

# Software Configurations for Non-SDR Devices

Office of Engineering and Technology  
Laboratory Division



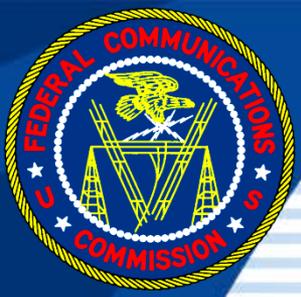
# Topics

- Software Configuration Issues for Wi-Fi Devices
- DFS Client Devices
- Modular Devices



# Compliance Considerations

- Grantee is required to ensure compliance of the approved device under all operating conditions and modes
- Many rule parts place special conditions on user access to operating parameters, for example:
  - Part 15 restrictions on user programming and access (§ 15.15)
  - Part 15 restrictions on master and client devices (§ 15.202)
  - Part 90 front panel programming restrictions (§§ 90.203(g) and 90.427 (b))
  - Part 95 restrictions (§§ 95.645 and 95.655)



# Compliance Approaches

- Grantee maintains complete control of how the parameters are configured and does not allow third party (users, installers, integrators, service centers, etc.) access to set or adjust parameters
  - *Operational description must be clear if such configurations are part of the design and how control is maintained (TCB must ask for this and review it)*
  - No user controllable or configurable software or network based software is provided
  - Alternative is to consider Software defined radio approvals



# Licensed Client Devices

- Licensed Client Devices generally operate under control of a base station or network
  - This requires the base station to control operating parameters of the device
  - Currently, it is not sufficient to rely on MCC or MNC to ensure compliance
    - It is possible to augment this type of information with additional geolocation (GPS or A-GPS) to fix country of operation
    - Such proposals are approved on a case-by-case basis



# Part 15 Client Devices

- Client devices defined under Section 15.202 may have capabilities to transmit outside the *permissible Part 15* frequencies under control of a master
- If the device is capable of transmitting within Part 15 frequencies it must comply with the applicable rules
  - Passive scanning may not be sufficient for compliance if device can transmit on Part 15 frequencies; may need some additional control to ensure compliance



# Wi-Fi Client Devices Supporting Peer – Peer communications

- Devices with Peer – Peer communications may include:
  - Ad-hoc mode of operation
  - Wi-Fi Direct: Group Owner (ie: Station GO)
  - Tunneled Direct-Link Setup (TDLS) (802.11-2012 - formerly in 802.11z)
- Such operation are permitted where the devices can meet all the requirements as a Part 15 master
- Areas where special attention must be paid:
  - Operation on Ch. 12 and 13 (Section 15.247 requirement in 2.4 GHz band)
  - Indoor operation in 5.1 GHz band (Section 15.407)
  - DFS and Radar detection requirements in 5.2 and 5.4 GHz band (Section 15.407)



# Wi-Fi Channel 12 and 13 Clients

- Passive scanning may not be sufficient for compliance, if
  - Full power operation permitted in ad-hoc or peer to peer modes including for Wi-Fi Direct and TDLS operations
- Reliance on a Master may not be sufficient if master is capable of transmitting at low power for Part 15 compliance unless there is some additional control used to operate at compliant power limits
- Issue is still under discussion to see if there are specific approaches to permit passive scanning in combination with some additional capabilities



# Wi-Fi Clients Operating in Bands Requiring DFS

- Client-to-Client communications may be permitted
  - All client devices maintain association with a master, or
  - All client devices **LISTEN** to the same master for channel information; and move channels when master announces channel move
- Wi-Fi Direct “Station GO” or TDLS group members cannot relay channel information to other devices;
  - Alternately, Group Owners need to implement DFS requirements



# Wi-Fi DFS Devices – Other requirements

- **Wi-Fi Hotspots**
  - Wi-Fi Hotspots are master devices and must have DFS with radar detection capability for operation in bands requiring DFS
- **Bridge Mode**
  - Permitted as master device (AP mode as defined in §15.403(a))
  - Application must show DFS compliance for this mode
- **Mesh Networks** – detailed Operational Description requires in application showing DFS compliance for mesh, nodes, etc.



# DFS Miscellaneous

- Streaming Method – while this is not specified the FCC prefers method is Unicast or Multicast. TCP/IP is least desirable.
- KDB Publication 905462 Updates
  - Guidance & Clarification added – references most relevant DFS KDB Publications
  - Summary Chart:
    - U-NII Rules
    - UNII Band Plan for 802.11 modes (including 802.11ac)



# Split Transmitter Modules

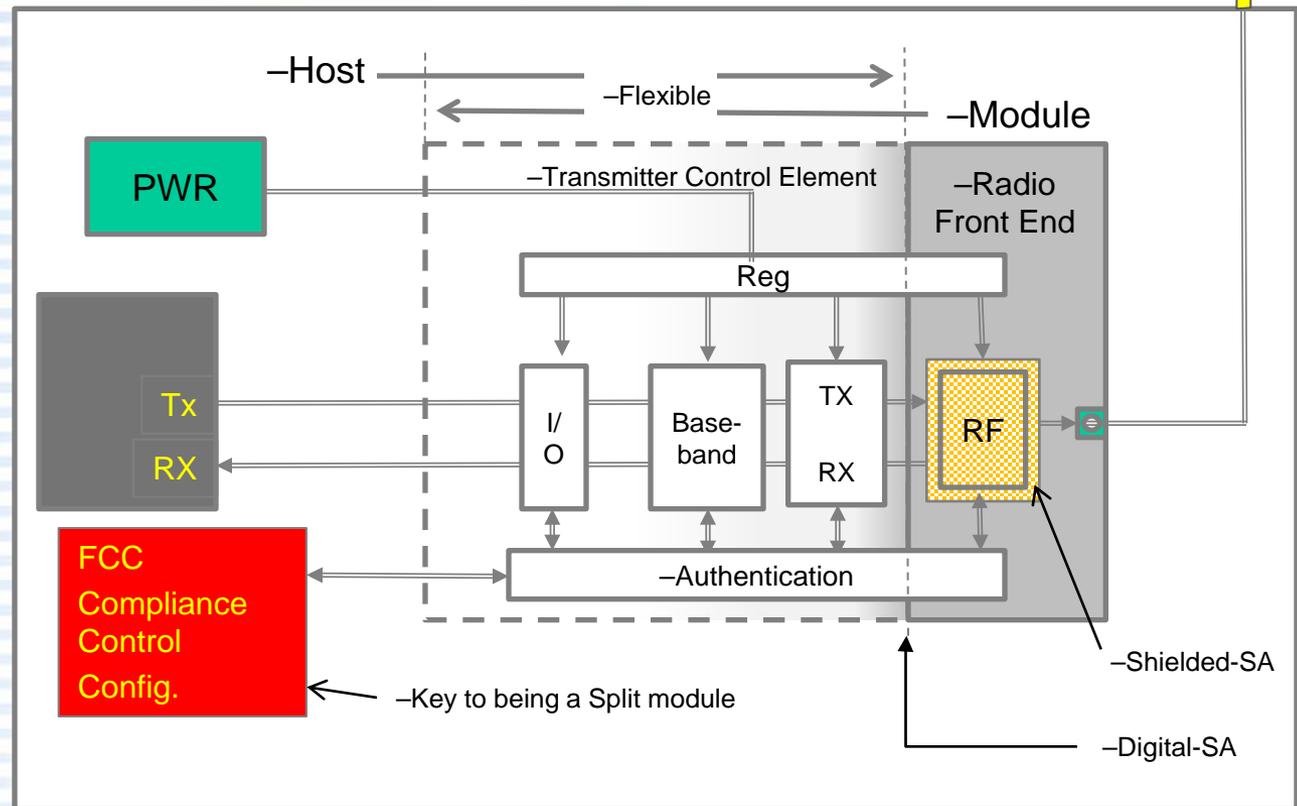
- Proposed to be move from the Exclusion List to the PBA List
- What is a Split Module?
  - Module in Two parts:
    - transmitter control elements and radio front end.
  - Radio front end must be a self-contained shielded module.
  - Transmitter control element can be integrated into the host.
  - Host Interface with module is flexible → up to the Radio Front end.



# Split Modular Transmitters

-FCC Compliance is Controlled by Hosts-  
key PBA items:

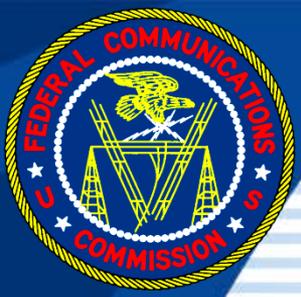
1. Configurations approved together-  
Authentication.
2. Platform similar to that intended for  
use.
3. Software Security procedure and  
description: Similar to SDR
4. Shared Responsibility.





# Plans to Update Several KDBs

- Propose to modify KDB Publication:
  - KDB 594280 (Software Configuration Control)
  - KDB 996369 (Modular Transmitter Guide)
  - KDB 905462 (DFS Test Guidance)
  - KDB 848637 (UNII Client Devices without Radar Detection or DFS)



# Questions and Answers

**Thanks!**