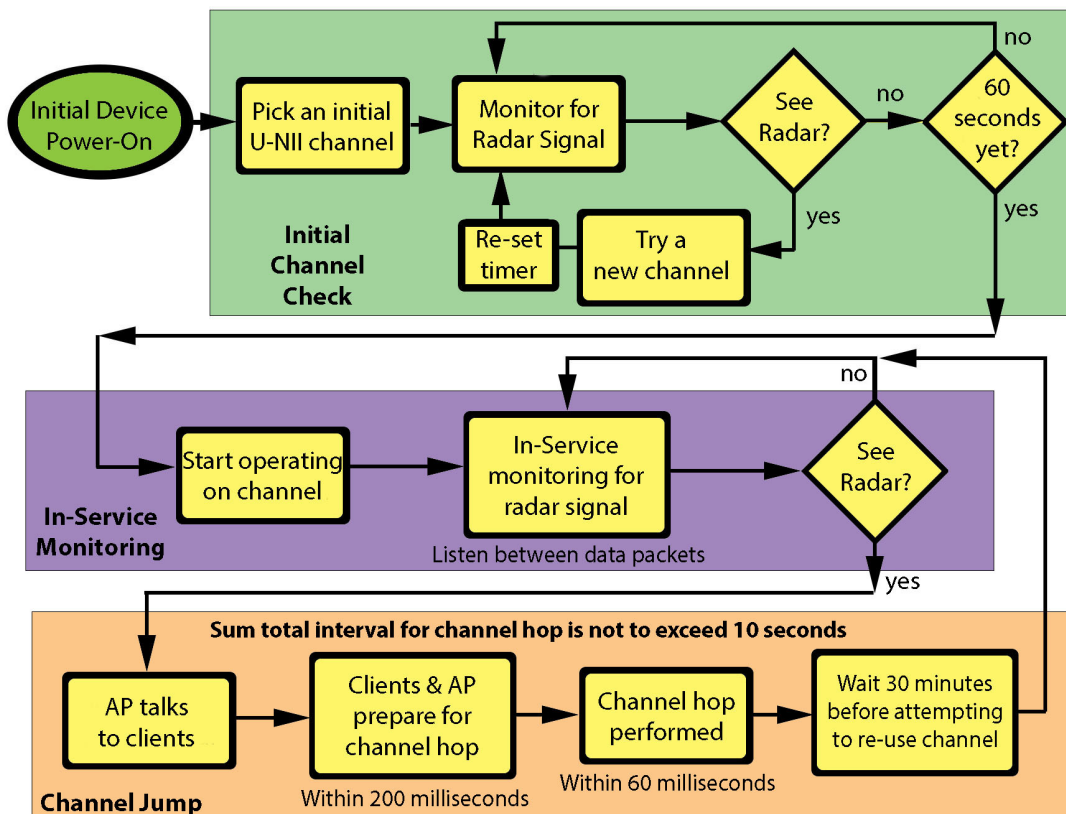


Figure 4. DFS algorithm flowchart.

The algorithm begins when the U-NII network is activated. The first network device that activates is the AP. Clients are to remain silent while the AP, before commencing any radio transmission, operates a completely radio-quiet *initial channel check* in which it monitors for any local radar signals. Radar signal detection is specified to occur at or above a pre-set threshold of -62 or -64 dBm per megahertz<sup>79</sup> in an AP receiver circuit via an isotropic AP antenna gain, as defined in the Commission's rules. This monitoring is performed on whatever band channel the AP is about to try to use between itself and its clients. The initial channel check runs for a fixed-length monitoring period (the initial channel-check interval) which is defined in the FCC rules to be not less than 60 seconds.

<sup>79</sup> Depending on U-NII transmitter power. See Appendix A.



If the initial channel check is negative for detectable radar activity after 60 seconds, the AP commences communications with its clients and the network goes into normal backhaul operation. If the initial channel check reveals a detectable radar signal, then another channel is selected as a candidate for operations and the initial channel check monitoring begins anew on that channel. This cycle continues until a usable channel (one not occupied by a radar) is found.

Once regular U-NII network operations have begun, the AP must continue to monitor for new radar signals that may appear. This *in-service monitoring* is effectively continuous, although in reality monitoring can only be performed during numerous time slices between other network data packet operations. (A key part of U-NII device testing is verification that AP monitoring is effective even when reasonably heavy data rates are being sustained by the network.)

During in-service monitoring the AP uses manufacturer-developed algorithms to search for radar signals at the detection threshold. If a radar signal is detected during in-service monitoring, then the AP immediately commences communications with its clients in preparation for a simultaneous channel-change by the entire network. All such communications must be accomplished within a 10 second *channel change interval*, the channel change itself occurring by the end of that interval. Moreover, during the 10 second interval the total amount of time that the system spends in sending data is not to initially exceed 200 milliseconds, with an additional 60 milliseconds allowed over the remainder of the 10 second period.

After a channel has been vacated due to radar signal detection, the AP is not to attempt to re-use the channel for a specified interval. This *non-occupancy interval* following radar detection and channel evacuation is specified as 30 minutes. The AP must still do a one minute channel check after the 30 minutes have elapsed before attempting to re-use the same DFS-band channel.

Ultimately, many DFS-enabled 5 GHz U-NII devices have been successfully designed, developed, tested, sold, and operated in the U.S. While the principles are straightforward, actual design and implementation of operational DFS capabilities are complex and have been fraught with a number of technical difficulties. Difficulties begin with some inherent problems in the basic concepts behind DFS. These are described below.

#### **4.1.2 DFS Parameter Space: Note on Frequency-Shift (Channel-Move) Protocols**

At the beginning of the DFS design and development cycle, one aspect of the new technology was especially difficult to address because DFS devices would not be built until protocols and requirements had been developed, but some protocols and requirements could not be adequately designed unless working DFS devices were available. Chief among these was the problem of *how much* frequency separation would be required of a DFS device when it detected a radar. That is, when a channel hop was to be performed, how large did the frequency change need to be? That question was not ultimately addressed until DFS devices had been deployed and had been operating for a number of years [4].

### **4.2 Theoretical Difficulties with DFS**

DFS is based on several technical assumptions. These are:

- Radar signals can be detected at given thresholds in the presence of background U-NII traffic.
- Detection of radar signals by a single AP in a U-NII network can provide adequate protection of radars from the transmissions of the entire network, including the transmissions from the AP's remotely located client units.
- An AP can use a radar-detection threshold that is sensitive enough to ensure that radar receivers will be protected when their associated radar transmitter emissions are detected by the APs at those thresholds.
- A sufficiently large and robust set of radar testing waveforms (called bins) can be devised to ensure that if a U-NII system passes DFS testing with those radar bins in a laboratory, then the system detection of radar waveforms in the field will be robust enough to adequately protect radar receivers from harmful interference.
- Firmware updates sent to DFS-equipped U-NIIs after the U-NIIs have undergone initial FCC DFS-certification testing will not accidentally corrupt or deactivate those systems' DFS functionality. This is despite the fact that DFS systems do not need to be re-certified after such firmware updates have been developed and distributed to WISP customers.<sup>80</sup>
- DFS-equipped U-NIIs will always be properly installed and operated by operators.

One last assumption is so subtle that the originators of the DFS concept never recognized it as such when DFS was proposed:

- Introduction of DFS technology into a band that had previously been allocated for radar-exclusive use will not encourage the *illegal introduction* of non-DFS equipped devices into that same band.

As with any system based on assumptions, there are limits to the conditions under which these assumptions hold true. The assumptions and their limits are examined here.

#### **4.2.1 Assumption: Radars Can Be Detected While U-NII Message Traffic is Running**

Monitoring for radar signals by a U-NII AP only during selected time intervals between regular message packets reduces the total probability per unit time that a radar signal will be detected, as compared to uninterrupted monitoring. If the probability of detection per unit time is greater than zero, however, then any radar signal will eventually be detected. The question becomes how long that detection interval is likely to be. This problem is addressed for 5 GHz U-NIIs by testing each new model hundreds of times for each certification radar bin while message traffic is running. The U-NIIs must pass each test with certain scores for individual radar bins and another score for composite detection performance across all radar bins. Those test results provide some

---

<sup>80</sup> The FCC does not track software updates of DFS-certified devices. It can be difficult to compare existing, current software in DFS-equipped devices with the software versions that were implemented in the AP articles that originally received DFS certification.

confidence that field-deployed DFS units will eventually, and adequately, detect ambient radar signals.

#### **4.2.2 Assumption: Detection of Radar Signals by APs Protects Radars from All Network Transmissions**

This assumption is only true to the extent that clients and APs have equally good, or at least nearly comparable, signal propagation paths to local radars. For airborne radars this assumption is probably quite good. For terrestrial radars such as TDWR, this assumption will not necessarily always be true. The assumption would fail in situations where propagation between a TDWR and an AP would be so poor that the radar signal did not exceed the AP's detection threshold, but one of the AP's client units conversely had propagation to the radar sufficient to cause interference to the radar. While the authors are not aware that this sort of situation has actually occurred, it remains an open possibility that results from the compromise DFS solution of only putting monitoring functions into AP units.

#### **4.2.3 Assumption: Radar-Detection Thresholds are Adequate to Protect Radars from Harmful Interference**

The problem of determining adequate radar detection thresholds to ensure protection of radar receivers from U-NII transmissions is central to the entire DFS concept. The heart of the assumption is this: *A particular received power level from a radar transmitter at a DFS AP monitoring location can be equated to a known (accurately predictable) power level in the radar's receiver circuitry.* To arrive at this detection threshold, the following calculation must be performed: First determine the power level in the radar receiver where the radar target-detection probability begins to degrade from a nominal baseline condition. For radars that ITS and OSM engineers at NTIA examined [3], this power level turned out to consistently be 6 dB *lower* than the radar receiver internal thermal noise levels; in other words, an interference-to-noise level, *I/N*, of -6 dB in the radar receivers.

The next step was subtle: Working under the assumption that signals propagate equally well in both directions between the radar and the U-NII (that is, that the radar transmitter power going outbound toward the U-NII AP monitor propagates equally well to the power coming inbound from the U-NII transmitters to the radar receiver), calculate the power level arriving *from the radar at the AP monitor* that equates to the condition that the U-NII *signals are arriving at the I/N = -6 dB power level* in the radar receiver. For 5 GHz radars with characteristics of those published in ITU-R Recommendation M.1652, this power level was determined to be -64 dBm as received with an isotropic-gain AP antenna.<sup>81</sup>

Obviously the adequacy of the detection-threshold condition is based on a number of individual assumptions. None of those assumptions is necessarily always true at all times and places, but all of them are probably true most of the time under most conditions. In other words, this condition

---

<sup>81</sup> It has been agreed that clients will do no monitoring. The entire scheme depends on detection by the APs.

is supposed to good enough to provide adequate but admittedly less-than-perfect protection of radar receivers from harmful interference.

#### **4.2.4 Assumption: Radar Waveform Testing is Sufficiently Robust**

It might be thought that the key to adequately robust radar waveform testing of DFS systems would be to exactly replicate the radar signals that currently occur in the shared spectrum band, and to test against those. This is not an especially good test. There are a number of reasons for this. First, DFS is supposed to be a *general* spectrum sharing solution that will work with *any* radar signals that might occur in the band, both those from known radars at present and those that may occur in the future or that may occur from radars that were not thought to be in the band at the time of testing.

Second, due to national security classification issues, there are radar signals in the 5 GHz band for which the government will not share exact emission parameters. With these factors in mind, radar test-bin waveforms must *not* exactly replicate any one type of 5 GHz radar. Rather, the five bins that have been developed are intended to have parameters of pulse width and repetition rate that *span the pulse-parameter range* of existing and expected future radars in the band. This approach ensures that DFS design engineers do not hard-code single radar pulse types into their detection algorithms, and thus that they keep their DFS algorithms generally applicable to any radar signals that might occur in the band. At the same time, the confidentiality of the government radars' pulse parameters is preserved.

However, this is not to say that NTIA and FCC would not modify the test waveform rules if they deemed it was required to protect new radar systems. The U-NII industry would be notified in advance if such changes were required. Industry would not be blindly given a new waveform to detect without some initial time period to modify their detection algorithms to accommodate such a waveform.

Time delays would be expected for new waveform introductions, associated with manufacturers needing to prepare and test new firmware. All users would need to be prompted to implement the new firmware when made available. Consequently there could be long periods where interference might continue while new firmware was being prepared.

It was discovered after initial DFS-equipped 5 GHz U-NIIs were deployed that some U-NIIs were not detecting all radar signals in the shared 5 GHz band. Part of the reason turned out to be insufficiently designed radar test-bin waveforms. Those waveforms were eventually expanded to make them robust enough to ensure that tests conducted with them would ensure adequate DFS field performance.

This experience with radar test-bin waveforms raises an important point: *Any non-trivial spectrum sharing scheme can be expected to be imperfect. Imperfections will especially tend to cause interference when the initial sharing units are field-deployed.* Thus spectrum managers and engineers should plan in advance of field deployments to expend time and budgets on sorting out and resolving interference problems that are likely to occur with initial deployments. The *causes* of the failures will not be known in advance (or else they would otherwise be fixed in

advance), but the fact that failures *are likely to occur due to unanticipated problems* with the sharing technology can be expected to be highly likely.

#### **4.2.5 Assumption: Firmware Updates Installed in DFS Units After Initial Certification Will Not Cause DFS to be Impaired or Disabled**

As noted above, DFS-equipped 5 GHz U-NIIs are not re-certified after a given model has passed its DFS testing and has received an FCC approval for operation unless major changes are made to its design, such as changing an amplifier or antenna. (An FCC sticker is placed on each production unit and is visible to purchasers; the stickers are visible proof of certification.)

Firmware changes generally do not require re-certification tests, so it is quite possible for consumers to procure devices with firmware updates that have not been re-tested for DFS certification. Subsequent to certification and approval of their units for sale, U-NII manufacturers tend to provide frequent firmware upgrades for their units. These upgrades are developed by the manufacturer's design engineers and are then downloaded to units that have already been purchased and deployed at field locations. It has been deemed to be neither practical nor necessary to re-certify every U-NII model for DFS performance after each new firmware upgrade throughout the subsequent operational history of the units. (It has been estimated informally by manufacturers that their DFS-equipped U-NIIs have about a 10-year half-life after they are purchased. The more expensive the units, the longer their deployment lifetimes can be expected to be.)

FCC lab tests do not generally enter lower sub-menu operations of devices where commands such as "turn DFS off" are possibly available. Nor would the FCC set a device to a non-U.S. country code that might disable DFS. ITS engineers, with direction from OSM, dug deeper into AP control menus to investigate such possibilities with devices that were bought off-the-shelf. When such problems have been found they have been reported to the FCC, and the FCC has contacted the manufacturers. ITS has neither time nor funding to perform more than a handful of such tests per year.<sup>82</sup>

This approach makes good sense from the standpoints of cost and practicality, as DFS performance testing is costly and time-consuming. But a problem with this approach is that it is possible for the DFS performance of certified U-NII models to be accidentally impaired or disabled by firmware engineers when they modify the firmware. Since those engineers do not normally have access to DFS testbeds of their own (such testbeds being costly and complicated, as described above), they have no way to *ensure* that any of their code changes have definitely *not* accidentally impaired or disabled DFS functionality.

NTIA and the FCC discovered and documented some cases where unintentional impairment has in fact happened due to firmware changes. No *ante rem* solution currently exists for this problem. The only way to be certain that a code change has not corrupted DFS functionality

---

<sup>82</sup> The authors have personally seen social media message boards informing users of ways to "stop DFS;" various websites and message boards have at times had discussions about DFS and how to disable or deactivate it.

seems to be to deploy the new firmware and then wait to see whether its introduction results in interference to radar receivers.

#### **4.2.6 Assumption: DFS-Equipped U-NIIs will be Properly Installed and Operated**

We have found this assumption to be imperfect. The FCC specifies that 5 GHz DFS-equipped U-NIIs are supposed to be installed by persons who are “professional.” Those installers are supposed to understand what DFS is, and that impairment or disablement of DFS functionality can imperil safety-of-life radar operations. They are supposed to follow FCC rules and regulations. The FCC does not however actually “license” U-NII installers. Things that installers are *not* supposed to do include intentional disablement or circumvention of DFS functionality and use of any antennas for the U-NIIs other than the ones provided by the manufacturers, with which the devices were originally tested and certified. In reality there have been numerous cases in which DFS protocols have been violated by U-NII installers or operators. This was especially true during the earliest period of initial deployment, but still happens occasionally to this day.

One feature that installers and operators violated with some regularity early-on was the prohibition against disabling the DFS software and firmware functionality of their units. In the early days of deployment, manufacturers sold their units with software that included user-selectable “country codes.” The operators were supposed to truthfully select the U-NII’s country of operation from a drop-down menu. These individual country codes allowed manufacturers to tailor their software and firmware operations to whatever country a U-NII was operating in, without needing to sell different versions of their devices on a country-by-country basis. For the U.S., this of course meant that DFS functionality would be activated when “USA” was selected from the installation menu.

Word quickly spread among operators who were using 5 GHz DFS-equipped U-NIIs that they could “improve” the performance of their devices by *not* selecting “USA” as the country code and selecting another country such as “Brazil” instead. With DFS thereby disabled, the 60-second initial channel-check disappeared. Additionally, the units would never try to switch from one channel to another during their in-service phase since they would of course never detect any radars. When this became common knowledge, the FCC notified U-NII manufactures that for devices sold in the U.S., the country code must be fixed to USA; AP control menus were to lock out this option in the U.S.

Another temptation that proved too much for some network and WISP operators was to substitute their own antennas (typically high-gain parabolic dishes) for the lower-gain patch-style antennas that were supplied with the units by the manufacturers and which met the legal not-to-exceed-23-dBi-gain requirement. Using higher gain but narrower beam-width antennas allowed them to reach customers at greater distances in places such as canyons and mountaintops, but FCC rules prohibit the use of antennas other than those used when devices are DFS-certified.

We note that the issues associated with less-than-professional installation practices mostly occurred early in the DFS roll-out. Once the interference problems emerged, the DFS industry became much more familiar with the issues and expectations associated with opportunistic spectrum access. As a result, the FCC suspended new certifications over nearly a three-year

period as the issues contributing to interference were being investigated, and the industry began self-policing their own installation practices.

#### **4.2.7 Assumption: Introduction of DFS to a Previously Unshared Band Will Not Encourage Illegal Introduction of Non-DFS-Equipped Devices Into the Band**

As noted above, the idea that introducing a band-sharing technology into a band that had previously had no sharing might encourage the introduction of new, *wholly illegal* devices into the same band was simply not anticipated by the creators of the DFS concept. But this may be what have happened.

Reviewing briefly, the band 5250–5925 MHz is allocated in the U.S. administration for various radar operations. As authorized by the U.S. administration following the adoption of ITU-R Recommendation M.1652 [2] at WRC-03, only two sub-bands within that range are authorized by the FCC for spectrum sharing between U-NIIs and radars, and strictly on the condition that those U-NIIs are DFS-equipped: 5250–5350 MHz and 5470–5725 MHz. Outside these two DFS-required sub-bands, intentional radiators are allowed to operate under those regulations specified in Subpart E of the Part 15 rules that do not require DFS capability.

In practice, however, some operators of 5 GHz Part 15 devices have *illegally* tuned their transmitters *out* of their allowed 5 GHz Part 15 bands and *into* the 5 GHz DFS-required U-NII bands. Having no DFS functionality, these illegally re-tuned Part 15 devices have caused interference to safety-of-life TDWR receivers.

A related problem has been that some people have imported illegal 5 GHz transmitters from abroad (primarily from Europe and China) and have operated them in 5 GHz DFS bands in the U.S., causing interference to TDWR receivers. These illegal transmitters have lacked any spectrum authorization for legal use in the U.S. That is, they are intentional radio radiators that lack any FCC authorization. As discussed in Appendix A of this report, even very low-powered devices transmitting just a few milliwatts of effective isotropic radiated power can cause harmful interference to radar receivers at distances of tens of kilometers.

It is difficult to know the extent to which illegally re-tuned Part 15 transmitters and outright, wholly illegal transmitters have been introduced into the 5 GHz DFS-only shared bands as a result of having opened those bands to DFS in the first place. This situation may be a classic example where correlation does not necessarily equate to causation. Introduction of illegal devices into DFS bands might have come about from the coincidental emergence of SDR, irrespective of DFS. But illegal tuning of legal devices and operation of wholly illegal transmitters seems to have occurred to a lesser extent or perhaps not at all in the 5 GHz DFS bands prior to the development and introduction of DFS-equipped U-NIIs. In any event, the advent of these phenomena in the DFS bands has prompted types of enforcement actions that were previously either rare or non-existent in those bands.

This particular issue is one that is associated with all SDR technologies; it is not necessarily limited to DFS. Many radio manufacturers now build a single device with capabilities tailored for the intended marketplace (e.g., USA, Europe, Asia) that can be activated or deactivated within the device's software. The issues associated with a user being able to defeat an intended

capability (such as DFS) by manipulating a user-accessible setting (such as the device's country code) were unanticipated. Such issues can be addressed by regulators. For example, the FCC has adopted a directive to lock the country code of DFS devices as a certification requirement.

### 4.3 Ongoing Need for Enforcement Actions in DFS Bands

It is not clear how often the operators of illegal, or at least illegally modified, DFS-band 5 GHz transmitters have understood that they are causing harmful interference and potentially endangering safety-of-life TDWR operations. A few operators who have been caught and fined by the FCC have subsequently *continued* to commit violations after they must have understood that what they had done was illegal, and that their actions were impairing TDWR operations.

In other words, it has turned out to be too much to expect that all operators of radio systems at 5 GHz, including supposedly professional DFS U-NII installers and operators, would always be good spectrum actors. The solutions for combatting bad actors have been multi-fold. First, the selectable country-code option has been eliminated; all units sold in the U.S. now have DFS functionality hard-coded into their firmware. Second, specialized RF antenna connectors are now provided with DFS units, making it more difficult (but not impossible) for installers and operators to substitute their own antennas for the proper antennas that come with the units.<sup>83</sup> In summary, multiple steps have been taken by U-NII manufacturers to make it much more difficult for bad actors to violate DFS rules by illegally modifying their devices.

As for illegal re-tuning of otherwise legal transmitters and illegal operation of wholly illegal transmitters, one solution may be stepped-up surveillance and enforcement activities by the government when such transmitters cause interference to 5 GHz radar receivers.<sup>84</sup> Another potential solution may be to impress upon industry the importance of self-regulation in this regard so as to avoid costly operational shutdowns and suspensions of new certifications.

Ultimately, enforcement actions by the FCC have turned out to be an important component of DFS implementation. The need for this robust enforcement activity was not anticipated by the developers of the DFS concept. Table 2 contains a summary list of these actions from 2007 to September 2019, with hyperlinks to detailed FCC information on each action.<sup>85</sup> A total of 53 actions are listed for those dozen years. Varying monetary fines have been levied by the FCC for some DFS rules violations. Virtually all FCC actions have been connected to interference to safety-of-life TDWRs. There has been an ongoing need for enforcement to make DFS function without causing harmful interference.

It appears that the need for an ongoing enforcement component of DFS will probably be a permanent feature of this spectrum-sharing technology. This continuing enforcement need

---

<sup>83</sup> Reverse polarity connectors are commercially available and may be procured by consumers.

<sup>84</sup> A court order signed by a Federal Judge is required for the seizure of illegal equipment by Federal authorities. The FCC typically works with a U.S. Attorney to provide an affidavit as to the violation. Typically it is executed by U.S. Marshals with FCC field agents as advisors.

<sup>85</sup> The FCC only publishes data on investigations after they have been completed and if some resulting public action has been taken.



apparently represents an unavoidable, ongoing opportunity cost for this version of spectrum sharing technology.

Table 2. Summary of FCC DFS-Related Enforcement Actions from 2007 to 2019<sup>86</sup>

<b>Date</b>	<b>Company Affected by FCC Enforcement Action</b>	<b>FCC Enforcement Action</b>
08-22-2019	<a href="#">WinPR, Inc., San Juan, Puerto Rico</a>	Notice of Apparent Liability
08-22-2019	<a href="#">CA Solutions, Inc., Boom Net, LLC, Caguas, Puerto Rico</a>	Notice of Apparent Liability
08-22-2019	<a href="#">Broadband Telecommunications Network, Corp., San Juan, Puerto Rico</a>	Notice of Apparent Liability
05-20-2019	<a href="#">Caribbean Network Solutions, Inc., Bayamon, Puerto Rico</a>	Notice of Apparent Liability
11-14-2017	<a href="#">RADWIN Ltd., RADWIN, Inc.</a>	ORDER & CONSENT DECREE
09-16-2016	<a href="#">Airosurf Communications, Inc., Edmond, Oklahoma</a>	Notice of Unauthorized Operation
07-29-2016	<a href="#">Towerstream Corporation, Middletown, Rhode Island</a>	ORDER & CONSENT DECREE
07-13-2016	<a href="#">Wide Cloud Communications, Hialeah, Florida</a>	Notice of Unauthorized Operation
06-13-2016	<a href="#">Aptech Networks Corp., Doral, Florida</a>	Notice of Unauthorized Operation
05-31-2016	<a href="#">Sooner Wireless, LLC, Norman, Oklahoma</a>	Notice of Unauthorized Operation
05-31-2016	<a href="#">Del Nero Communications Management, LLC, Norman, Oklahoma</a>	Notice of Unauthorized Operation
04-28-2016	<a href="#">Fastlane Internet, Francesville, Indiana</a>	Notice of Unauthorized Operation
03-11-2016	<a href="#">Satell SJNet, Corp., San Juan, PR</a>	Notice of Unauthorized Operation
03-13-2015	<a href="#">Directlink, LLC, Parker, Colorado</a>	Petition for Reconsideration Order
03-10-2015	<a href="#">5 GHz Devices Causing Interference to Essential Safety Systems Must Cease Operations - Letter Issued by FCC Enforcement Bureau Tampa, Florida Office</a>	LETTER
10-01-2014	<a href="#">CMARR, Inc., San Juan, PR</a>	FORFEITURE ORDER
06-24-2014	<a href="#">CMARR, Inc., San Juan, PR</a>	Notice of Apparent Liability
02-21-2014	<a href="#">Directlink, LLC, Parker, Colorado</a>	FORFEITURE ORDER
02-07-2014	<a href="#">Skybeam Acquisition Corporation, Englewood, Colorado</a>	FORFEITURE ORDER
02-07-2014	<a href="#">Rapidwave, LLC Saratoga Springs, Utah</a>	FORFEITURE ORDER
11-21-2013	<a href="#">VPNet, Inc., San Juan, PR</a>	ORDER & CONSENT DECREE
11-18-2013	<a href="#">Ayustar Corporation, San Juan, PR</a>	ORDER & CONSENT DECREE
08-06-2013	<a href="#">Towerstream Corporation, Middletown, Rhode Island</a>	Notice of Apparent Liability
02-12-2013	<a href="#">Argos Net, Inc., Caguas, PR</a>	FORFEITURE ORDER
01-16-2013	<a href="#">American Wireless Broadband, Chicago, Illinois</a>	Notice of Unauthorized Operation
01-04-2013	<a href="#">Directlink, LLC, Parker, Colorado</a>	Notice of Apparent Liability
12-13-2012	<a href="#">HiPoint Technology Services Inc., Chicago, Illinois</a>	Notice of Unauthorized Operation
09-27-2012	<a href="#">Skybeam Acquisition Corporation, Englewood, Colorado</a>	Notice of Apparent Liability
09-27-2012	<a href="#">AT&amp;T, Inc., San Juan, PR</a>	FORFEITURE ORDER
03-23-2012	<a href="#">VPNet, Inc., San Juan, PR</a>	Notice of Apparent Liability
03-23-2012	<a href="#">Argos Net, Inc., Caguas, PR</a>	Notice of Apparent Liability

<sup>86</sup> “U-NII and TDWR Interference Enforcement,” FCC, Washington, DC. Last visited on September 27, 2019. <https://www.fcc.gov/general/U-NII-and-tdwr-interference-enforcement>

<b>Date</b>	<b>Company Affected by FCC Enforcement Action</b>	<b>FCC Enforcement Action</b>
03-23-2012	<a href="#">Insight Consulting Group of Kansas City, LLC, Kansas City, MO</a>	FORFEITURE ORDER
03-13-2012	<a href="#">The WIFI Store, Toa Baja, PR</a>	Notice of Unauthorized Operation
03-13-2012	<a href="#">David Robles dba dmwireless, Manati, PR</a>	Notice of Unauthorized Operation
12-20-2011	<a href="#">ExtraSpace Storage, Henderson, NV</a>	Notice of Unauthorized Operation
09-19-2011	<a href="#">Sling Broadband, LLC</a>	FORFEITURE ORDER
07-29-2011	<a href="#">Sling Broadband, LLC, Hollywood, FL</a>	Notice of Apparent Liability
07-29-2011	<a href="#">Insight Consulting Group of Kansas City, LLC, Kansas City, MO</a>	Notice of Apparent Liability
07-29-2011	<a href="#">Ayustar Corporation, San Juan, PR</a>	Notice of Apparent Liability
07-28-2011	<a href="#">Rapidwave, LLC, Saratoga Springs, Utah</a>	Notice of Apparent Liability
06-02-2011	<a href="#">Crucito Marrero dba CMARR, San Juan, PR</a>	Notice of Unauthorized Operation
02-17-2011	<a href="#">AT&amp;T, Inc., San Juan, PR</a>	Notice of Apparent Liability
02-11-2011	<a href="#">Utah Broadband, Sandy, Utah</a>	Notice of Apparent Liability and ORDER
11-24-2010	<a href="#">Ayustar Corporation</a>	Petition for Reconsideration Order
08-13-2010	<a href="#">Wireless Metro LLC, Houston, Texas</a>	Notice of Unauthorized Operation
08-13-2010	<a href="#">NSN Wireless LP, Houston, Texas</a>	Notice of Unauthorized Operation
07-20-2010	<a href="#">Sling Broadband, LLC, Miami, Florida</a>	Notice of Unauthorized Operation
04-26-2010	<a href="#">Axxcelera Broadband Wireless, Inc.</a>	ORDER & CONSENT DECREE
04-15-2010	<a href="#">Airspan Networks (Israel), Ltd.</a>	ORDER & CONSENT DECREE
04-14-2010	<a href="#">Motorola, Inc.</a>	ORDER and CONSENT DECREE
01-28-2010	<a href="#">Ayustar Corporation, San Juan, PR</a>	FORFEITURE ORDER
04-20-2009	<a href="#">Aeronet Wireless Broadband, San Juan, PR</a>	Notice of Unauthorized Operation
01-23-2007	<a href="#">Neptuno Networks, Inc., San Juan, PR</a>	Notice of Apparent Liability

#### **4.4 Lessons Learned from DFS Principles and Implementation**

All spectrum sharing technologies will have limits on what they can and cannot do. In the case of DFS, the effectiveness of the technology to prevent harmful interference depends on:

- The quality of the radar-detection algorithms
- The rate at which the APs monitor for radar pulses in the midst of regular message traffic
- The robustness of the DFS test regimes
- The extent to which DFS devices are installed and operated in accordance with manufacturer's included hardware, firmware, software and operating instructions
- The extent to which ongoing firmware upgrades do not unintentionally impair or disable DFS functionality

DFS technology can prevent most harmful interference at most times and places. It cannot and does not guarantee that absolutely no harmful interference will ever occur anywhere, in so much as such a guarantee could ever exist, even absent the introduction of spectrum sharing technologies. This less-than-perfect situation is, in effect, the price that is paid for implementing spectrum sharing and making use of the 5 GHz DFS band for more than just radar systems.

Summarizing the additional Lessons Learned from DFS principles and implementation:

**Lesson 2:** The use of dynamically based spectrum sharing technologies requires permanent, ongoing government expenditures for testing facilities and maintenance of trained, competent engineering staff for permanent ongoing surveillance of such devices. This state must continue for as long as any given class of dynamic spectrum-sharing devices continues to be sold and used in markets. Dynamic spectrum sharing is associated with ongoing post-certification compliance auditing<sup>87</sup> costs. This is not to say that the expenditures are not worth the advantages that society gains from more and better spectrum sharing; it is to say that such sharing has recurring technology-opportunity costs. The need for adequate ongoing technical auditing resources needs to be recognized.

**Corollary to Lesson 2:** Technical analysis and measurements will have to be performed to assess the impact of changing U-NII device technology on incumbent federal radar systems.

**Lesson 3:** Any non-trivial, innovative, dynamic spectrum sharing technology introduction, no matter how carefully it is initially devised, may result in some elevated interference potential when it is initially deployed. The more complicated or innovative the technology, the more likely it is that some unanticipated field-deployment situation may result in an increase in the potential for interference.

**Corollary to Lesson 3:** When new, innovative dynamic spectrum sharing technologies are introduced to a band, resources should be set aside in advance to accommodate the initial harmful interference cases that may be expected to occur.

**Lesson 4:** Post-certification compliance auditing may be necessary to identify spectrum sharing devices that have been illegally sold without proper regulatory certification.

**Lesson 5:** If installers and operators are able to illegally modify spectrum sharing devices to disable spectrum-sharing features, some will do so even knowing that they will be fined by regulators when they are eventually caught.

**Corollary 1 to Lesson 5:** Manufacturers need to restrict the ability to disable or modify their devices' spectrum sharing functionality as much as is physically possible. Regulatory entities need to do thoroughly examine all of a spectrum-sharing device's set-up and control sub-menus.

**Corollary 2 to Lesson 5:** Introducing legitimate, legal spectrum sharing devices to a band can have the unintended consequence of encouraging the proliferation of illegal devices in the same

---

<sup>87</sup> Such auditing, when done by NTIA, is done on DFS-equipped U-NII devices that NTIA purchases off-the-shelf from commercial vendors.

band. This is especially true if the band is used worldwide for such functions, but does not have the same spectrum sharing rules internationally as the U.S. has domestically.

## 5. DFS CHALLENGES FOR MANUFACTURERS AND VENDORS

The development and introduction of DFS technology into what was essentially a radar-only band required a very close collaboration among industry, which designs and builds DFS-enabled U-NII devices, and government spectrum regulators and government agencies that use multiple types of 5 GHz radars to accomplish their missions. This section focuses on some of the challenges that manufacturers faced in designing and developing DFS-enabled radio systems at 5 GHz.

### 5.1 Challenges to U-NII Device Manufacturers Understanding of Radar Systems

There is a deep technical divide between the radar and U-NII engineering communities. U-NII device design and development is part of a vast world-wide telecommunications industry that makes use of widely known and shared principles and approaches for research and development, prototype engineering,<sup>7</sup> and manufacturing engineering. Telecommunication industries sustain enormous markets that significantly contribute to entire national economies.

Radar systems, in contrast, are designed and developed by a relatively small engineering community. Radars are very expensive (a single radar station can cost hundreds of millions of dollars) and are sold in niche customer markets that are often, in essence, national governments. Radar design principles and requirements are typically not widely understood in telecommunications engineering communities. Generally, only a small cadre of technical specialists has a thorough understanding of radar systems. All of which means that technical characteristics and requirements of radar systems may not be understood by the design and development industry for systems like U-NIIs.

Lack of understanding by the U-NII device manufacturers of radar technology is exacerbated by:

- Reluctance of the radar industry, and of governments that are the radar industry's chief customers, to divulge technical details of their radar systems
- Reluctance and lack of motivation to discuss or explain much in general about how radars are designed and built
- Lack of public availability of many radars' technical operating characteristics
- Lack of motivation to describe why radars tend to have particular characteristics for pulse parameters, radiated power and antenna gain (e.g., the physical reasons why many radars have roughly one microsecond pulse widths and one millisecond pulse repetition intervals, about one megawatt of peak transmitted power, and about 30 dBi of antenna gain)
- Reluctance to reveal specific information about radars' susceptibility and vulnerability to interference that might be expected to be due to U-NII like signals, which has implications for radars' susceptibility to electronic warfare (EW)
- Reluctance or refusal in some cases to publicly disclose exactly which radar systems are deployed in any given spectrum band

There can be some justifications for aspects of non-transparency or even secrecy. Not least among these are security concerns for government and corporate trade advantages for industry. One of the most significant aspects of ITU-R Recommendation M.1652-1 [2] was that it represented an attempt by a number of administrations, not least the United States, to shed more light on a number of these points for 5 GHz radars where possible. Regarding the exact technical characteristics of individual types of radars, it has been the authors' experience that spectrum sharing development does not require that exact radar characteristics be disclosed in order for sharing to occur. In fact, it is arguably better for spectrum sharing to *not* be based on any one set of exact radar characteristics, as discussed in Section 4.2.4.

Even with that ITU-R Recommendation in hand, industry was faced with the need to begin to design radar-detection algorithms for U-NII devices while not necessarily having much knowledge about the radar signals that they were going to be expected to detect. Virtually their only official source for this information ITU-R Recommendation M.1652-1, and even it only described in fairly general terms the characteristics of the types of radar signals that AP receivers would have to detect.

Designing radar-detection algorithms (which must function in the midst of U-NII data traffic) was not a small or simple undertaking. Electronic intelligence (EI) gathering and monitoring systems that search for radar signals are typically sold to national governments at multi-million dollar prices. While the DFS goal of yes-no threshold detection of radar signals was not as complex as the full range of problems faced by EI designers, it was nevertheless technically challenging and furthermore had never before been implemented in commercially sold devices intended for use by consumers.<sup>88</sup>

Thus it was that industry U-NII manufacturers worked closely with U.S. government agencies at the engineering level for several years from the late 1990s to the early 2000s to devise working prototypes of DFS receivers that would effectively monitor for radar signals. Much of this collaborative effort occurred during industry visits to the ITS laboratory in Boulder, Colorado. During these visits the government provided helpful information and feedback to industry for DFS development, as described further below.

## **5.2 Difficulty of Detecting General, As Opposed to Specific, Radar Waveforms**

There was a persistent disconnect between industry and government during DFS development concerning the extent to which DFS monitors would or would not search for a specific set of radar signals. Government insisted that radar-model-specific algorithms should *not* be used for DFS. Industry sometimes seemed to not fully appreciate this goal. This communication disconnect was exacerbated by the fact that DFS rules and protocols were developed by people who were not themselves the design engineers who would be responsible for actually writing and coding the DFS detection algorithms.

After the rules had been agreed and the responsibility for actually making DFS systems fell to manufacturer's engineers, those engineers sometimes ended up with misunderstandings about

---

<sup>88</sup> A government requirement for 5 GHz DFS U-NIIs in the U.S. is that the devices are prohibited from collecting or retaining in memory the characteristics of the radar pulses that they receive during their operations.

exactly what they were supposed to be looking for in-between their U-NII transmission data packets. Chief among these misunderstandings was the idea there was “a” radar model in the 5 GHz band, and that it alone needed to be detected. Thus there was a presupposition by some design engineers who presumed that they only needed an algorithm to find this one radar’s unique waveform, as opposed to having an algorithm that would detect radar pulses in general, across a wide range of waveform values for pulse width, pulse repetition rate, and number of pulses.

### **5.3 Lack of Industry Testbeds for DFS**

A further challenge was that industry did not have any testbeds of its own for testing DFS radar monitors. This lack was entirely reasonable on both technical and financial grounds. First of all, the knowledge of how to even begin to design a testbed such as the one shown in Figure 1 was unavailable among U-NII manufacturers. Such testbeds are typically only built by a niche group of companies that specialize in EI and EW systems.

A second challenge was financial. Even if a system such as shown in Figure 1 had been completely sketched by the government for industry, the cost to build it might have been prohibitive considering the relative smallness of the U-NII market that it would serve. It also would seem wasteful for several U-NII manufacturers to each build their own DFS testbed when a single such testbed at a single location such as Boulder would suffice to meet everyone’s needs and could be used on a shared basis (albeit only by one manufacturer at a time) instead.

### **5.4 Development of the NTIA DFS Testbed and Its Use by Industry and FCC**

The development of the DFS testbed (Figure 1) by ITS and OSM engineers at the ITS lab in Boulder represented a significant investment by the government to move 5 GHz spectrum sharing forward. In its totality the development of this testbed absorbed about two engineering years (roughly \$650 thousand in today’s dollars) of government resources. This included procurement and programming of specialized test-and-measurement equipment and of specialized software for controlling the measurements and recording and analyzing the resulting data sets. A DFS test-set was not available off-the-shelf. Starting around 2010, various test device manufacturers were able to develop and sell their own equivalents of the ITS design. The FCC and NTIA only approved those test devices when they proved their equivalence.

In 2005 the U-NII manufacturing industry was invited by NTIA to make use of this testbed on a no-cost basis. Any U-NII manufacturer could send its prototype device or devices to the lab, as long as the devices were accompanied by knowledgeable DFS design engineers who could work the systems’ software on an as-needed basis during testing. A large number of companies took advantage of this offer and tested their devices at ITS.

Routine certification testing of radio systems is not part of the NTIA-ITS mission. ITS does not have authority to grant certifications for consumer or commercial devices; such certifications must come from the FCC. After the initial testbed was built and used to verify the performance of both early DFS monitors and of the testbed itself, NTIA transferred the testbed technology to the FCC and eventually to industry test houses. It would be the FCC and industry test houses that

would, in the long run, use the NTIA testbed design to perform routine ongoing testing and certification of DFS U-NII systems. The ITS-built testbed was however retained at ITS and is used to this day to perform some one-off spot-checks of off-the-shelf DFS U-NIIs and to troubleshoot individual types of DFS U-NIIs that have been flagged by the FCC or other government agencies as having potential problems with effective detection of radar signals. (This has come up mainly with examining firmware upgrade effects on DFS devices.)

### 5.5 Laboratory and Field Tests of DFS with Industry Participation

Starting in 2005, three U-NII manufacturers with DFS-capable prototypes accepted the NTIA offer to use the new testbed at ITS in Boulder. Each of these companies was scheduled to have up to two weeks of time at the lab to test their devices, although none actually ended up needing more than a week. Each manufacturer worked at the lab alone, with only ITS and OSM engineers to assist. There was no overlap between manufacturers with the testbed; ITS engineers did not share or discuss data among the manufacturers.

The fundamental information disconnect (described above) about specific versus generalized radar waveform detection was only finally resolved when the three manufacturers sent DFS design staff to perform early testing on prototype DFS monitoring devices. *It was only at that point, when the government system of Figure 1 was used to fire radar pulses at the DFS receivers, that some of the industry engineers finally got to see at first-hand exactly what it was that their systems were supposed to detect.*

To the manufacturers' great credit, when they finally got to see what the 5 GHz radar pulses (at least, the test pulses) looked like, they were all able to get their prototype DFS monitors running reasonably well in fairly short order. None of these companies had prior experience in generating or detecting radar-like pulses.

It is difficult to over-state the need for eventual face-to-face technical exchanges between spectrum engineers on the government and industry sides when nuts-and-bolts engineering of spectrum sharing systems needs to be accomplished. Design goals and specifications for sharing systems are necessary, but there is no substitute for human interchanges such as occurred when the government and industry people began to work together on testing at the ITS Boulder laboratory. The exchanges do not need to be long or complicated. But without them, huge misunderstandings can develop about what systems are supposed to do and how they are supposed to work.

**Lesson 6:** There is no substitute for person-to-person interchanges of critically important design information about technical requirements and needs for spectrum sharing systems. These human interchanges (as opposed to non-human interactions such as database sharing) must be between and among multiple government agencies (including regulatory agencies and agencies operating incumbent radio systems), the industry that is developing new devices, and private sector companies that will eventually buy and operate the devices.

**Lesson 7:** Development and implementation of a dedicated operational testbed might be well-advised, prior to widespread introduction of a new spectrum sharing technology. But testbeds



consume time and resources to build and operate. They tend to run counter to the desire to develop and deploy new technologies as quickly and inexpensively as possible.

## **6. CHALLENGES FOR GOVERNMENT DEVELOPMENT OF DFS TESTING AND CERTIFICATION PROTOCOLS**

When spectrum sharing protocols are being developed, it is the responsibility of government to inform industry of exactly what those protocols and technical requirements are going to be. This section examines the challenges to government agencies of developing such requirement when no such sharing approach has been implemented before.

### **6.1 The Difficulty of Designing DFS Protocols for Non-Existent Radio Systems**

Spectrum-sharing development has the advantage of knowing exactly which systems are already incumbent in a proposed sharing band, and what most of the technical characteristics of those systems are. But it has the disadvantage of not knowing the technical characteristics of future systems to be introduced into the band. Something is typically known of the likely general technology that will be used in the new sharing systems, but specifics may be hard to come by because nobody, not even industry itself, may know exactly what they intend to deploy.

This uncertainty may be caused by the desire of a government to remain technology-neutral regarding what it going to be newly introduced to a band. Thus only the broadest guidance outlines may be provided to industry, such as “communication systems will be introduced...”. In the case of the 5 GHz band, it was agreed at WRC-03 that the new systems would be wide area networks and radio local area networks (WANs and RLANs). This is fairly broad. Only later was the U.S. implementation at 5 GHz limited to U-NIIs. And even that was a broad technology area. For example, there were two general types of technology employed by U-NII devices: IEEE 802.11 standard technology and frame-based transmissions defined by IEEE 802.16. It can be an open question as to whether one type of spectrum sharing technology can or will work across all available types of communication systems within a single service such as U-NII.

### **6.2 Advantages of Working on a Blank Slate**

Government agencies may have to be somewhat vague and general about exactly what the requirements of their spectrum sharing protocols will be. They may specify channel-check times and channel move times based on the vulnerabilities of their own incumbent systems (5 GHz radars in this case). But other sharing requirements may depend on the characteristics of the new radar systems that are to be eventually introduced into a band at a later date. As noted above, those characteristic may be unknown in advance.

A good aspect of this situation is that it may be regarded as an opportunity for some party, either a government agency or industry or both, to move the process forward by considering that the new spectrum sharing is going to be a blank slate for new development. This condition can then become an opportunity for innovation. But some initiative may be required of both sides to take advantage of this situation. In the case of 5 GHz DFS development, forward movement was achieved over time by numerous technical interchanges in which certain aspects of sharing were negotiated. These included:

- Only AP units (not clients) would monitor for radar signals

- The government would provide industry with a monitoring threshold for radar signals
- The government would not ask industry how their radar detection algorithms worked
- Industry would submit their DFS devices for general-purpose radar waveform detection testing rather than radar-specific testing
- Industry could use any basis for U-NII data packet protocols (i.e., both IEEE 802.11 based and frame based systems). They would all be submitted to a single set of tests and would be subject to a uniform set of pass-fail criteria.

### 6.3 Disadvantages of Having Areas of Developmental Doubt and Uncertainty

Neither government nor industry may necessarily be able to specify other important aspects of the spectrum sharing protocols in advance of actual sharing implementation. This is because some protocols may depend on design characteristics of the new sharing devices that cannot be known until the devices (or at least good prototypes) have finally been built.

In the case of 5 GHz DFS, two such problems had to be solved. The first was to determine the power levels in 5 GHz radar receivers that would cause harmful interference. This was not a parameter that had ever been defined for radar receivers. Very little work had been done in that area, or at least none that had been published in open technical literature. Thus government engineers (ITS and OSM) had to undertake a multi-year, roughly million-dollar effort to determine harmful interference thresholds for a number of different radar system receivers. This work involved numerous other agencies including the Department of Transportation (FAA); DoD (Army and Navy); and Department of Homeland Security (Coast Guard). Industry was also involved as they were manufacturers of the radar systems. Some of the work was even done by NTIA engineers in cooperation with the UK administration<sup>89</sup> at Southampton and Funtington sites in that country.

In the end the government was able to provide an  $I/N$  ratio of -6 dB that would be considered a threshold for harmful interference. That interference threshold for radar receivers was then converted into a detection threshold at the antenna outputs of DFS devices, to preclude interference to radar receivers. So the problem was solvable in advance of DFS deployment via mathematical and simulation modeling. Federal agencies and U-NII industry engineers worked together to develop the simulations based on common assumptions, scenarios, and propagation settings. They developed and ran independent simulations that showed common outputs.

The other main problem that occurred in this area was the question of how much frequency change would be required of the DFS units when they had detected a radar. This problem was not so easily solved in advance of DFS-system construction because it depends on two factors, only one of which could be accommodated in advance: The 3-dB bandwidth and shape of radar receiver intermediate frequency (IF) stages and the roll-off rate of U-NII spectrum emissions. The radar IF problem was addressed by measuring radar IF stage responses for every radar type that was checked for  $I/N$  response. But the U-NII roll-off rates could not be known until the

---

<sup>89</sup> Office of Communications (OFCOM) and the Ministry of Defense (MoD).

U-NIIs were built, and the U-NIIs were not going to be built until the rules for sharing were in place. It was a classic Catch-22 situation.

In the end, the original DFS rules ended up simply calling for U-NII devices to vacate their operational channels when they sensed a radar signal. Thus they could jump as little as one channel up or down in frequency in their band when they sensed a radar, so long as they first did a channel check. If that new channel showed radar activity, then they would have to keep selecting and attempting other channels or simply go to another band entirely, such as 2.4 GHz.

This one-channel minimum jump requirement turned out to not always be adequate in practice. With the evolution of the 802.11 standard and wider bandwidth devices, the newer devices in some cases did not move enough and still affected TDWRs. But it could not be modified until DFS U-NIIs were built and a government agency (NTIA) had an opportunity to measure the emissions of an entire family of such devices. These measurements were eventually published in [4]. They were used as the basis for refined estimates of how much frequency (channel) change would be needed to preclude interference to radars when DFS U-NIIs sensed them.<sup>90</sup>

**Lesson 8:** Some technical spectrum sharing parameters cannot be known until after spectrum-sharing devices have been built and possibly deployed. This lack of knowledge can result in flaws in spectrum sharing device certification testing.<sup>91</sup>

---

<sup>90</sup> In practice many U-NIIs ended up not jumping a single channel at a time upon radar detection, but instead simply changing operating bands and going to the Industrial, Scientific, and Medical (ISM) band at 2.4 GHz to preclude interference. This was an industry expedient rather than an FCC requirement.

<sup>91</sup> ITS was not able to measure the emission spectra of the U-NII devices until they were available via commercial production. Simulations done prior to U-NII devices being commercially produced were based on proposals or existing data for similar devices operating in other radio bands.

## **7. EARLY DFS DEPLOYMENTS: FIRST SUCCESSES AND FAILURES IN THE FIELD**

The events recounted in this section have already been described in detail in two NTIA Technical Reports [5], [6]. They are summarized briefly here for their relevance to the problem of DFS Lessons Learned.

### **7.1 San Juan, Puerto Rico and New York City Harmful Interference Events Review**

In 2009 the FAA began to experience a puzzling new type of interference at multiple TDWR stations in the continental U.S. and the Possession of Puerto Rico. The worst of the interference occurred at the San Juan, Puerto Rico, TDWR with the second-worst interference occurring at New York City area TDWRs. FAA teams met with some initial success with examining the interference. Based on initial information from the FAA there were indications that the interference might be caused by 5 GHz DFS-enabled U-NII devices in these areas. The FAA contacted NTIA and requested a joint effort to examine and resolve the interference problem. Because the interference sources were suspected to be private-sector systems, the FCC was also contacted for support and assistance via their offices in Washington, DC, and San Juan, Puerto Rico.

### **7.2 Identification of Interfering DFS-Equipped Devices at San Juan**

It was agreed that, since the interference characteristics were similar at all TDWR locations, a detailed study of a single such location was necessary. Its results would be applicable to all locations. The interference problem was worst at San Juan, Puerto Rico, so this was selected as the study location.

Prior to traveling to San Juan, the lead author of this report made a one-day field trip to the FAA Aeronautical Center in Oklahoma City to examine the TDWR there. He especially needed to see how to partially disassemble the radar for the work that would need to be done in San Juan so that he could determine how to access the various test points in the TDWR receiver chain, from the antenna output to the IF output that feeds the quadrature and in-phase (I and Q) detector prior to signal processing.

Shortly afterward, the joint FAA-FCC-NTIA (ITS and OSM) team assembled at San Juan. The approach for identifying the interference sources was methodical:

- First, examine and document the interference characteristics on the radar data display. This included observation of how many radial interference lines (strokes) appeared.<sup>92</sup>
- Second, examine and document the appearance of the radar in the time domain in the radar receiver IF stage. This examination showed that the interfering signals were coming from

---

<sup>92</sup> Multiple strokes could indicate either multiple sources of interference. Alternatively they could be produced by a single interference source that was hitting the radar hard enough to couple into both the radar antenna main beam and its side lobes. Such antenna multi-lobe coupling can produce a multi-stroke “rising-sun” radar display.

multiple sources that used both 802.11 and frame based data packet protocols (which of course meant that the problem was originating with U-NII devices).

- Third, partially disassemble the radar's radiofrequency (RF) front end stage and examine its responses to the interference and to input test signals. This was to determine whether any front-end overload was occurring. As part of this stage in the work the radar's RF low noise amplifier (LNA) was tested to determine its overload point and compare that power level to the interference power level.
- Check and document the exact correlation between every azimuth where interference was occurring and the type of signal causing interference on each of those azimuths.
- Perform field work with the FCC to locate interfering transmitters and determine their technical characteristics, including whether they were adhering to DFS rules.
- Tests on an in-service operational radar must be performed carefully and expeditiously. While tests are being performed the radar is considered to be out of service and its data are not available for monitoring or controlling airspace and weather.

The entire effort took two weeks. The work at the radar was completed by the second day and the rest of the two-week period was absorbed in locating and examining interfering DFS-equipped U-NII devices. Several interfering U-NIIs were identified and located. In the end it was determined that one U-NII device had been illegally imported and operated in the TDWR band without DFS functionality. Other units were nominally legal as purchased but had been illegally modified, as for example being operated with after-market antennas. Puzzlingly (at that time), some units seemed to have been bought and set up legally but nevertheless were causing interference to the TDWR, as documented in [5].

San Juan turned out to have the worst interference problem in US&P because the local topography is extremely rugged; local WISPs found wireless links to be an attractive solution to their Internet backhaul problem under this condition [5]. U-NII devices being utilized for Internet backhaul communications tended to be sited at high elevations, such as on mountains, and thus often had direct line of sight to the San Juan TDWR antenna. This resulted in the interference coupling into the TDWR mainbeam as the radar antenna rotated.

### **7.3 NTIA-FAA-FCC Cooperative Efforts at Field Locations**

The problem with the San Juan DFS U-NIIs that had passed certification testing and had been properly installed but had nevertheless failed to detect a TDWR in the field was a mystery that had to be resolved. To do this, NTIA and FAA set up a series of tests and measurements with the FAA TDWR in Oklahoma City. Since this was an engineering unit at the Aeronautical Center, it could be used for such work without interrupting service in any airport operations.

The work, as documented in [6], showed that the protocols being used for radar test-bin waveforms for DFS certification could be passed by DFS-equipped AP monitors that nevertheless could not reliably detect actual TDWR transmitter stations. The problem was

rectified by adding more waveforms to the existing radar test-bin waveforms, waveforms that were more representative of the pulses actually transmitted by TDWRs.

It is important to note that this problem did not occur for all DFS U-NII device types that had been certified. Some devices certified with the original radar waveforms did detect TDWRs reliably. In other words, the problem of insufficiently designed radar-testing waveforms could only be discovered and found after several different models of DFS-equipped U-NII devices had been put through the testing and deployed in the field.

Another outcome of the work at San Juan and Oklahoma City was that local FCC field agents acquired a great deal of proficiency in developing measurement techniques that can be used to search and locate U-NII devices that cause interference to TDWR. These measurement techniques have been used extensively since then to identify non-compliant U-NII devices at locations across US&P.

The FCC staff working on these efforts found that the transmission of service set identifiers (SSIDs) was of enormous assistance in identifying interference sources. They developed an equipment package to read SSIDs (as also noted in the discussion of the Air Force experience in locating interference to Range Instrumentation Radars in Section 8). The transmission of SSIDs (or some other identifying information, i.e. GPS coordinates) would greatly simplify the identification of interference sources.

**Lesson 9:** Shortcomings in certification testing (such as initially inadequate radar waveform characterization for DFS) may only be discovered after a variety of devices (multiple models marketed by numerous manufacturers) have already been tested, certified, and deployed.

**Corollary to Lesson 9:** In hindsight, it would have been well advised for commercially produced 5 GHz DFS-equipped U-NII devices to have been initially introduced at a limited number of pre-identified field sites in close proximity to TDWRs (and other 5 GHz radars). Their operations at those sites could have been evaluated, with corrections to certification testing, prior to full-scale certification and deployment of such devices in open markets.

**Lesson 10:** Certification testing requirements for spectrum sharing devices need to be as technically robust as possible. Manufacturers may have concerns that some certification testing might be difficult to pass. But experience has shown that if devices are allowed to pass testing with less-than-robust protocols, their developers tend to build devices that only meet the reduced requirements. Such devices may then tend, disproportionately, to cause harmful interference to incumbent systems when they are deployed at field locations.

**Lesson 11:** Some technical modifications or additions may need to be made to develop new or improved spectrum sharing technology subsequent to initial market introduction.

## 8. HARMFUL INTERFERENCE AT U.S. ROCKET TEST AND SPACE LAUNCH RANGES

Harmful interference from U-NII transmitters to TDWR receivers has been thoroughly documented in previous NTIA Technical Reports ([4]–[6]) and has been summarized again in this report (Section 7). Since the original publications, additional harmful interference has occurred from U-NII transmitters to Range Instrumentation Radars (RIRs), more formally known as Missile Precision Instrumentation Radars (MPIRs), at U.S. rocket test and space launch ranges on the east and west coasts. This section focuses on the problem as it exists at Cape Canaveral, Florida, because NTIA, the FCC, and the U.S. Air Force have documented first-hand experience with the problem at that location. This section is structured as follows:

- The use of 5 GHz RIRs during normal range operations, including
  - Radar skin tracking and reinforced-pulse radar beaconing
  - Radar calibrations
  - Space observation missions
- Overview of spectrum sharing between RIRs and 5 GHz U-NIIs
- Interference coupling from U-NIIs to RIR receivers
- How U-NII interference affects the radars and implications for possible impacts on range operations
- Proposed ways forward to prevent the interference, both now and in the intermediate and long-term future

Some of these topics involve detailed, digressive technical discussions. Those discussions have been placed in Appendices B through D.

### 8.1 Overview of 5 GHz Range Instrumentation Radars

The federal government uses RIRs to track launch vehicles (LVs) during their ascents. An example of one of these radars is pictured in Figure 5. This equipment operates mostly in the 5250–5925 MHz band, which is allocated on a primary basis for radiolocation functions. Occupancy of the upper part of this band is described in [7].

Tracking radars do not sweep broad swaths of sky in the manner of air traffic control or weather radars.<sup>93</sup> Instead, they use narrow beams of highly directed energy to locate and actively follow objects on individual tracks as they move across the sky, as shown in Figure 6. Some of these radars have an additional mission to observe objects in Earth orbit, but again as individual objects at a single time.

---

<sup>93</sup> One RIR variant, the AN/TPQ-39, has been modified to function as a weather surveillance radar.





Figure 5. A RIR antenna (8.8 m diameter). Note three strut support points for an earlier-generation RF feed. Circular aperture at right is for a co-axial telescopic camera.

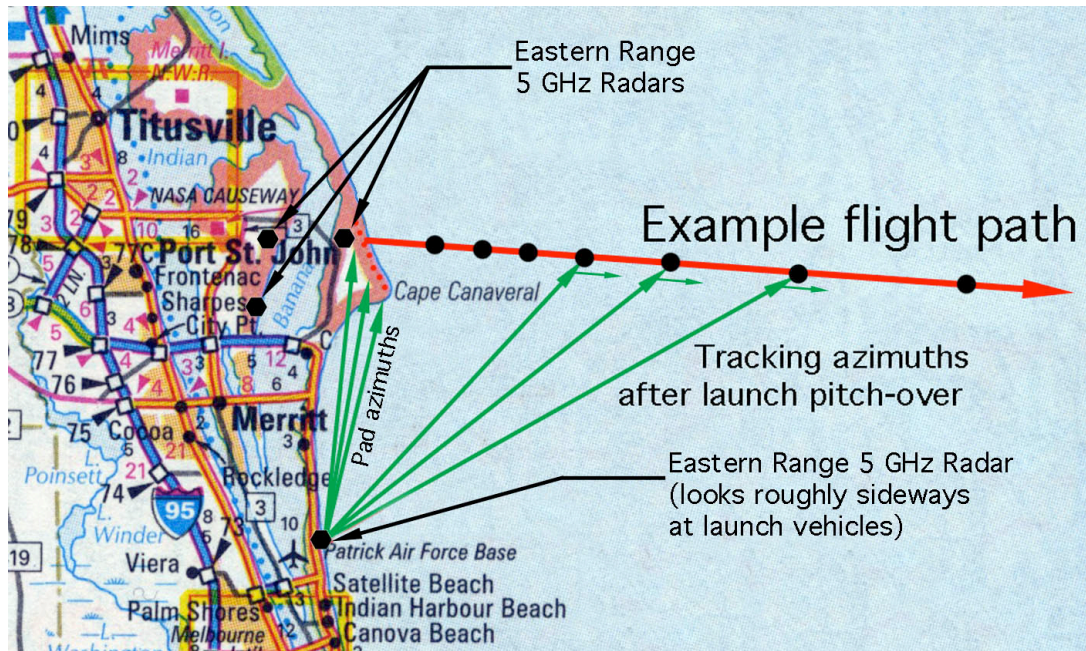


Figure 6. Example of multiple-RIR deployment at a single range.

As described in Appendix B (Table B-1), a substantial variety of 5 GHz RIR models (at least 15 types) exists. But with the exception of the phased array AN/MPS-39 and AN/FPQ-17 they

are all related to each other by common descent from the Radio Corporation of America (RCA) AN/FPS-16, itself developed from the experimental Navy Bumblebee radar of 1946–50. With the arguable exception of the original FPS-16, each RIR model has been produced individually in small numbers. But as shown in Appendix B (Figure B-1) their deployments are widespread at many test and launch ranges. Each of these places typically hosts multiple RIRs, as shown by example in Figure 6 for the Eastern Range at Cape Canaveral.

## 8.2 RIR Missions

To understand how RIRs are used, what their susceptibility is to RF interference, and how they are affected by RF interference, it is necessary to first understand how they work. And how they work is a direct result of their three operational missions.

The first mission is missile-launch tracking, in which a target's three-dimensional position (range, azimuth angle, and elevation angle  $(r, \theta, \phi)$ ) is measured relative to the radar station on a continuously updated basis during a launch or flight (providing a set of  $(r(t), \theta(t), \phi(t))$  data). Even more important than position-versus-time data are rapidly updated target velocity component vectors  $(V_{1,2,3}(t))$  that are required for range safety, as described further below.

The second mission is tracking debris from launch anomalies, these events ordinarily being either dynamic break-up or intentional termination (destruction) of LVs in flight. In the event of an anomaly, the RIR tracking follows, in order of priority: *crewed elements* emerging from the break-up, *thrusting elements* (e.g., still-burning solid-fuel booster sections), and then the *payload section*. Other debris may be followed with lower priority. If a cloud of hazardous, aerosolized fuel is released and drifting, the RIRs may track the cloud's progress for provision of safety warnings.<sup>94</sup>

The third RIR mission is observation of space objects. This, too, is fundamentally a tracking operation. As an object in space is held in the radar's tracking beam for an arbitrarily long time interval,<sup>95</sup> the number of pulse echoes that can be integrated from the target can likewise be made arbitrarily large. Long-term integration of thousands or even millions of pulse echoes allows space objects with very small echo-return cross sections to be closely observed and processed with fine detail. Observation data include highly accurate orbital element determination and, with chirped pulses, observations of objects' spatial forms.

Given that all RIR missions involve tracking, it is necessary to understand how the tracking works to see in turn how U-NII transmitters can interfere with the tracking and what the interference mechanism is. These topics are explained in detail in Appendices C and D.

## 8.3 Range Safety and 5 GHz RIR Tracking

With the operational missions and functionality of the 5 GHz RIRs understood, the next step is to examine the role that these radars play in range safety. Prior to a launch, a range is cleared

---

<sup>94</sup> Information in this paragraph is *pers. comm.*, Mr. C. C. Harrison, Eastern Range Radar 0.134.

<sup>95</sup> Even brief space object transits above a local horizon may last for a few minutes.

through a combination of visual observations from aircraft and boats, sweeps of water surfaces with 3 GHz and 9 GHz surface surveillance radars, and observation and coordination of the local airspace via 1030–1090 MHz air traffic control transponders and short-range (approx. 80 nmi) 2.7–2.9 GHz surveillance radars such as ASR-9s, ASR-11s, and GPN-30s.

With the range cleared and the vehicle prepared for launch, the RIRs are trained as closely as possible<sup>96</sup> on the launch pad (or water surface for submarine launches or mother aircraft for airborne launches). As the vehicle clears the launch gantry (or water or mother aircraft) and begins its pitch-over maneuver, it is tracked by at least two and sometimes three of the following systems: 5 GHz skin tracking, 5 GHz beaconing, and S-Band (roughly 3 GHz) metric GPS tracking. Table 3 describes the criteria for employing these systems with any given vehicle.

As the vehicle flies downrange its progress is followed by a pair of Range Safety Officers (RSOs) sitting side-by-side at a control panel with an identical pair of displays and control switches in front of them. Although the tracking systems provide vehicle position updates, the most important thing for the RSOs to know is not where a vehicle *is* but where it is *going*. The tracking systems’ most important data is therefore vehicle velocity vectors (direction and speed of movement). High-speed digital computers convert raw tracking data into rapidly updated (about 10 updates per second) predictions for impact points *ahead of the flight track* for the vehicle based on its currently reported velocity vectors.

Table 3. Overview of Criteria for Launch Vehicle Tracking Selections

Launch Guidance & Control (G&C) Reliability:	Tracking Systems Used:
Vehicle G&C system has been proven to be reliable through numerous successful flights	Two: S-Band (3 GHz) GPS beacon and 5 GHz skin tracking
Vehicle G&C system has not flown enough successful missions to be considered proven	Three: S-Band GPS (3 GHz) beacon, 5 GHz radar beaconing and 5 GHz skin tracking

*Redundancy in the data sources for impact predictions is vital.* The two best data sources are the 5 GHz radar beacon and the GPS beacon. This is because the beacon pulses are received at higher power than skin echoes; the beacons provide better tracking and velocity information than the 5 GHz skin echoes.

But skin tracking is still critically important. Skin tracking is independent of any systems carried on-board a launch vehicle (LV). It is the *only* redundancy for the GPS beacon for vehicles with proven guidance and control systems which therefore do *not* carry the 5 GHz radar beacon (Table 3). And *only* skin tracking can follow booster elements that have been hurled randomly across the sky after a launch anomaly in which a vehicle breaks up. Figure 7 shows a schematic booster being skin-tracked while flying both beacon systems.

<sup>96</sup> In populated areas such as Cape Canaveral radiation safety cut-outs may preclude exact radar antenna boresighting on the launch pad, as noted above.

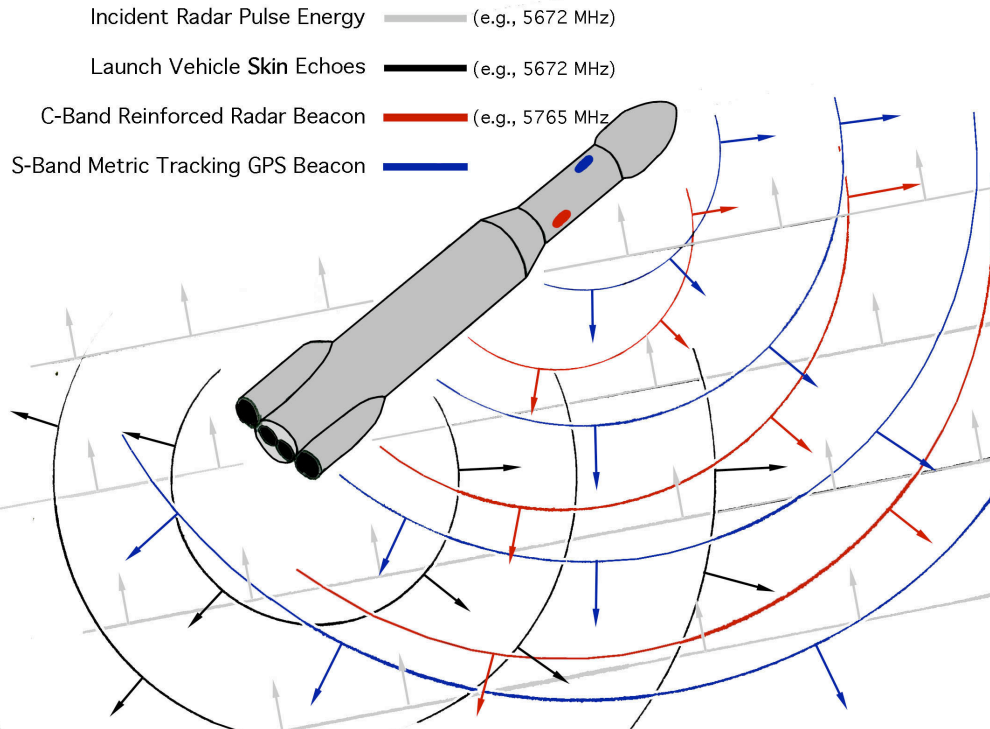


Figure 7. Schematic diagram of a booster being skin tracked while flying both possible beacons.

If RSOs lack tracking information to provide location, velocity and impact-point updates, they cannot guarantee that the vehicle is flying nominally. Lacking adequate tracking information, their range-safety protocols can require termination (destruction) of a vehicle along with its payload in that circumstance. This destruction requirement can occur even if the vehicle itself is actually flying and guiding completely nominally. This is why it is crucially important to maintain multiple redundant tracking sources throughout every launch.

To state the situation slightly differently, in the event that data should be lost due to 5 GHz RF interference to the skin tracking radar signal and the 5 GHz beacon (if an LV is so equipped per criteria of Table 3), the RSOs would be left with a single tracking system, the S-Band GPS beacon, to verify LV performance and impact points. If the LV is *not* flying with the 5 GHz radar beacon then interference to *just* the skin tracking would reduce the RSOs to having *only* the GPS beacon data for flight monitoring at that point in the mission.

If for any reason that last line of defense, that last GPS-based tracking data flow, should then be lost, the RSOs would be unable to verify that predicted impact points were still in safe zones. This could put them into the position described above, where they could be faced with a requirement to terminate an LV and its payload even though the vehicle might in fact be guiding and thrusting perfectly well.<sup>97</sup>

<sup>97</sup> Within the next few years this issue will extend to crewed vehicles being launched from Cape Canaveral.

## 8.4 RIR Spectrum Shared with U-NII Transmitters

Figure 8 shows a schematic of 5 GHz spectrum that is shared between RIRs and U-NIIs.<sup>98</sup> The Eastern Range RIR frequencies are shown by way of example; other particular frequencies are used for RIRs at other facilities.

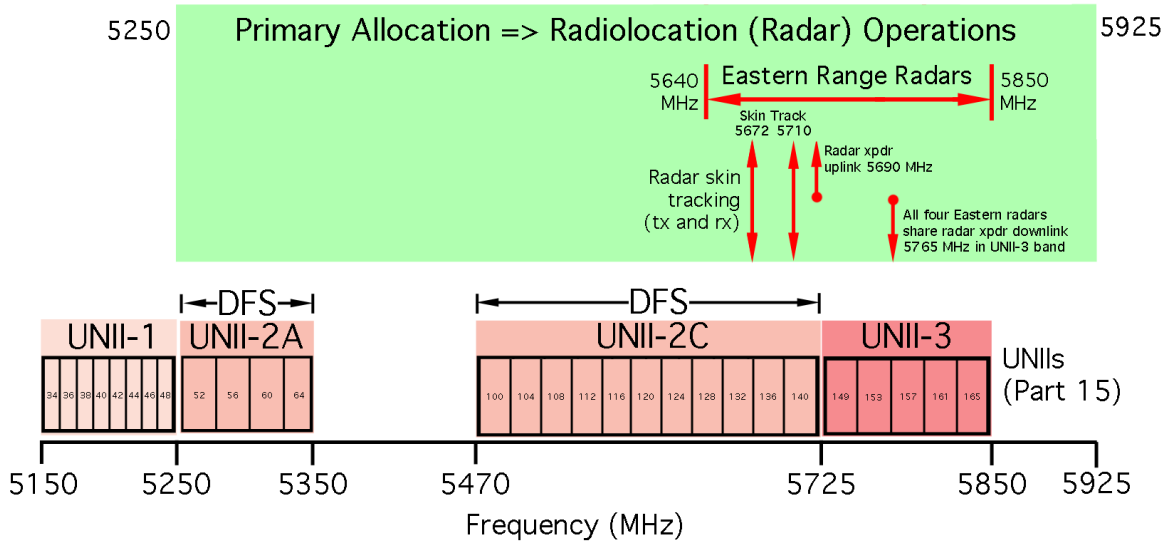


Figure 8. The 5 GHz spectrum that is shared between RIRs and U-NIIs, with Eastern Range frequencies used as an example case. U-NII Band 3 shares spectrum with radars, including some RIR frequencies, but has never had any DFS requirement.

The spectrum between 5250 and 5925 MHz is allocated on a primary basis for radiolocation (radar) operations. RIR operations use the upper part of this band, 5640–5850 MHz in the case of the Eastern Range, for example.<sup>99</sup> Skin tracking at that range is done on frequencies of 5672 and 5710 MHz. Radar beaconing is done for all of the Eastern Range radars on a common, shared downlink frequency of 5765 MHz. (The beacon uplink is a shared frequency of 5690 MHz.)

Unlicensed intentionally radiating devices (FCC Part 15), including 5 GHz U-NIIs, operate on a not-to-interfere basis in four bands at 5 GHz, three of which are shared with radiolocation. The lowest U-NII band, designated U-NII-1, is 5150–5250 MHz. It is below the lower edge of the radiolocation band and is of no further concern here.

The next two U-NII bands, 5250–5350 and 5470–5725 MHz, are designated 2A and 2C (see Figure 8). They share spectrum with radars. This includes frequencies near 5.6 GHz that are used by FAA TDWRs. *In both of these bands the U-NIIs are required to employ DFS technology.*

Finally comes the uppermost U-NII band, designated U-NII-3, between 5725 and 5850 MHz. U-NII-3 devices are *not required to use DFS detect-and-avoid technology to prevent interference to radar receivers*. The power limit for U-NII-3 transmitters is an EIRP of 4 watts = +36 dBm,

<sup>98</sup> U-NII bands in Figure 8 are from CFR 47, Sub-Part 15.407. Channels are taken from Annex J of IEEE 802.11-2007, as modified by amendments k, y, and n.

<sup>99</sup> A range radar at Wallops Island, Virginia, is authorized to operate at frequencies up to 5925 MHz.



the same as is used for our interference distance calculation in Appendix A. The U-NII allocation for it was made prior to the development of DFS. It is not clear why this third U-NII band that shares spectrum with radars has never had a DFS requirement for its sharing.

All of the U-NII bands are divided into channels according to designations specified by the IEEE 802.11 standards committee. The channeling scheme is somewhat complicated. Basic channels (Figure 8) can be combined to make wider channels for operators to use.<sup>100</sup>

## **8.5 Example U-NII-to-RIR Interference Case Histories at Cape Canaveral**

U-NII transmitters are causing harmful interference to RIR receivers at Cape Canaveral (the Eastern Range) and have caused such interference at Vandenberg AFB. U-NII interference may possibly be occurring to RIR receivers at some other locations. The ongoing Eastern Range interference is described here in some detail because the authors have had access to complete case histories at that location and have been able to interview range personnel there. The Cape interference cases are examples of what is apparently happening at a number of locations.

At the Eastern Range, for example, 5 GHz skin tracking is done on frequencies of 5672 and 5710 MHz (Figure 8). These frequencies are within the U-NII-2C band in which DFS employment is mandatory. Radar beaconing at the range is performed on a shared downlink frequency of 5765 MHz. This frequency is in the U-NII-3 band where DFS is *not* required.

Interference occurs in both of these bands at Cape Canaveral. Range radar and frequency management personnel<sup>101</sup> have estimated that roughly ten percent of the problems are occurring on the skin-tracking frequencies in the DFS-required U-NII-2C band and that the remaining ninety percent of problems are in the non-DFS U-NII-3 band where the beacons are operated.

Unfortunately, since the beacons provide better data than skin tracking and are therefore considered more important for range operations and safety than the skin tracking data, the 5 GHz RIR band where the most important data (beacon data) are produced is also the one where the bulk of the interference problem exists, at least at the Eastern Range.

### **8.5.1 Interference in the DFS-Required U-NII-2C Band**

Eastern Range radar personnel have seen persistent interference to skin-tracking operations at multiple RIR stations (see Figure 6). The interference has originated from a variety of devices that are mostly terrestrial and sometimes marine. Some systems are used by private individuals but many are operated by businesses or companies. The sources are typically but not always used for wireless backhaul by WISPs. The U-NIIs are used in WANs and RLANs. Most interference has been caused by outdoor transmitters but a minority share of problems has come from indoor

---

<sup>100</sup> IEEE 802.11 provides for channels that are 20 MHz wide and can be combined into multiples that are 40, 80, and 160 MHz wide.

<sup>101</sup> Mr. Scott Peterman, Senior EMC engineer of the Frequency Control and Analysis (FCA) Space Communications Squadron (SCS), 45<sup>th</sup> Space Wing, and Mr. C.C. Harrison, engineer at Eastern Range Radar Station 0.134.

devices. This suggests the outdoor devices such as outdoor Internet backhaul communications represent the greatest interference potential to incumbent radar operations.

Because DFS is required for all devices operating in the U-NII-2C band, Eastern Range radar operators have attempted on multiple occasions to force the U-NIIs off the radar frequencies by directly aiming their radar mainbeams in the directions of interference sources (with allowance being made for radiation safety cut-outs). *In no cases have the U-NIIs detected the RIR signals and vacated the radar frequencies, as would have been expected for DFS-equipped U-NIIs.* As described below, we believe that this non-detection problem is due to the fact that the range radars use pulse repetition rates (PRRs) that are outside the range of PRRs used to test and certify 5 GHz DFS devices.

A particular problem occurs with U-NII transmitters on cruise ships. A number of these vessels operate out of Port Canaveral and employ on-board 5 GHz U-NIIs. They are mostly non-U.S. flagged and may therefore have 5 GHz U-NII systems operating onboard that are not necessarily set to the U.S. country code that would enable DFS. These ships sometimes route their U-NII traffic to shore stations (e.g., in at least one known case to an AP at a shore-side restaurant) to avoid the cost of satellite-based backhaul links.

When the cruise ships first leave Port Canaveral, they often stop dead in the water due east of the Eastern Range radars while they perform mandatory lifeboat-muster drills. Their ship-to-shore links then boresight the radar stations and cause harmful interference for extended periods of time. This type of situation or scenario was not considered when the U-NII rules were developed. Some RIR receivers are equipped to observe interference from U-NIIs in their receiver diagnostic outputs. A sketch of one of these is shown in Figure 9.

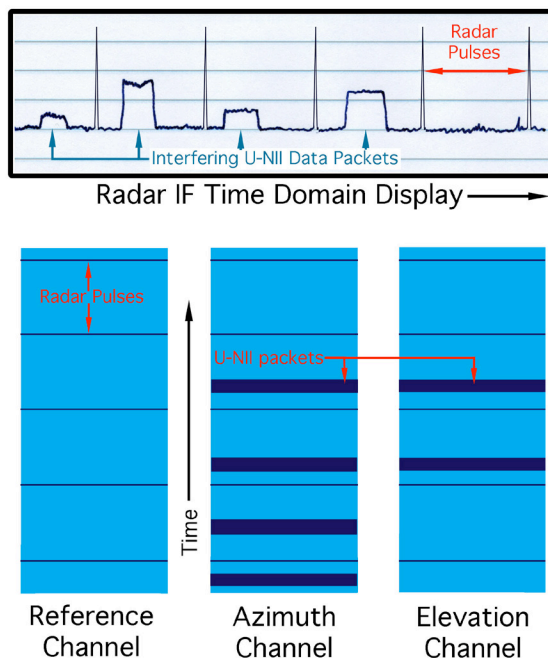


Figure 9. Sketch of a RIR receiver diagnostic display where operators can see interference during radar operations (drawn from the lead author’s *in situ* notes at a Cape Canaveral radar station).

The radar operators can see the U-NII data packets in the time domain, along with the radar's own pulses, in the upper portion of their display. In the lower part of their display, three channels are streamed from bottom to top as the radar runs. These channels are Reference, Azimuth and Elevation. Interfering U-NII packets will manifest as harmful interference in one or both of the azimuth and elevation channels but *not* in the reference channel. When an operator sees a feature in either or both of the azimuth and elevation channels but *not* in the reference channel, that feature represents harmful interference. This situation occurs frequently at Eastern Range radars.

### **8.5.2 Interference in the Non-DFS U-NII-3 Band**

The same comments and descriptions regarding interference for the DFS U-NII-2C band (above) are true for the non-DFS U-NII-3 band. Of course, there is no expectation that interference sources should detect and avoid radar channels in the U-NII-3 band. As noted already, range personnel estimate that ninety per cent of all U-NII interference problems are occurring in this band. The interference harms the radar beacon tracking even more than the skin tracking; in both cases range personnel state that the interference pulls the tracking away from targets.

### **8.5.3 Interference Case Summary for Cape Canaveral**

The 45<sup>th</sup> Space Wing staff have written well-documented reports describing their efforts to locate and mitigate 5 GHz interference at the Eastern Range. They have developed a specialized system for automatically reading 802.11 standard SSID numbers so as to identify transmitters relatively quickly and efficiently. Use of SSID is effective for identifying most transmitters. Some units that use proprietary, non-SSID communication protocols still have to be identified with manual direction-finding and door-to-door visits. (U-NII rules do not mandate SSIDs be transmitted to make it easier to identify and locate possible interference sources.)

The number of individual interference cases that have been documented at Cape Canaveral over the last few years is, to estimate from the Air Force reports, in the low hundreds. Range personnel have not been the only ones who have dealt with these cases. The FCC has repeatedly deployed technical investigatory teams into the area from offices in Tampa and Washington, DC. These teams have likewise found and documented numerous harmful interference cases.

Hotels, restaurants, apartments, condominiums, private residences, and cruise ships have all been documented as hosting interfering devices,<sup>102</sup> usually as outdoor transmitters but sometimes indoors, too. When these devices' U-NII channels are identified, they are almost always co-channel or adjacent-channel to the radar skin tracking and beacon tracking frequencies.

Observed interference distances have turned out to be completely consistent with the back-of-the-envelope calculation in this report: 10 km or more for ground-level transmitters and

---

<sup>102</sup> Many interfering 5 GHz devices once operated within base housing at Patrick AFB. A dedicated effort by the Air Force to remove them from the housing has reduced harmful interference from that source to essentially zero, according to Air Force personnel who have been involved in mitigation efforts. (*Pers. Comm.*, Mr. Scott Peterman, Air Force 45<sup>th</sup> Space Wing, Patrick AFB.)



essentially unlimited (to the edge of line-of-sight) distances for transmitters on building upper floors and rooftops.

Whenever U-NII operators have been contacted by Air Force spectrum engineers and FCC engineers tracing interference to their transmitters, they have been told to cease operations on the interfering channels. Ordinarily they do cease such operations. But as quickly as one operator abandons a channel, another operator finds the channel to be available and re-occupies it. One local WISP developed a pattern of attempting to re-use interfering channels after having been told to cease using the channels.<sup>103</sup>

Another problem with vacating interfering U-NII channels has been documented: After a power failure and subsequent re-powering, some U-NII transmitters with volatile memory do not remember the channels that were being used prior to the power failure. Instead, they re-boot on default start-up channels that were originally programmed into their firmware by their manufacturers. Operators of these devices who have vacated interfering channels are often unaware that power failures and automated re-boots have occurred. Even if they are aware of drop-outs and re-boots, they typically do not know that their devices have re-awakened on interfering channels that they had earlier vacated. These re-booted devices must then be tracked down repeatedly by spectrum engineers. The operators have to be instructed to more carefully monitor their devices for re-boots, and to monitor their devices' channel selections subsequent to those events.

#### **8.5.4 Interference Analysis**

The 5 GHz U-NII-to-RIR interference that has been documented is technically straightforward. It is mostly co-channel and sometimes adjacent-channel to the RIRs. Co-channel interference interactions are suggestive of disabled or otherwise ineffective DFS capability. Adjacent-channel interference is explained by the out-of-band (OoB) roll-offs of the U-NII transmitters putting enough power into the adjacent RIR frequencies to cause interference to the RIR receivers.

Interference to RIR receivers is easily observed by radar operators with high-quality, state-of-the-art diagnostic displays inside the radar stations. When the interference occurs it potentially endangers range safety by pulling RIR antennas (both reinforced radar beacons (most important) and skin tracking (less important but still necessary)) away from desired targets. The mechanism for being drawn off is explainable by the way that monopulse tracking works (see Appendix C and Appendix D).

As noted above, there are scenarios in which the interference effect of RIR antennas being drawn away from LVs could, in conjunction with an unrelated failure of a metric-tracking GPS beacon, cause RSOs to be forced to terminate (destroy) an LV with its payload even if the vehicle were thrusting and guiding normally.

Additional impacts of U-NII interference to the 5 GHz radars include interference to the radar calibrations that run prior to launch operations and interference to space-object observations that these radars routinely perform for a number of federal agencies. Future impacts may occur as

---

<sup>103</sup> *Pers. Comm.*, Mr. Scott Peterman, Air Force 45<sup>th</sup> Space Wing, Patrick AFB.

well on wideband-chirped pulsed radar operations for enhanced space observations. But the most serious and immediate impact of U-NII interference is on the safety and effectiveness of launch operations.

The harmful interference cases that occur due to non-detection of radar signals in the DFS-required U-NII-2C band are explainable by the DFS certification regime: DFS certification tests currently only go down to PRRs of about 300/second (as described in detail in Appendix E). But the range radars almost always use a PRR of 160/second. The current DFS certification requirement is insufficient to detect the range radars on their most-used (ordinarily the only used) PRR mode of 160/second.

The range radars have available PRRs of 160, 320, 640 and 1280 pulses per second. The higher PRRs fall within the DFS test-and-certification regime. We believe that personnel who at one time or another reviewed a database of RIR technical characteristics during the development of DFS may have imagined, when they saw PRRs as high as 1280/second, that the RIR emissions would therefore be detected by DFS-equipped U-NIIs. But the radars at the ranges must track LVs at long distances where only the lowest PRR of 160/second will suffice.<sup>104</sup> So the ranges only rarely use the higher PRRs. The ordinary use of the low PRR of 160/second prevents the RIRs from being seen by the U-NII APs. Because the commonly-used 160/second PRR was not incorporated into the test suite of radar signals provided to the FCC for use in lab testing, the devices that emerged from certification testing would not ordinarily respond to the range radars.

Interference cases have been well documented in the hundreds by range personnel and the FCC in the Cape Canaveral area alone. Similar problems have been documented at other test and rocket-launch ranges. Most U-NII operators have cooperated with efforts to keep the affected frequencies clear but a few operators have persisted in testing the situation by re-occupying channels after being told to stand down on previously identified channels.

But as quickly as one operator vacates a frequency another often occupies it (because it has become “available”). The harmful interference re-occurs co-channel to the radars. Clearly a comprehensive solution is needed for both the short term and the long term. As relates to the topic of this report, DFS, the certification testing requirement needs to be extended to include lower PRRs (down to 160 pulses per second) that are not part of the current testing regime.

The DFS experience with U-NII-2C transmitters interfering with 5 GHz RIRs reinforces Lessons Learned numbers 3 (some interference will inevitably occur), 9 (some flaws in certification testing (in this case, PRRs that are not low enough) may only be discovered after the fact), and 10 (certification testing needs to be as robust as possible). Regarding Lesson 10, this robustness must include the full range of operational parameters (e.g., all of a radar system’s available pulse repetition rates) of incumbent systems that require protection from harmful interference.

---

<sup>104</sup> With the exception of some airborne radars, radar pulses are conventionally emitted at a rate that allows each transmitted pulse to travel to the operational range limit and reflect back to the receiver before the next pulse is emitted. This conventional minimum pulse-to-pulse interval is 12.4 microseconds per nautical mile of radar range. For LVs that must be tracked at up to 500 nautical miles distance before they drop below the local horizon, the interval between pulses must therefore be at least 500 nautical miles times 12.4 microseconds per nautical mile, or 0.0062 seconds. This equates to 160 pulses per second.

## **9. ONGOING DFS SPECTRUM SHARING SUPPORT**

It should be clear at this point that DFS spectrum sharing technology is not a shoot-and-forget method. It requires ongoing support. This section summarizes that support. This need for ongoing support may turn out to be true for most complex spectrum sharing technologies.

### **9.1 Continuing Monitoring of Legal FCC-Certified DFS Devices**

As noted above, DFS-equipped systems can fail after they have been certified and field-deployed. The primary reason for such failure of properly installed and operated systems is firmware updates<sup>105</sup> that can cause DFS to be unintentionally impaired or disabled. Other than waiting for interference reports submitted to the FCC, this problem calls for ongoing spot-check monitoring of DFS-enabled U-NII devices that are for sale to the public.

At the ITS laboratory in Boulder, NTIA periodically selects, on a random basis, some 5 GHz DFS U-NIIs for such testing. The units are purchased from commercial outlets without interaction with manufacturers. The DFS testbed system in Figure 1 is used for the testing. Some of the higher-end commercial grade U-NII devices can cost more than three thousand dollars; ITS does not have funding for such purchases.

NTIA also undertakes DFS performance checks on U-NII devices that have been reported by the FAA and FCC to be causing interference to TDWR even though those units have been DFS-certified. Again, the problem has usually turned out to be new firmware loads that unintentionally affected DFS functionality. All of this work requires some ongoing support from NTIA (for the Boulder laboratory work) and from the FAA and FCC field offices (to track down interfering U-NII devices).

### **9.2 Illegal (Non-DFS-Equipped) Device Imports**

Illegally imported and operated 5 GHz transmitters, although not strictly a DFS problem, may, as noted above, be an unintended consequence of having opened the 5 GHz DFS bands for worldwide sharing. As for legal devices with problematic firmware downloads, locating and disabling these devices requires ongoing support from FAA and FCC field offices.

### **9.3 Accommodating More Complex Future Radar Waveforms**

NTIA works with other federal agencies to determine the characteristics of future radars that are being built at 5 GHz in the DFS sharing bands. If these radars should have waveforms that would call for modification of the DFS radar test bins, NTIA will alert the FCC and new test bin protocols can be published in the CFR. Keeping track of new 5 GHz radar development requires continuing, ongoing support in this area from both NTIA and FCC.

---

<sup>105</sup> Ordinarily firmware updates are authorized by manufacturers. Some unauthorized firmware files have however been provided by third parties to intentionally make devices that are FCC compliant operate in an unauthorized manner.

#### **9.4 Accommodating Changing U-NII Device Technology**

U-NII device technology will probably not remain static. As industry seeks to develop and deploy new sorts of U-NIIs, DFS rules, regulations and technology will likely need to be adapted to accommodate those changes. It remains to be seen how much difficulty will be entailed in implementing such changes.

**Lesson 11:** Some technical modifications or additions may need to be made to develop new or improved spectrum sharing technology subsequent to initial market introduction.

## 10. SUMMARY OF LESSONS LEARNED FOR FUTURE DYNAMIC SPECTRUM SHARING TECHNOLOGIES

The lessons learned for future dynamic spectrum sharing technologies developed from the 5 GHz DFS experience are summarized in this section.

**Lesson 1:** The development time for dynamic spectrum technologies, even when government and industry work closely and cooperatively together on the necessary technical and regulatory framework, can be something on the order of a decade. This is because innovation requires considerable advance work in the absence of existing implementations. The more innovative and technically challenging the new sharing scheme, the longer the advance-work timeline can be expected to be.

**Lesson 2:** The use of dynamically based spectrum sharing technologies requires permanent, ongoing government expenditures for testing facilities and maintenance of trained, competent engineering staff for permanent ongoing surveillance of such devices. This state must continue for as long as any given class of dynamic spectrum-sharing devices continues to be sold and used in markets. Dynamic spectrum sharing is associated with ongoing post-certification compliance auditing<sup>106</sup> costs. This is not to say that the expenditures are not worth the advantages that society gains from more and better spectrum sharing; it is to say that such sharing has recurring technology-opportunity costs. The need for adequate ongoing technical auditing resources needs to be recognized.

**Corollary to Lesson 2:** Technical analysis and measurements will have to be performed to assess the impact of changing U-NII device technology on incumbent federal radar systems.

**Lesson 3:** Any non-trivial, innovative, dynamic spectrum sharing technology introduction, no matter how carefully it is initially devised, may result in some elevated interference potential when it is initially deployed. The more complicated or innovative the technology, the more likely it is that some unanticipated field-deployment situation may result in an increase in the potential for interference.

**Corollary to Lesson 3:** When new, innovative dynamic spectrum sharing technologies are introduced, resources should be set aside in advance to accommodate and resolve the inevitable initial harmful interference cases that may be expected to occur.

**Lesson 4:** Post-certification compliance auditing<sup>107</sup> may be necessary to identify spectrum sharing devices that have been illegally sold without proper regulatory certification.

**Lesson 5:** If installers and operators are physically able to illegally modify spectrum sharing devices to disable spectrum-sharing features, some will do so even knowing that they will be fined by regulators when they are eventually caught.

---

<sup>106</sup> Such auditing, when done by NTIA, is done on DFS-equipped U-NII devices that NTIA purchases off-the-shelf from commercial vendors.

<sup>107</sup> Auditing, when done by NTIA, is done on devices that NTIA purchases off-the-shelf from commercial vendors.

**Corollary 1 to Lesson 5:** Manufacturers need to restrict the ability to disable or modify their devices' spectrum sharing functionality as much as is physically possible. Regulatory entities need to do thoroughly examine all of a spectrum-sharing device's set-up and control sub-menus.

**Corollary 2 to Lesson 5:** Introducing legitimate, legal spectrum sharing devices to a band can have the unintended consequence of encouraging the proliferation of illegal devices in the same band. This is especially true if the band is used worldwide for such functions, but does not have the same spectrum sharing rules internationally as the U.S. has domestically.

**Lesson 6:** There is no substitute for person-to-person interchanges of critically important design information about technical requirements and needs for spectrum sharing systems. These human interchanges (as opposed to non-human interactions such as database sharing) must be between and among multiple government agencies (including regulatory agencies and agencies operating incumbent radio systems), industry that is developing new devices, and private sector companies that will eventually buy and operate the devices.

**Lesson 7:** Development and implementation of a dedicated operational testbed might be well-advised, prior to widespread introduction of a new spectrum sharing technology. But testbeds consume time and resources to build and operate. They tend to run counter to the desire to develop and deploy new technologies as quickly and inexpensively as possible.

**Lesson 8:** Some technical spectrum sharing parameters cannot be known until after spectrum-sharing devices have been built and possibly deployed. This lack of knowledge can result in flaws in spectrum sharing device certification testing.

**Lesson 9:** Some flaws in spectrum sharing device certification testing may only be discovered after a variety (various device models marketed by numerous manufacturers) of spectrum sharing radio models have already been tested, certified, and deployed.

**Corollary to Lesson 9:** In hindsight, it would have been well advised for commercially produced 5 GHz DFS-equipped U-NII devices to have been initially introduced at a limited number of pre-identified field sites in close proximity to TDWRs (and other 5 GHz radars). Their operations at those sites could have been evaluated, with corrections to certification testing, prior to full-scale certification and deployment of such devices in open markets.

**Lesson 10:** Certification testing requirements for spectrum sharing devices need to be as technically robust as possible. Manufacturers may have concerns that some certification testing might be difficult to pass. But experience has shown that if devices are allowed to pass testing with less-than-robust protocols, their developers tend to build devices that only meet the reduced requirements. Such devices may then tend, disproportionately, to cause harmful interference to incumbent systems when they are deployed at field locations.

**Lesson 11:** Some technical modifications or additions may need to be made to develop new or improved spectrum sharing technology subsequent to initial market introduction.

## 11. REFERENCES

- [1] Chapter 4 of *Manual of Regulations and Procedures for Federal Radio Frequency Management (Redbook)*, U.S. Dept. of Commerce, September 2017 Revision of the September 2015 Edition, <https://www.ntia.doc.gov/page/2011/manual-regulations-and-procedures-federal-radio-frequency-management-redbook>
- [2] International Telecommunication Union Radio-Communication Sector (ITU-R), “Dynamic frequency selection (DFS) in wireless access systems including radio local area networks for the purpose of protecting the radiodetermination service in the 5 GHz band,” ITU-R Recommendation M.1652, Jun. 2003.
- [3] Sanders, F. H., R. L. Sole, B. L. Bedford, D. Franc and T. Pawlowitz, “Effects of Radiofrequency (RF) Interference on Radar Receivers,” NTIA Technical Report TR-06-444, U.S. Dept. of Commerce, Feb. 2006.  
<https://www.its.bldrdoc.gov/publications/details.aspx?pub=2481>
- [4] Carroll, J. E., G. A. Sanders, F. H. Sanders and R. L. Sole, “Case Study: Investigation of Interference into 5 GHz Weather Radars from Unlicensed National Information Infrastructure Devices, Part III,” NTIA Report TR-12-486, U.S. Dept. of Commerce, Jun. 2012. <http://www.its.bldrdoc.gov/publications/2677.aspx>
- [5] Carroll, J. E., F. H. Sanders, R. L. Sole, and G. A. Sanders, “Case Study: Investigation of Interference into 5 GHz Weather Radars from Unlicensed National Information Infrastructure Devices, Part I,” NTIA Report TR-11-473, U.S. Dept. of Commerce, Nov. 2010. <https://www.its.bldrdoc.gov/publications/2548.aspx>
- [6] Carroll, J. E., F. H. Sanders, R. L. Sole, and G. A. Sanders, “Case Study: Investigation of Interference into 5 GHz Weather Radars from Unlicensed National Information Infrastructure Devices, Part II,” NTIA Report TR-11-479, U.S. Dept. of Commerce, Jul. 2011. <http://www.its.bldrdoc.gov/publications/2554.aspx>
- [7] Sanders, F., “Measured Occupancy of 5850-5925 MHz and Adjacent 5-GHz Spectrum in the United States,” NTIA Report TR-00-373, U.S. Dept. of Commerce, Dec. 1999.  
<https://www.its.bldrdoc.gov/publications/2404.aspx>.
- [8] “Compliance Measurement Procedures for Unlicensed-National Information Infrastructure Devices Operating in the 5250-5350 MHz and 5470-5725 MHz Bands Incorporating Dynamic Frequency Selection,” Office of Engineering and Technology Laboratory Division, FCC, Washington, DC. April 8, 2016.  
[https://apps.fcc.gov/kdb/GetAttachment.html?id=V2DzGgztnfxjTcht59nQ7Q%3D%3D&desc=905462%20D02%20UNII%20DFS%20Compliance%20Procedures%20New%20Rules%20v02&tracking\\_number=27155](https://apps.fcc.gov/kdb/GetAttachment.html?id=V2DzGgztnfxjTcht59nQ7Q%3D%3D&desc=905462%20D02%20UNII%20DFS%20Compliance%20Procedures%20New%20Rules%20v02&tracking_number=27155).

## ACKNOWLEDGEMENTS

The work described in this report has involved dozens of people in government and industry. The authors particularly thank the following people and organizations who have participated in, assisted in, and contributed to the investigations whose results we present in this report.

FAA personnel in Washington, DC, including Mr. Mike Richmond and Mr. Bruce Williams, were instrumental in all of the work associated with TDWR interference. They alerted NTIA to initial interference problems with TDWR stations, coordinated our TDWR work in Oklahoma City and San Juan, Puerto Rico, helped to plan the work to be done to identify the interference sources and mechanisms, assisted with field investigations, worked with NTIA on data analysis, and reviewed and edited the final NTIA reports on all of that work.

FAA spectrum and engineering staff in San Juan supported us at the San Juan TDWR site. They were especially understanding in letting us partially disassemble their TDWR and having confidence in our ability to later re-assemble it without having any parts left over.

FCC field staff in San Juan, especially Mr. Reuben Jusino, without whom we would never have located a number of sites where problematic U-NIIs were operating.

FAA technical staff at the FAA Aeronautical Center in Oklahoma City, especially engineers Mr. Rajiv Gautam and Mr. Tim Pigg, and staff meteorologist Mr. Aaron Tuttle. Their assistance and insights were crucially important to analyzing the TDWR problem and developing mitigation options.

The engineering staff and management of the 45<sup>th</sup> Space Wing at Cape Canaveral provided us with extensive background information on interference at test ranges and provided us with excellent access to all facets of the radar and RSO operations at the Eastern Range, Cape Canaveral. Especially thanked are Mr. Tong Tang and Mr. Scott Peterman. The engineering and operations staff at the Eastern Range Radar 0.134, especially Mr. C.C. Harrison, also provided invaluable, outstanding information about their tracking systems.

Mr. Michael Ha of the FCC provided excellent technical background and insights on U-NII issues at the Eastern Range and Cape Canaveral areas from the Commission's perspective. Mr. Bruce Jacobs, FCC liaison to NTIA, has likewise provided much useful discussion and many good ideas about addressing issues with RIR interference.



**APPENDIX A**  
**HOW DFS DETECTION THRESHOLDS ARE COMPUTED AND WHY DFS**  
**DETECTION DOES NOT REQUIRE RADAR MAINBEAM COUPLING TO WORK**

Variables used in this Appendix, in the order that they are introduced:

$P_{rx\_radar|tx\_UNII}$  = power received by radar given UNII transmitter, dBm.

$P_{tx\_UNII}$  = output power of the U-NII transmitter, fed to the antenna, dBm.

$G_{tx\_UNII}$  = gain of the U-NII transmitter antenna, dBi.

$L_{prop, radar-UNII}$  = propagation loss between the U-NII and the radar, dB, taken as a negative number.

$G_{rx\_radar}$  = gain of the radar receiver antenna, dBi.

$P_{radar\_interf\_thresh}$  = power threshold in radar receiver that causes harmful interference, dBm/MHz.

$P_{radar\_DFS\_thresh}$  = DFS power threshold for harmful interference, same as  $P_{radar\_interf\_thresh}$ , dBm/MHz.

$k$  = Boltzmann's constant,  $1.38 \cdot 10^{-23}$  J/K = -138.6 dBm/MHz/K.

$T$  = ambient temperature, ordinarily taken to be 290 K.

$B_{radar}$  = radar receiver bandwidth, hertz.

$NF_{radar}$  = noise figure of the radar receiver, dB.

$L_{rx\_radar}$  = loss between the radar receiver RF front end and its antenna, dB.

$(I/N)_{radar\_interf\_thresh}$  = ratio of interference power to noise power that causes harmful interference in a radar receiver, linear;  $10\log$  of this quantity gives the ratio in dB.

$P_{rx\_AP\_monitor}$  = power received in the AP monitor receiver circuitry, dBm/MHz.

$P_{tx\_radar}$  = peak power produced by the radar transmitter antenna, dBm.

$G_{tx\_radar}$  = gain of the radar transmitter antenna, dBi.

$G_{rx\_UNII}$  = gain of the U-NII receiver antenna, dBi.

For a (potentially victim) radar receiver, power received from a U-NII transmitter is (working in decibel units):

$$P_{rx\_radar|tx\_UNII} = P_{tx\_UNII} + G_{tx\_UNII} + L_{prop, radar-UNII} + G_{rx\_radar} \quad (\text{A-1})$$

and

$$P_{radar\_interf\_thresh} = P_{radar\_DFS\_thresh} = 10\log(kTB_{radar}) + NF_{radar} + L_{rx\_radar} + 10\log(I/N)_{interf\_thresh} \quad (A-2)$$

For the U-NII AP DFS monitor:

$$P_{rx\_AP\_monitor} = P_{tx\_radar} + G_{tx\_radar} + L_{prop, radar-UNII} + G_{rx\_UNII}. \quad (A-3)$$

Now we solve (A-1) and (A-2) for  $L_{prop, radar-UNII}$  to obtain (A-1') and (A-2'):

$$L_{prop, radar-UNII} = P_{rx\_radar|tx\_UNII} - P_{tx\_UNII} - G_{tx\_UNII} - G_{rx\_radar} \quad (A-1')$$

and

$$L_{prop, radar-UNII} = P_{rx\_AP\_monitor} - P_{tx\_radar} - G_{tx\_radar} - G_{rx\_UNII} \quad (A-2')$$

and then we equate these two expressions for  $L_{prop}$ :

$$P_{rx\_radar|tx\_UNII} - P_{tx\_UNII} - G_{tx\_UNII} - G_{rx\_radar} = P_{rx\_AP\_monitor} - P_{tx\_radar} - G_{tx\_radar} - G_{rx\_UNII}. \quad (A-4)$$

Now solve (A-4) for  $P_{rx\_AP\_monitor}$ :

$$P_{rx\_AP\_monitor} = P_{tx\_radar} + G_{tx\_radar} + G_{rx\_UNII} + P_{rx\_radar|tx\_UNII} - P_{tx\_UNII} - G_{tx\_UNII} - G_{rx\_radar}. \quad (A-4')$$

This equation simplifies because *by reciprocity*  $G_{tx\_radar}$  always equals  $G_{rx\_radar}$  at every point in the radar antenna pattern. This is why DFS does not require radar mainbeam coupling to work. This is illustrated graphically in Figure A-1.

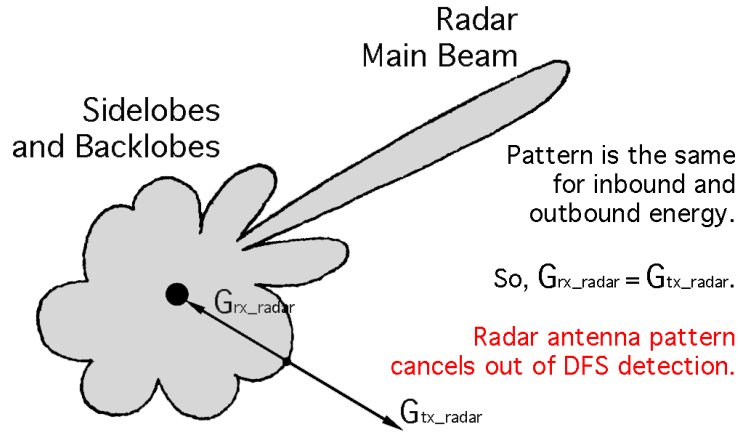


Figure A-1. Radar antenna gain subtracts out of the DFS equations via reciprocity.

So, (A-4') reduces to:

$$P_{rx\_AP\_monitor} = P_{tx\_radar} + G_{rx\_UNII} + P_{rx\_radar|tx\_UNII} - P_{tx\_UNII} - G_{tx\_UNII} \quad (A-5)$$

What is  $P_{rx\_radar|tx\_UNII}$ ? For DFS protection it is  $P_{radar\_DFS\_thresh}$  from (A-1):

$$P_{radar\_DFS\_thresh} = 10\log(kTB_{radar}) + NF_{radar} + L_{rx\_radar} + (I/N)_{radar\_interf\_thresh} \quad (A-6)$$

Typical values for these are:  $T = 290$  K;  $B_{radar} = 1$  MHz =  $10^6$  Hz;  $NF_{radar} = 1$  dB;  $L_{rx\_radar} = 1$  dB;  $10\log(I/N)_{interf\_thresh} = -6$  dB; and  $k = 1.38 \times 10^{-23}$  J/K = -138.6 dBm/MHz/K.

This gives  $P_{radar\_DFS\_thresh} = (-174$  dBm/Hz + 60 dB + 1 dB + 1 dB + (-6 dB)) = -118 dBm.

Therefore (A-5) is:

$$P_{rx\_AP\_monitor} = P_{tx\_radar} + G_{rx\_UNII} - 118 \text{ dBm} - P_{tx\_UNII} - G_{tx\_UNII}. \quad (A-5')$$

Finally, inserting values for radar and U-NII parameters as follows:

$$P_{tx\_radar} = 1 \text{ MW} = +90 \text{ dBm}; P_{tx\_UNII} = 4 \text{ W} = +36 \text{ dBm}; G_{rx\_UNII} = G_{tx\_UNII} = 0 \text{ dBi},$$

we get

$$P_{rx\_AP\_monitor} = (+90 \text{ dBm} + 0 \text{ dBi} - 118 \text{ dBm} - 36 \text{ dBm} - 0 \text{ dBi}) = -64 \text{ dBm}.$$

This level of -64 dBm is the DFS detection threshold specified by the FCC for U-NIIs with transmitter power of 200 milliwatts or more.<sup>108</sup> This calculation demonstrates the origin of the specified thresholds.<sup>109</sup>

Reviewing the terms in (A-5') for DFS detection threshold for U-NII AP monitors,

$$P_{DFS\_AP\_detect\_threshold} = P_{tx\_radar} + G_{rx\_UNII} - 118 \text{ dBm} - P_{tx\_UNII} - G_{tx\_UNII}. \quad (A-5')$$

If a U-NII uses the same antenna for transmitting and monitoring radars, then the form of (A-5') reduces to:

$$P_{DFS\_AP\_detect\_threshold} = P_{tx\_radar} - 118 \text{ dBm} - P_{tx\_UNII}. \quad (A-5'')$$

The preceding discussion shows that:

- The regulatory DFS detection threshold (e.g., -62 dBm per megahertz) is calculable from, and determined entirely by, the technical characteristics of U-NIIs and radars.

<sup>108</sup> Higher-powered U-NII transmitters have a detection threshold of -64 dBm. Full details in Table 3, “DFS Detection Thresholds for Master Devices and Client Devices with Radar Detection,” in “Compliance Measurement Procedures for Unlicensed-National Information Infrastructure Devices Operating in the 5250-5350 MHz and 5470-5725 MHz Bands Incorporating Dynamic Frequency Selection,” Office of Engineering and Technology Laboratory Division, FCC, Washington, DC.

[https://apps.fcc.gov/kdb/GetAttachment.html?id=V2DzGgztnfxjTcht59nQ7Q%3D%3D&desc=905462%20D02%20UNII%20DFS%20Compliance%20Procedures%20New%20Rules%20v02&tracking\\_number=27155](https://apps.fcc.gov/kdb/GetAttachment.html?id=V2DzGgztnfxjTcht59nQ7Q%3D%3D&desc=905462%20D02%20UNII%20DFS%20Compliance%20Procedures%20New%20Rules%20v02&tracking_number=27155)

<sup>109</sup> The final detection thresholds of -62 dBm and -64 dBm per megahertz involved negotiations and considerations that went beyond this simple calculation. The mathematical calculation shown here demonstrates the core physical principle upon which the final, negotiated detection thresholds were based.

- It is possible to incorporate all detect-and-avoid triggering in DFS-equipped U-NIIs without needing to modify incumbent radars themselves to do anything with DFS.
- Radar antenna pattern gain values *do not matter* for DFS detection. Mainbeam, sidelobe, and backlobe levels are not part of the final equation. Radio signal path reciprocity eliminates antenna characteristics and radio propagation factors from the equations and from the physical problem.
- If a U-NII uses the same antenna for monitoring radar signals as it does for transmitting data, then its antenna gain likewise drops out of the equations via reciprocity.
- The DFS detection threshold *increases* as radar transmitter peak power increases.
- The DFS detection threshold *decreases* as U-NII transmitter power increases.

**APPENDIX B**  
**TECHNICAL CHARACTERISTICS OF RANGE INSTRUMENTATION RADARS**

Table B-1 provides a summary of 5 GHz RIR parameters. Table B-2 lists RIR parameters values that are relevant to spectrum sharing. Figure B-1 shows some 5 GHz RIR locations in the U.S.

Table B-1. Technical Summary of 5 GHz RIRs<sup>110</sup>

<b>Radar Nomenclature<sup>111</sup></b>	<b>Description</b>	<b>Notes</b>
AN/FPS-16	High-precision fixed-based RIR. Magnetron oscillator transmitter tube, 1 MW peak power; 3.6 m (12 ft) diameter +44 dBi gain parabolic antenna. Beamwidth = 1.2 deg.; range resolution = 5 meters (15 ft).	Derived from 1946-50 Navy Bumblebee radar, circa 1952-55. First purpose-designed RIR/MIPIR. 52 built by RCA 1955-1969.
AN/MPS-25	Mobile (trailer modules) version of the FPS-16.	Seven built 1956-1966.
AN/FPQ-6	Upgraded version of FPS-16. Transmitter modulator feeds traveling wave tube (TWT) which drives klystron, 3 MW peak power. 8.8 m (29 ft) diameter antenna, +52 dBi gain. Beamwidth = 0.38 deg.	Five built 1958-1964.
AN/TPQ-18	Transportable (trailer modules) version of FPQ-6.	Six built 1958-1967.
FPS-105	Compact RIR.	Five built 1962-1969.
AN/MPS-36	Another mobile version of the FPS-16.	Fourteen built 1966-1973. Two units at Kwajalein.
AN/FPQ-14	Upgraded version of the FPQ-6/TPQ-18.	Unknown number.
AN/FPS-134	Version of the FPQ-14. Direct conversion of RF to IF (no LO stage) in the receiver.	Unknown number.
AN/MPS-39 (aka Multiple Object Tracking Radar (MOTR))	High power phased array using 1 MW TWT and crossed-field (CFA) amplifiers. Simultaneously tracks 40 targets; data feeds for 10 targets. +46 dBi antenna w. 1 deg. angular resolution.	Five built 1988-1994.
FPQ-17 (aka Multiple Target Instrumentation Radar (MIR))	Phased array using 150 kW TWT. Tracks up to 16 targets simultaneously.	One built.
RIR-716, RIR-778, RIR-778C RIR-980, High Accuracy Instrumentation Radar (HAIR), Remotely Operated Instrumentation and Test Radar (ROTR)	Variants of the original FPS-16 design.	Numerous, at many test range, rocket launch and space launch locations

<sup>110</sup> The AN/TPQ-39, a weather surveillance variant of the FPS-16, is not included in this table.

<sup>111</sup> “AN” in these designations originally meant Army-Navy (antecedent to 1947 creation of the U.S. Air Force). The codes that follow are from the Joint Electronics Type Designation System (JETDS). JETDS details are in Military Standards Document MIL-STD-196.

Table B-2. Typical 5 GHz RIR Technical Parameter Values Relevant to Spectrum Sharing

RIR Technical Parameter	Typical Value
5 GHz Radiolocation Band	5250-5925 MHz
Band Primary Allocation	Radiolocation
Operating Frequency Range	Mostly between 5640-5850 MHz <sup>112</sup> (210 MHz of spectrum)
Mainbeam Antenna Gain	Between +44 to +54 dBi; +52 dBi is typical.
Sidelobe and Backlobe Gain	$\cong 0$ dBi
Pulse Repetition Rates	Between 20/second to 2560/second, non-staggered. 160/second is commonly used.
Pulse Modulations	CW (P0N) for beaconing; chirped (Q3N) for skin tracking.
CW (P0N) Pulse Widths	Between 0.25 to 5 $\mu$ s; 1 $\mu$ s is commonly used.
Chirped (Q3N) Pulse Widths	Between 6 to 50 $\mu$ s.
Chirped (Q3N) Bandwidths	Between 4 MHz to 100 MHz; 5 MHz is commonly used
Future Pulse Bandwidth (Q3N) Capability for Some Units	Upgraded chirp bandwidths of 250 and 500 MHz
Polarization	Circular or linear depending on individual radar
Beam Scanning	Tracking on individual vehicles in the atmosphere or space. No wide-angle sky searching or volume scanning.

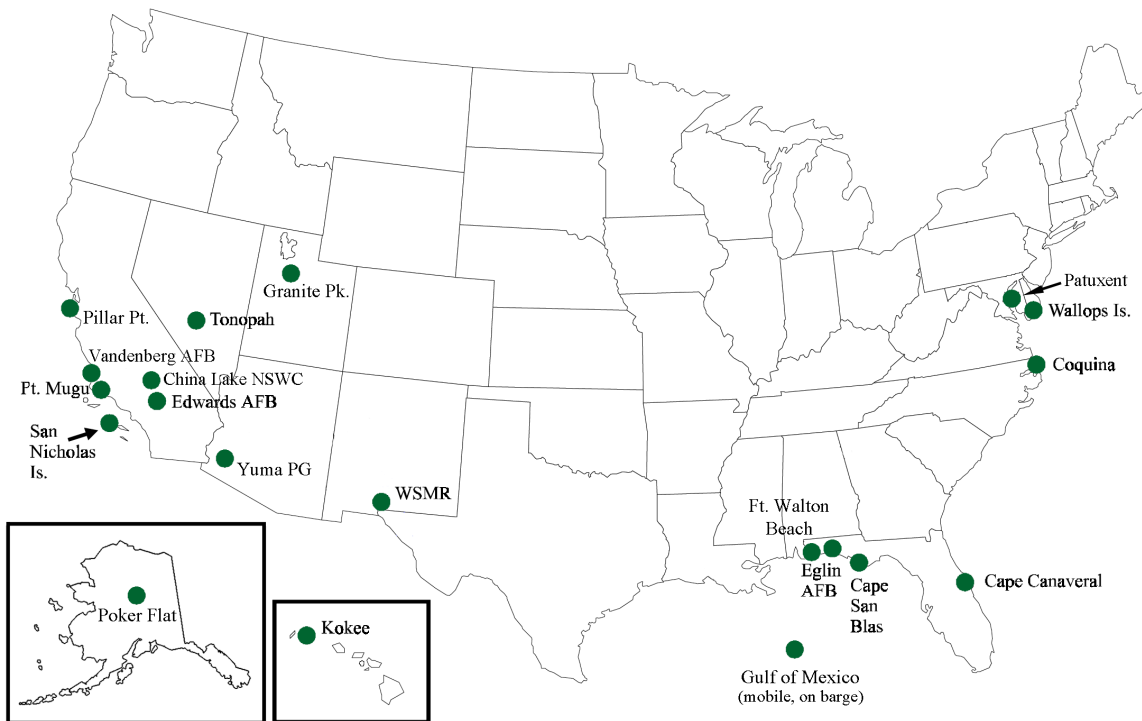


Figure B-1. Some 5 GHz RIR locations in the U.S.

<sup>112</sup> This 210 MHz is the currently allowed operational frequency range for typical 5 GHz RIRs. The available *hardware tuning range* for many of these radars is wider than this.

## APPENDIX C RANGE INSTRUMENTATION RADAR TRACKING TECHNIQUES

### C.1 Monopulse Technique for RIR Tracking

The fundamental RIR missions all involve tracking. Tracking requirements set the design parameters of these radars. Although there are a number of ways to build tracking radars, RIRs use what is arguably the best overall method. It is called single-pulse, or monopulse, technology. A diagram of a basic monopulse radar receiver, and of the antenna beam geometry necessary to make monopulse target-track processing work, is shown in Figure C-1.

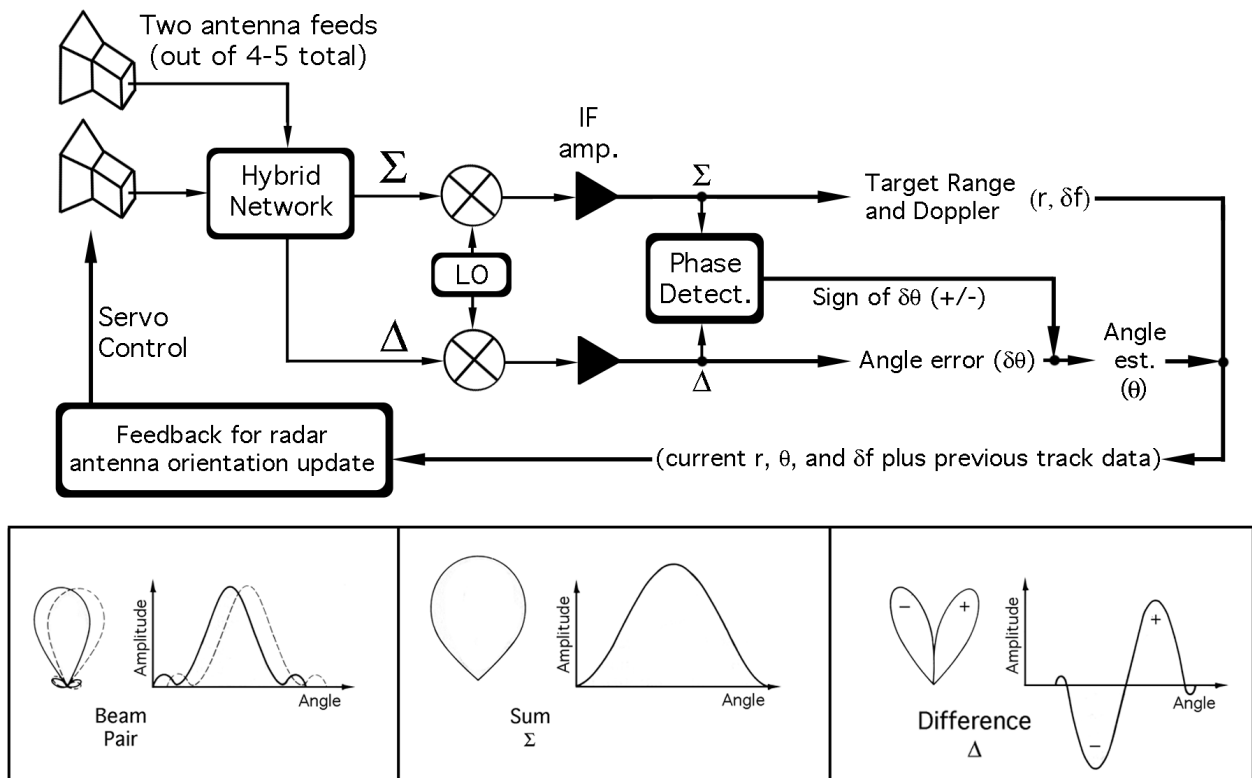


Figure C-1. Block diagram of a monopulse radar receiver including the sum-and-difference ( $\Sigma$  and  $\Delta$ ) antenna beam-feed geometry required to make it work. Radar boresight is the center-line axis of symmetry in each diagram.

To understand the monopulse process, begin by imagining a pair of microwave horns located at the focal point of a high-gain parabolic dish reflector, the feed point for the dish. Bolted together side-by-side, the horns have identical radiation patterns that are slightly laterally displaced from the center<sup>113</sup> as depicted in Figure C-1. Radar pulse echoes received by these two horns are

<sup>113</sup> The angular horn-pattern displacement shown in Figure C-1 results automatically from the fact that neither horn is exactly at the receiving dish focal point. One is a little to the left and the other a bit to the right, the focus itself being exactly in-between the two. So each horn sees the incoming plane-wave from a pulse echo at a slightly different angle relative to the wave front. Neither horn is at an exact right angle to the wave front as would be the case if either were located precisely at the dish focus.

routed into a hybrid electronic network with two inputs (one for each horn) and two outputs. The network is built so as to produce two outputs that are the angle-dependent *sum and difference* ( $\Sigma$  and  $\Delta$  in Figure C-1) *radiation patterns* of the two offset, input horn patterns. This sum-and-difference output from the hybrid circuit works on a single radar pulse echo at a time, hence the term *monopulse*.

The sum-and-difference hybrid outputs are mixed down (classically) or more often direct-digitized (nowadays) to an intermediate frequency (IF) where they are independently amplified. The *sum* IF path is used to acquire a target and to process its range and Doppler shift (equivalent to its velocity) using classic radar receiver processing techniques. This path is ineffective for determining angular information about a target's bearing because the sum lobe is angularly broad.

The IF *difference* path, in contrast, forms a sharp null. This null makes it unsuitable for acquisition, range, and velocity processing. But it is perfect for determining the (absolute) value of the *angle* between the target's true bearing and the center of the null (the radar antenna's pointing direction) with high accuracy. This *differential* between the target bearing and the radar antenna pointing direction is called the *angle error*.

It is not possible, however, to know *which side* of the null (up/down or left/right) the target is on from the difference-path output alone; only the *absolute angular distance* from the center of the null is known. To know *which direction* the angle error has moved, which is the sign (+/-) of the angle error, a separate phase-detection circuit takes in the sum and difference signals from the radar's two IF paths and outputs the side of the null on which it lies. This is the *directional sense* of the angle error. This output is based on which phase (sum or difference) leads the other.

All of these data from the radar's three output channels (range, Doppler shift, and sense-signed angle error) are fed back to a controller computer that has been pre-calibrated to know how much and in which direction to move the radar antenna via servo controllers to update the antenna pointing angle to the next place where the target should be in the sky. It implements this as a solution to a classic feedback control-loop problem.

In actual implementation, a set of four or five RF feed horns (a left-right pair, an up-down pair and perhaps a reference) are used to produce a full two-dimensional ( $\theta(t)$ ,  $\phi(t)$ ) angle-update set of outputs for the pointing-system feedback controller. (The concept is easily extended, in theory if not so easily in practice, to phased-array antenna elements.) Further, modern monopulse RIR tracking systems use stored information about a target's recent positions and velocities to augment the receiver's raw monopulse data and thus produce digital computer calculation-based predictions that give better and smoother pointing-angle updates than would otherwise have been available from monopulse outputs alone. Called Radar Open System Architecture (ROSA), this modern computer-augmented type of monopulse feedback tracking has been implemented, for example, in the FPS-134 radar.



## C.2 Monopulse Skin Tracking with RIRs at Launch Facilities

Prior to each launch support operation, each RIR is calibrated using towers located a number of kilometers from each radar station. As can be gleaned from the description of monopulse tracking given above, the monopulse technique is highly sensitive to the exact radiation pattern characteristics of the monopulse antenna feed elements, the positions and orientations of those elements relative to the dish surface, and ancillary factors such as gains and losses and phase-response characteristics of RF cabling. *The performance of a monopulse radar is no better, in other words, than the pre-flight calibration results.* This will be a factor to consider when interference is discussed below, as interference can (and does) occur during calibrations as well as during launch supports; interference-corrupted calibrations can adversely affect subsequent tracking performance.

Just before each launch, the RIR mainbeam is pivoted to the azimuth of the launch pad and is depressed to nearly zero degrees elevation angle, allowance being made for any prescribed radiation-hazard exposure cut-outs near the horizon around each station. For many RIRs, such as for example those near Cape Canaveral, this initial pre-launch beam positioning puts the mainbeams of the radars or at least their first sidelobes directly into strong RF coupling with developed town areas where potentially interfering sources are operating. This geometry is shown for example in Figure 6 for the RIR at Patrick AFB, south of Cape Canaveral.

As soon as the vehicle clears the gantry at the pad (or clears the water or separates from a carrier aircraft for submarine or airborne launches, respectively), monopulse skin tracking commences. In skin tracking, the radar's transmitted pulses (typically 4 or 5 MHz Q3N chirped modulation at a PRF of 160/second) impinge on the vehicle and are reflected (echoed) back toward the receiver. The radar receiver and associated feedback-loop control system, including ROSA, work for the rest of the flight to track the vehicle using those skin-reflected echoes.

Initially climbing vertically, vehicles headed for Earth orbit (or for the South Atlantic if they are ballistic) perform a pronounced pitch-over maneuver shortly after launch so as to start gaining horizontal velocity (ultimately about 28,000 km/hr = 17,500 mi/hr) for orbit. Radars that are located collinearly with the flight track (e.g., the three Canaveral RIRs located west of the launch pads in Figure 6) tend to have sub-optimal geometry toward the boosters as they are looking into a fairly small radar echo-return cross section (mostly the engine bells) and are seeing through dense, ionized engine exhaust gases subsequent to pitch-over. RIRs with side-looking geometry, such as the fourth radar south of Cape Canaveral in Figure 6, have better geometry for tracking since they are seeing larger side-aspect cross-sections and are not looking through exhaust gases for their echo returns. In other words, not all RIRs are equally useful for skin tracking; impairment of a single, more-useful RIR due to harmful interference can have a disproportionate effect on overall tracking accuracy.

Tracking continues until the LV drops below the RIR's local horizon. For atmospheric flight trajectories that are bound for orbit, this corresponds to a slant distance of about 900 km (500 nmi) downrange and a total tracking interval on the order of about 8–10 minutes. (A vehicle will enter orbit after about 12–15 minutes of powered flight.)

### C.3 Monopulse Beacon Tracking

Radar skin tracking suffers from the disadvantage that every transmitted pulse spreads out on an expanding spherical surface as it travels and thus spatially dissipates its energy as the square of distance traveled. Its echoes back toward the radar receiver likewise dissipate as the square of the return distance; every received radar pulse echo therefore sees an energy loss that goes as the *fourth power* of target range. In decibel terms this loss goes as  $-40\log(r)$ , where  $r$  is the target distance. An additional significant loss to radar echo returns occurs due to the cross section,  $\sigma$ , of the target, which is always less than unity and often around 0.01. For example,  $\sigma = 0.01$  gives an additional  $-20$  dB of echo-return loss in addition to the factor of  $-40\log(r)$ .

Some LVs carry a *radar beacon transponder* to improve on the performance of skin tracking. Figure C-2 shows a block diagram of such a transponder.

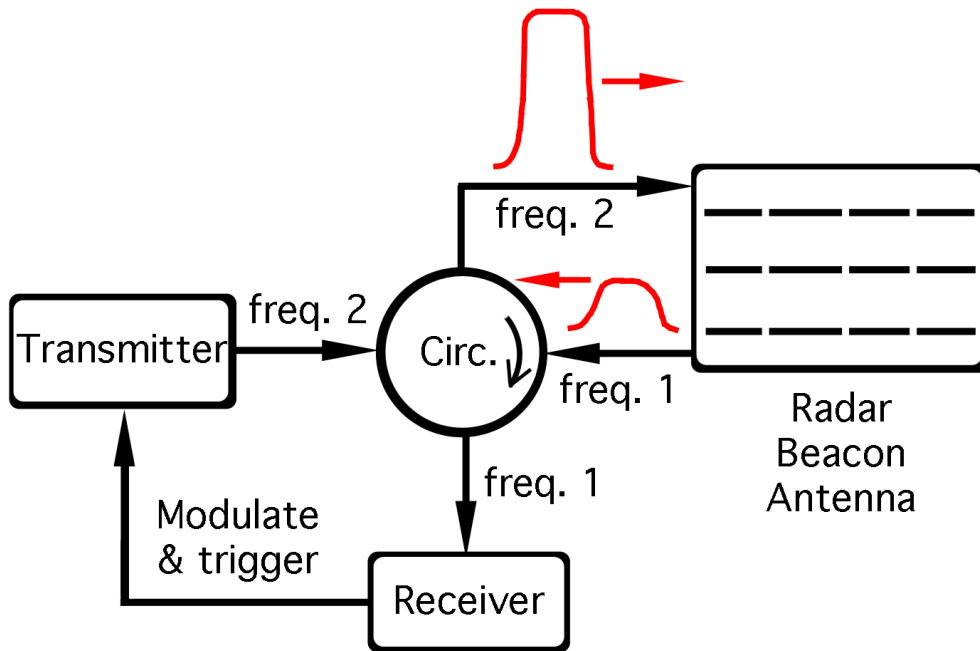


Figure C-2. Block diagram of a simple radar-pulse beacon transponder.

Although exact designs will vary from one LV to the next, Figure C-2 shows a simple design. A single conformal antenna on the LV skin with a hemispherical radiation pattern (and therefore about +3 dBi gain) is used for both transmit and receive. The antenna is connected to a four-port circulator. Radar pulses received from the RIR are routed by the circulator to a receiver. The receiver output is gated to trigger a transmitter, which itself produces high-power RF pulses. These pulses are generated on a different frequency than the received pulses but have the same pulse width, modulation, and PRR as the received pulse sequence. The transmitted pulses are routed back to the transponder antenna via the circulator. RIR beacon systems use constant-carrier (CW, PON) pulses that are around 500 ns to 1  $\mu$ s long, running at a PRR of 160/second. The separate uplink and downlink frequencies are discussed below.

The key to the beacon system's desirability compared to conventional pulse-echo skin tracking is that the transponder's on-board transmitter, running from vehicle-supplied power, significantly boosts the power of the downlink pulses relative to the strength of radar skin echoes. Additionally, the reliable directive gain factor,  $G$ , of the beacon transponder system's antenna takes the place of the variability, uncertainty, and loss of the booster's physical radar echo-return cross section  $\sigma$ .

Overall the use of the radar beacon system converts a system with a  $-40\log(r)$  round-trip signal drop-off and perhaps  $-20$  dB of cross sectional loss into a round-trip loop with just  $-20\log(r)$  loss and roughly  $+3$  dBi antenna gain in the middle. The transmit power of the beacon's return pulses is 400 watts.

In RIR receivers, monopulse tracking is performed on the beacon transponder downlink pulses in the same manner as skin-reflected echoes. The only difference is that the beacon system uses different frequencies for uplink and downlink, whereas with skin tracking the emitted and reflected energy is always on a single carrier frequency (with allowance made for Doppler shifting of the reflected pulses). The disadvantage of beaconing is that it can fail if a vehicle breaks up in flight.

#### **C.4 Metric-Tracking GPS Beaconing**

A second, independent LV beacon system is available. This system is based on reception, processing, and re-transmission of Global Positioning System (GPS) position and velocity data. Timing signals are received from GPS satellites at L-Band frequencies near 1.6 GHz; processed data are re-transmitted to ground-based receivers at the launch facility via a so-called S-Band (2–4 GHz) transmitter and body-conformal antenna. This system is called *metric-tracking GPS beaconing*.

At some launch ranges (e.g., the Eastern Range at Canaveral) most or all LVs are so equipped. Just as for monopulse beaconing, GPS beaconing can fail if a vehicle breaks up in flight. This potential failure mode creates a requirement for skin tracking, which does not depend upon any on-board systems in LVs.

## APPENDIX D INTERFERENCE FROM U-NII TRANSMITTERS TO 5 GHZ RANGE RADARS

### D.1 Effect of RF Interference on Monopulse Radar Tracking

With the 5 GHz RIR tracking system designs and operations understood (Appendix C), we move to the topic of how these radars' tracking is affected by co-channel RF interference. This description is cursory but it highlights the first and foremost effect, which is to corrupt and disrupt radar tracking channels. Consider the interference situation as drawn in Figure D-1.

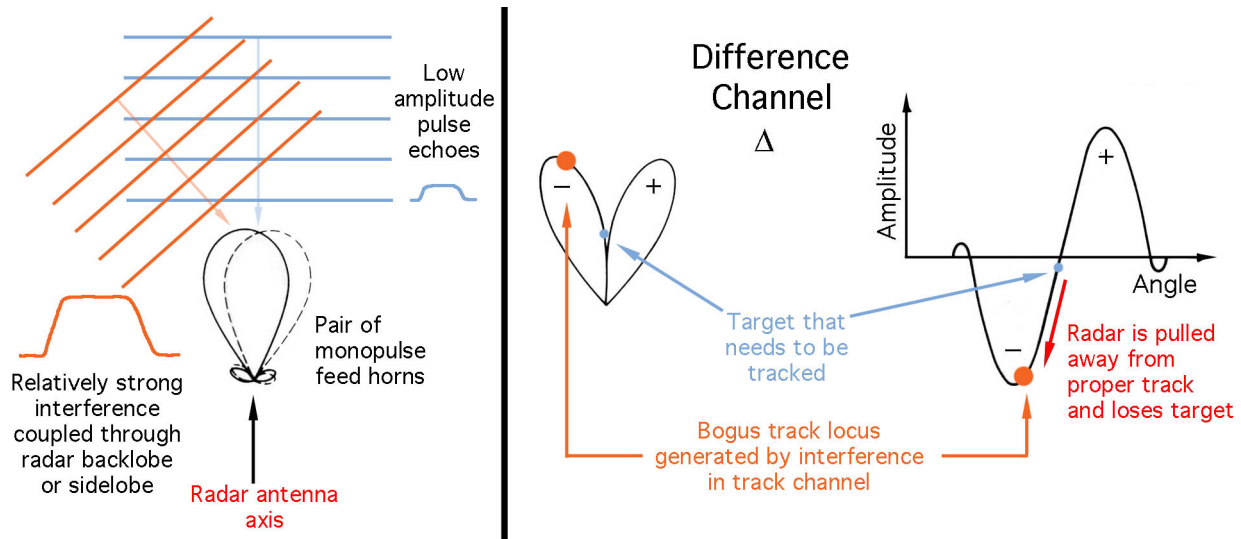


Figure D-1. Interference effect in a monopulse radar's difference (angle error) channel.

In Figure D-1 the monopulse radar initially tracks an object that is held nearly in the center of the radar's mainbeam. The object's direction is nearly collinear with the radar antenna's central axis. Then an RF interference signal couples into the radar antenna. As discussed further below, the interference will almost certainly *not* couple via the radar mainbeam; it will instead couple into the radar antenna via its backlobes or sidelobes. And so the wave front of the interference arrives at the radar's monopulse feeds from a direction that is off-axis from that of the radar antenna. When this happens, the difference channel (that is, the angle error tracking channel) in the radar receiver sees the signal from the object being followed *plus* a second, significantly off-axis signal from the interference source. If the signal power from the interference source is comparable to or stronger than the radar echo power from the tracked object, then the tracking channel may lock onto the interference signal as if *it* were the "object" being tracked. In that case the radar's track channel will be pulled off-axis, away from the actual object of interest; proper tracking will be lost.

According to Eastern Range (Cape Canaveral) radar personnel, this effect has happened and has been documented during launch operations. The quote of note is: "The radar antenna pulls away [from the target that needs to be tracked] toward the interference source."<sup>114</sup> Because skin

<sup>114</sup> *Pers. Comm.*, Mr. C. C. Harrison at Eastern Range (Cape Canaveral) range instrumentation radar number 0.134.

tracking and beacon tracking are both performed via monopulse processing, they both will be (and apparently are) affected this way.

## **D.2 Other Possible Effects of RF Interference on RIR Receivers**

The sum channel (used for target acquisition and ranging) of a monopulse radar may also be affected by RF interference. This interference would presumably cause the same sort of target-loss as has been described and documented in previous NTIA Technical Reports (e.g., [3]) for search-and-surveillance radars. Unlike search radars that only return 15–20 echo pulses from each target in each scan, RIRs expose their targets to thousands or even millions of pulses during long, continuous observations. Such long integrations may reduce target losses in these radars' sum channels. But this mitigating factor is academic if overall target tracking is lost in the first place due to the difference-channel tracking interference effect described above.

NTIA has not done interference-effects testing on wideband chirped radars. We do not know to what extent and with what effects future wideband-chirped (250-500 MHz bandwidth) RIR observations of space objects may be impacted by RF interference.

## **D.3 Interference Coupling from U-NII Transmitters to RIR Receivers**

As described in Table B-2, the RIR antenna mainbeams have gains between +44 and +54 dBi, with +52 dBi being typical. Measuring well under an angular degree wide at their 3 dB points and being aimed into the sky except at the beginnings and ends of each launch support, these beams will not usually couple directly into terrestrial interference sources.

The RIR antenna backlobes and sidelobes can and do, however, couple interference into the monopulse radar antenna feeds. An order-of-magnitude calculation follows for an estimation of how much distance would be required between a 4 watt effective isotropic radiated power (EIRP) interfering source and a RIR receiver station to avoid interference if the interference couples into the RIR via its backlobes or sidelobes.

The power received by a RIR receiver from the interference source will be:

$$P_{rx\_radar} = P_{tx\_interf} + G_{tx\_interf} + L_{prop} + G_{rx\_radar} \quad (D-1)$$

where:

$P_{rx\_radar}$  = power coupled into the radar receiver;

$P_{tx\_interf}$  = power out of the interfering transmitter;

$G_{tx\_interf}$  = antenna gain of the interfering transmitter;

$L_{prop}$  = propagation loss between the interfering transmitter and the radar receiver;

$G_{rx\_radar}$  = gain of the radar antenna in the direction of the interfering source.

The threshold for harmful interference into the radar receiver is taken to be, from previous studies, 6 dB below the radar receiver's internal thermal noise floor:

$$P_{radar\_rx\_harmful\_interf\_thresh} = 10\log(k \times T \times B_{radar\_rx}) + NF + L_{radar\_rx} - 6 \text{ dB} \quad (\text{D-2})$$

where:

$P_{radar\_rx\_harmful\_interf\_thresh}$  = threshold of harmful interference power in radar receiver

$10\log(k \times T \times B_{radar\_rx})$  = radar receiver internal thermal noise floor in bandwidth  $B_{radar\_rx}$ ;

$k$  = Boltzmann's Constant =  $1.38 \cdot 10^{-23}$  J/K = -138.6 dBm/MHz/K;

$T$  = radar receiver temperature = 290 K;

$NF$  = RIR receiver noise figure, dB;

$L_{radar\_rx}$  = other losses in radar receiver.

In (D-2) we take  $B_{radar\_rx} = (1/(1 \mu\text{s pulse width})) = 10^6$  Hz,  $NF = 8$  dB and  $L_{radar\_rx} = 3$  dB.

So our estimate for a RIR receiver interference threshold is:

$$P_{radar\_rx\_harmful\_interf\_thresh} = -174 \text{ dBm/Hz} + 60 \text{ dB} + 8 \text{ dB} + 3 \text{ dB} - 6 \text{ dB} = -109 \text{ dBm}.$$

Going back to (D-1) and inserting the value from (D-2) into it,

$$P_{rx\_radar} = -109 \text{ dBm} = P_{tx\_interf} + G_{tx\_interf} + L_{prop} + G_{rx\_radar}. \quad (\text{D-1})$$

We solve this for the value of  $L_{prop}$  that would be needed to decouple enough to avoid interference:

$$L_{prop} = -109 \text{ dBm} - P_{tx\_interf} - G_{tx\_interf} - G_{rx\_radar}. \quad (\text{D-1}')$$

Inserting some nominal values for the remaining variables,

$$(P_{tx\_interf} + G_{tx\_interf}) = 4 \text{ W} = +36 \text{ dBm in 1 MHz bandwidth (UNII-3 limit)}$$

and

$$G_{rx\_radar} = 0 \text{ dBi in backlobe/sidelobe.}$$

We get for  $L_{prop}$  (the decoupling needed to prevent interference):

$$L_{prop} = -109 \text{ dBm} - 36 \text{ dB} - 0 \text{ dBi} = -145 \text{ dB}.$$

This would correspond to a free-space separation distance of 80 km (50 mi) at 5.6 GHz.

Even if we assume 20 dB of propagation loss above free space due to clutter effects (absorption and scattering) so that we only need -125 dB of propagation loss, the required separation distance to get below the harmful interference threshold in victim RIR receivers is still 8 km (5 mi).

This calculation shows that interference sources such as U-NII transmitters with EIRPs on the order of just a few watts can cause interference to RIR receivers at distances of at least a few kilometers and sometimes (e.g., when the interferers are on rooftops) all the way to the edge of local line-of-sight coverage between the interferers and the radar stations, at distances on the order of 80 km (50 mi).

**APPENDIX E**  
**CURRENT DFS PRF CERTIFICATION TESTING LIMITS**

The FCC Office of Engineering technology (OET) has published the requirements for certification of DFS-capable devices [8]. A summary is provided here, pertaining to the requirements for pulse repetition frequencies (PRFs) of test radar waveforms, called bins.

**B.1 Radar Test Waveforms for DFS Certification**

Tables E-1 through E-4 show the waveforms used in DFS certification testing, as taken from the FCC Knowledge Database (KDB) [8].

Table E-1. DFS Certification Short Pulse Radar Test Waveforms

Radar Type	Pulse Width (μsec)	Pulse Repetition Interval (PRI) (μsec)	Number of Pulses	Minimum Percentage of Successful Detection	Minimum Number of Trials
0	1	1428	18	See Note 1	See Note 1
1	1	Test A: 15 unique PRI values randomly selected from the list of 23 PRI values in Table 5a of [8]  Test B: 15 unique PRI values randomly selected within the range of 518-3066 μsec, with a minimum increment of 1 μsec, excluding PRI values selected in Test A	Roundup:  [(1/360)* (19·10 <sup>6</sup> )]/PRI <sub>us</sub>	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
Aggregate (Radar Types 1-4)		80%		120	
<b>Note 1:</b> Short Pulse Radar Type 0 should be used for the detection bandwidth test, channel move time, and channel closing time tests.					

Table E-2. Pulse Repetition Interval Values for DFS Certification Test A

Pulse Repetition Frequency Number	Pulse Repetition Rate (PRR) (pulses per second)	Pulse Repetition Interval (microseconds)
1	1930.5	518
2	1858.7	538
3	1792.1	558



Pulse Repetition Frequency Number	Pulse Repetition Rate (PRR) (pulses per second)	Pulse Repetition Interval (microseconds)
4	1730.1	578
5	1672.2	598
6	1618.1	618
7	1567.4	638
8	1519.8	658
9	1474.9	678
10	1432.7	698
11	1392.8	718
12	1355	738
13	1319.3	758
14	1285.3	778
15	1253.1	798
16	1222.5	818
17	1193.3	838
18	1165.6	858
19	1139	878
20	1113.6	898
21	1089.3	918
22	1066.1	938
23	326.2	3066

Table E-3. DFS Certification Long Pulse Radar Test Waveforms

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

Table E-4. DFS Certification Frequency Hopping Radar Test Waveform

Radar Type	Pulse Width (µsec)	PRI (µsec)	Pulses per Hop	Hopping Rate (kHz)	Hopping Sequence Length (msec)	Minimum Percentage of Successful Detection	Minimum Number of Trials
6	1	333	9	0.333	300	70%	30

The largest PRI values in the tables correspond to the lowest PRRs. In the tables, the largest PRI values are 200-500 microseconds.

Table E-5. Largest PRIs Used in DFS Certification Testing with Corresponding PRRs

Reference Table	Largest PRIs ( $\mu\text{s}$ )	Corresponding PRRs	Notes
E-1	200-500	2000-5000/second	
E-2	3066	326/second	Lowest of all DFS-testing PRRs
E-3	1000-2000	500-1000/second	
E-4	333	3003/second	

None of the current DFS certification waveforms comes close to the 160/second PRR that is preferred for RIR operations. The closest testing waveform, 326/second from Table E-2, is used in just one set of DFS certification tests. This omission of the low PRR from DFS testing is thought to be root cause of the U-NII-2C interference to RIR receivers.

## BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION NO. TR-20-544	2. Government Accession No.	3. Recipient's Accession No.
4. TITLE AND SUBTITLE Lessons Learned from the Development and Deployment of 5 GHz Unlicensed National Information Infrastructure (U-NII) Dynamic Frequency Selection (DFS) Devices		5. Publication Date December 2019
		6. Performing Organization Code
7. AUTHOR(S) Frank H. Sanders, Edward F. Drocella, Robert L. Sole and John E. Carroll		9. Project/Task/Work Unit No.  3171012-300
8. PERFORMING ORGANIZATION NAME AND ADDRESS Institute for Telecommunication Sciences National Telecommunications & Information Administration U.S. Department of Commerce 325 Broadway Boulder, CO 80305		10. Contract/Grant Number.
		12. Type of Report and Period Covered
11. Sponsoring Organization Name and Address National Telecommunications & Information Administration Herbert C. Hoover Building 14th & Constitution Ave., NW Washington, DC 20230		
14. SUPPLEMENTARY NOTES		
15. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)  This report is a case-history of the development, deployment, and operational experiences associated with 5 GHz unlicensed national information infrastructure (U-NII) devices that incorporate a detect-and-avoid approach to spectrum sharing. Such dynamic frequency selection (DFS) technology was authorized by the Federal Communications Commission (FCC) to accommodate co-band operation of U-NII transmitters among other incumbent radio systems, specifically radars. DFS-equipped U-NII systems are designed to detect frequencies occupied by radar transmissions and then command their own transmitters to avoid operation on those occupied frequencies. Examining the historical and technical aspects of the development and deployment of 5 GHz DFS-equipped U-NIIs, this report focuses on issues encountered with the deployment of this nascent DFS technology, particularly with respect to two government radar systems that have experienced harmful interference: Terminal Doppler Weather Radars (TDWRs) and Range Instrumentation Radars (RIRs). These interference interactions and the likely underlying causes are described, along with steps that have already been taken in an effort to mitigate existing and potential future interference interactions. This report's narrative summarizes the DFS experience and shares the Lessons Learned from these experiences that may be applied to future similar spectrum-sharing approaches.		
16. Key Words (Alphabetical order, separated by semicolons) 5 GHz band; access point (AP); band sharing; detect and avoid; Dynamic Frequency Selection (DFS); electromagnetic compatibility (EMC); emission limits; out-of-band (OOB) emissions; radar; radio interference; Range Instrumentation Radar (RIR); Terminal Doppler Weather Radar (TDWR); spectrum measurement; spectrum sharing; spurious emissions; unlicensed national information infrastructure (U-NII)		
17. AVAILABILITY STATEMENT  <input checked="" type="checkbox"/> UNLIMITED.  <input type="checkbox"/> FOR OFFICIAL DISTRIBUTION.	18. Security Class. (This report)  Unclassified	20. Number of pages  108
	19. Security Class. (This page)  Unclassified	21. Price:  N/A

# **NTIA FORMAL PUBLICATION SERIES**

## **NTIA MONOGRAPH (MG)**

A scholarly, professionally oriented publication dealing with state-of-the-art research or an authoritative treatment of a broad area. Expected to have long-lasting value.

## **NTIA SPECIAL PUBLICATION (SP)**

Conference proceedings, bibliographies, selected speeches, course and instructional materials, directories, and major studies mandated by Congress.

## **NTIA REPORT (TR)**

Important contributions to existing knowledge of less breadth than a monograph, such as results of completed projects and major activities.

## **JOINT NTIA/OTHER-AGENCY REPORT (JR)**

This report receives both local NTIA and other agency review. Both agencies' logos and report series numbering appear on the cover.

## **NTIA SOFTWARE & DATA PRODUCTS (SD)**

Software such as programs, test data, and sound/video files. This series can be used to transfer technology to U.S. industry.

## **NTIA HANDBOOK (HB)**

Information pertaining to technical procedures, reference and data guides, and formal user's manuals that are expected to be pertinent for a long time.

## **NTIA TECHNICAL MEMORANDUM (TM)**

Technical information typically of less breadth than an NTIA Report. The series includes data, preliminary project results, and information for a specific, limited audience.

For information about NTIA publications, contact the NTIA/ITS Technical Publications Office at 325 Broadway, Boulder, CO, 80305 Tel. (303) 497-3572 or e-mail [ITSinfo@ntia.gov](mailto:ITSinfo@ntia.gov).