Software Configurations Guidance KDB 594280 - Discussion

Office of Engineering and Technology

Laboratory Division

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

Wi-Fi Channel 12 and 13 Clients

- Main concern about clients using passive scanning – need to ensure compliance under all conditions (including ad hoc and peer-peer communications modes)
  - Suggested alternative approaches to ensure compliance:
    - GNSS data, or
    - Mobile Country Code, or
    - Geo-location based on IP address
  - Other options may be considered on case by case basis

Wi-Fi Channel 12 and 13 Clients – current status

- Many comments requesting time to implement
- FCC extended time to Sept. 1, 2014
  - **Will further extend the deadline till Jan. 1, 2015 to permit considerations of other options.**

Wi-Fi Clients Operating in U-NII Bands

- KDB guidance under review in light of new rules in U-NII-1 band
  - Outdoor restriction removed for client devices
  - Guidance will be updated
- Operation in U-NII-2A and U-NII-2C bands will permit peer-peer operation under certain circumstances
  - Discussed in draft guidance
  - Will be further updated to address comments

U-NII Device Software Security Requirements

- New requirement in the rules for software security for all U-NII devices
- Currently under review - options for further guidance
  - Possibly create a new attachment specific to security in the U-NII measurement KDB
- Security guidance will apply to master and client devices
  - Will require additional information in operations description
  - For devices that operate in multiple modes as client and master additional security descriptions of mode controls, frequency selections, etc. will be required

Additional Consideration for Wi-Fi Devices in the U-NII-2 Bands

- 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.

CMRS Subscriber Devices

- Added options to permit use of MCC under certain conditions
- Require details in operations requirements
- Considerations of overlapping LTE bands and country code based selection for compliance
- Reviewing comments about test conditions and frequency of checking
- Plan to release updated guidance soon.

Modular Devices

- Challenges if functions are host dependent
  - Provided some guidance
- Most comments concerned about Wi-Fi Channel 12 and 13 operation
  - As discussed above this is under review
- Comments on MCC are also being reviewed for CMRS operation

Questions and Answers

Thanks!