|  |  |  |
| --- | --- | --- |
| Project | **IEEE 802.15 Wireless Specialty Networks Working Group <**<http://ieee802.org/15>**>** | |
| Title | **IEEE 802.15.16t System Requirements Document** | |
| Date Submitted | **2022-01-18** | |
| Source(s) | 16t Task Group | Voice:  E-mail: |
| Re: | 16t Task Group: Licensed Narrowband Amendment | |
| Abstract | System Requirements Document | |
| Purpose | To develop System Requirements for 802.16t | |
| Notice | *This document does not represent the agreed views of the IEEE 802.16 Working Group or any of its subgroups*. It represents only the views of the participants listed in the “Source(s)” field above. It is offered as a basis for discussion. It is not binding on the contributor(s), who reserve(s) the right to add, amend or withdraw material contained herein. | |
| Copyright Policy | The contributor is familiar with the IEEE-SA Copyright Policy <http://standards.ieee.org/IPR/copyrightpolicy.html>. | |
| Patent Policy | The contributor is familiar with the IEEE-SA Patent Policy and Procedures:  <<http://standards.ieee.org/guides/bylaws/sect6-7.html#6>> and <rmation is located at <<http://standards.ieee.org/board/pat/pat-material.html>> and <<http://standards.ieee.org/board/pat>>. | |

IEEE 802.16t System Requirements Document

January 18, 2022

## Introduction

This document is to summarize the performance requirements for IEEE 802.16 operation in channel bandwidths greater than or equal to 5 kHz and less than 100 kHz. This SRD will act as a guide for the development of an amendment to IEEE Std 802.16-2017. This amendment builds on the 802.16s Amendment completed in 2017 and incorporated in the revision IEEE Std 802.16-2017

The following terminology is used in this document:

SHALL: This word, or the terms "REQUIRED" or "MUST", mean an absolute requirement of the specification.

Note that the word WILL shall not be used when stating mandatory requirements; WILL is only used in statements of fact.

SHALL NOT: This phrase means an absolute prohibition of the specification.

SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

MAY: This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

# Markets and Use Cases

Markets and use cases were identified in IEEE [802.15-20-0213r13](https://mentor.ieee.org/802.15/dcn/20/15-20-0213-13-016t-ieee-802-16t-use-cases.xlsx) (or subsequent revision)

Some example markets include agriculture, drones, electric, water, and gas utilities, fleet management, oil/gas, manufacturing, rail, transportation, smart city, wastewater, environmental monitoring, and flood control.

The standard should support this set of use cases for field area networks, and similar critical infrastructure industry applications, that require high reliability and availability.

## 802.16t Amendment Requirements

Amendment Requirements that must be specified in the amendment in order to meet the operational requirements. These requirements identify the gaps in the existing standard that must be addressed by the amendment in order to attain those capabilities.

**Topology:**

Support of the following topologies is required:

Network topology:

Multicell and multisector,

Direct peer to peer with no base station infrastructure

Sector topology: Point to Multipoint

Repeater for range extension:

S&F on the same carrier frequency/carrier frequency pair

Use of distinct carrier frequency/carrier frequency pair.

Base Station Controller (BSC) for:

Seamless handover

Coordination of base station operation to minimize self-interference.

A Base Station to Base Station Controller communication protocol to support the above functions will be standardized.

Consider impact of PTT one-way LMR on topology.

**Frequency Range**

While the IEEE 802.16t amendment does not require or exclude support for any specific frequency, the majority of bands used for the IEEEE 802.16t air interface protocol will be in the sub 1 GHz frequency range.

**Band Support Requirements**

See [IEEE 802.15-20-0055-04-016t-frequency-band-layout.xls](https://mentor.ieee.org/802.15/dcn/20/15-20-0055-03-016t-frequency-band-layout.xlsx)

* Support operation in paired and unpaired continuous licensed bands available for private networks is required (e.g., AMTS, IVDS, 454 A2G, 700 MHz A-Block, RR 900 MHz, 1.4 GHz).
* Support for partition of continuous licensed bands into multiple channels is required for frequency reuse and link budget/coverage considerations.
* Support operation in Private Land Mobile Radio (PLMR) bands (e.g., RR160 MHz) is required. This includes:
* Support of common PLMR channel bandwidth: 6.25, 12.5, 25 and 50 kHz
* Support special PLMR channel bandwidth: 5, 7.5 and 15 kHz
* Support aggregation of multiple adjacent and non-adjacent PLMR channels to enable higher throughput services.

**Channel BW Range**

From PAR: “The amendment defines operation for channel bandwidths greater than or equal to 5 kHz and less than 100 kHz.”

Operation above 100 kHz is already supported and will not be changed in this amendment.

* The specification will support simultaneous remote operation over one or more aggregated (adjacent or non-adjacent) subchannels of bandwidth as low as 5 kHz.
* The specification will support base station operation over any one or more sub-channels. The base station may support aggregation of multiple subchannels such that the total bandwidth in the sector is not limited to 100 KHz.

**Duplexing Requirements**

* The standard shall support TDD.
* TDD shall be used in unpaired spectrum. TDD may be used in paired spectrum if allowed by the applicable regulation authority.
* The standard shall support FDD.
* HD-FDD or FDD shall be used in paired spectrum if TDD is not allowed. HD-FDD shall use the same framing as in TDD.
* For TDD and HD-FDD, DL:UL ratio of at least 1:10 to 10:1 shall be supported.
* Hybrid duplexing shall be supported, where a remote may operate in HD-FDD while connected to a base station operating FDD.

Note: This is done for the purpose of reducing complexity in remotes due to small duplexer gap.

**TDD Frame Configuration**

The standard shall support configurable TDD frame configuration including:

* The Configuration of the downlink subframe duration
* The Configuration of the uplink subframe duration
* The duration of the transmit to receive and the receive to transmit gap durations.

The standard shall support a range of TDD frame durations consistent with throughput, latency, frequency utilization and overhead requirements defined in this document.

The standard shall support a range of downlink to uplink subframe duration ratios between 10:1 to 1:10. The ratio will be constrained by the frame duration and the minimum capacity of the downlink/uplink subframe.

The gaps duration should support the maximum distance requirement defined in this document.

**Mobility Requirements**

The standard shall support a relative speed of remote to base station of up to 614 mph.

The standard shall support seamless handover between base stations.

**Data transport requirements:**

The standard will support concurrent operation of low, medium, and high throughput endpoint devices with the following characteristics:

* Low- throughput end point requirements:
* End user throughput < 1 kb/s.   
  Note: Given the periodicity characteristics, this seems to be a peak throughput, not average.
* End to end latency: in most cases, not time sensitive. One use case requires end to end latency < 100 msec. Other use cases require end to end latency below 1 second or higher.
* Number of endpoints per base station: up to 150[[1]](#endnote-2)
* Most use cases in this category are fixed but some are mobile.
* Most use cases in this category are reverse asymmetrical but some are symmetrical, and some are asymmetrical. UL:DL ratio is in the range 90:10 to 10:90.
* Medium- throughput end point requirements:
* 1 kb/s < end user throughput < 10 kb/s
* End to end latency < 60 ms
* End to end jitter < 20 ms
* Number of end points per sector < 60
* Fixed and mobile use cases. Some of the use cases, require high speed support.
* UL:DL ratio in the range 90:10 to 30:70
* High- throughput use cases characteristics.
* The amendment will support endpoint applications requiring up to 100 kb/s.
* End to end latency for high throughput applications < 20 ms (or subsequent revision)

Specific use cases are summarized in IEEE [802.15-20-0213r13](https://mentor.ieee.org/802.15/dcn/20/15-20-0213-13-016t-ieee-802-16t-use-cases.xlsx) (or subsequent revision)

Figure 1 presents the use cases where all data is available for user throughput vs. latency vs. number of end points per sector. The use case IDs in the scatter plot are the same as the ones used in the use cases document.

**Additional general data transport requirements for operation in narrow channel bandwidths:**

* Frequency utilization: Spectral efficiency [[2]](#footnote-2)of higher than 4 bits/sec/Hz is an objective, but some modes of operation may trade off spectral efficiency for range or lower complexity.
* Air interface protocol overhead goals:
  + PHY layer excluding FEC: < 10%
  + MAC overhead: < 10%



Figure 1 - User Throughput vs Latency for use case groups

**Predictable Performance:**

* Licensed band (mandated by the PAR)
* Central scheduling[[3]](#footnote-3)
* QOS

**Range (DL or UL) and Coverage Requirements:**

A base station to remote range of up to 200 miles will be supported subject to link budget constraints.

**Advanced Antenna Systems:**

The standard will continue to support beam steering with one or multiple beams per base station.

**Coexistence with PLMR channels operating with other standards**

It is desirable to support coexistence of voice and data in low utilization voice channels referred to as “grey channels.” This capability would require a mechanism to avoid channel contention and may result in additional RF requirements for the 16t system.

**Cyber Security**

The requirements listed below will conform to the air interface protocol requirements in mission critical security standards including IEC-62443, CIP 005-5, DO-377 SER-08 and FIPS 140-3

1. The air interface protocol shall support the following options for data encryption/decryption algorithms and key sizes (amendment to 802.16-2017, section 7.5.1):

|  |  |  |  |
| --- | --- | --- | --- |
| Algorithm | Mode | key length | Reference in 802.16-2017 |
| AES (NIST.FIPS.197) | CBC (NIST.SP.800-38A) | 128, 192, 256 | Add to 802.16 |
|  | CCM / CTR (NIST.SP.800-38C) | 128,  Add: 192, 256 | 7.5.1.2, 7. 5.1.3 |
|  | GCM (NIST.SP.800-38D) | 128, 192, 256 | Add to 802.16 |
|  | XTS-AES (NIST.SP.800-38E) | 128,  Add: 192, 256 | Add to 802.16 |
|  | CBC with key wrapping (NIST.SP.800-38F) | 128, 192, 256 | 7.5.1.4 |
| DES | Remove option |  | 7.5.1.1 |

1. The air interface protocol shall support the following algorithms options for TEK encryption (amendment to 802.16-2017, section 7.5.2)

|  |  |  |  |
| --- | --- | --- | --- |
| Algorithm | Mode | key length | Reference in 802.16-2017 |
| TDEA (3-DES)  NIST.SP.800-67r2 | CBC (NIST.SP.800-38A/F)  Disallowed after 2023 | 128 | 7.5.2.1 |
| RSA |  | 1024  Add: 2048, 4096 | 7.5.2.2 |
| AES (NIST.FIPS.197) | ECB (NIST.SP.800-38A) | 128,  Add: 192, 256 | 7.5.2.3 |
|  | CBC with key wrapping (NIST.SP.800-38F) | 128, 192, 256 | 7.5.2.4 |

1. The air interface protocol shall support HMAC authentication with 112 bits key length or higher. HMAC (amendment to 802.16-2017, section 7.5.3) shall be calculated using SHA-2 (NIST.FIPS.180-4) or SHA-3 (NIST.FIPS.202) with key length ≥224
2. The air interface protocol shall support CMAC-AES or GMAC-AES for message authentication.
3. The air interface protocol shall support the following public key encryption/decryption algorithm options for AK encryption (amendment to 802.16-2017, section 7.5.8):

|  |  |  |
| --- | --- | --- |
| Algorithm | Key length | Reference in 802.16-2017 |
| RSA | Remove: 1024,  Add: 2048, 4096 | 7.5.8 |
| ECC | 224 or higher | Add to protocol |

1. Key management: the air interface protocol shall support PKMv2 (amendment to 802.16-2017, section 7.2.2). It will not support PKMv1 only (amendment to 802.16-2017, section 7.2.1)
2. Authentication mode (amendment to 802.16-2017, section 7.8.2): mutual authentication mode will be used. The base station shall send its X.509 certificate in the Authorization Reply message.

**Glossary**

|  |  |  |
| --- | --- | --- |
| **ACRONYMS** | **Acronym Expansion** | **Definition** |
| AES | Advanced Encryption Standard | A U.S. government approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information.  SOURCE: FIPS 197 |
| AMTS | Automated Maritime Telecommunications System | A commercial mobile radio service in the USA. It offers voice and data communications to maritime customers. |
| BSC | Base Station Controller |  |
| BW | Bandwidth |  |
| CIP 005-5 | Critical Infrastructure Protection 005-5 | An electronic security perimeter around cyber assets. |
| DES | Data Encryption Standard | A symmetric block cipher algorithm for the encryption of digital data. |
| DL | Downlink |  |
| ECC | Elliptic-curve cryptography | Asymmetric public key cryptographic methods used for authentication and encryption |
| FDD | Frequency Division Duplex | FDD refers to a duplexing scheme where uplink and downlink are separated by a different frequency channel |
| FIPS 140-3 | Federal Information Processing Standard 140-3 | Security requirements for cryptographic modules. |
| HMAC | Hash-based message authentication code | A message authentication code with cryptographic hash function and a secret cryptographic key. |
| IEC-62443 | International Electrotechnical Commission-62443 | A set of security standards used to defend industrial networks from cyber threats. |
| IEEE | Institute of Electrical and Electronics Engineers |  |
| IVDS | Interactive Video Data Service |  |
| LMR | Land Mobile Radio | A push-to-talk system for mission critical voice communication. |
| PAR | Project Authorization Request | IEEE SA document for starting a standards project |
| PLMR | Private Land Mobile Radio |  |
| PTT | Push-to-Talk |  |
| QOS | Quality of Service |  |
| RR | Railroad |  |
| RSA | Rivest–Shamir–Adleman | An asymmetric public key signature algorithm that may also be used for encryption and decryption. |
| SDD | System Description Document |  |
| SDU | Service Data Unit | Packets passed from an OSI layer to a lower layer. |
| SHA | Security Hash Algorithm | A family of cryptographic hash functions. |
| SRD | System Requirements Document |  |
| TDD | Time Division Duplex | TDD refers to a duplexing scheme where uplink and downlink are separated by allocation of different time slots in a same frequency band. |
| UL | Uplink |  |

1. The number of endpoints per base station depends on the base station coverage which may be increased to reduce infrastructure cost. [↑](#endnote-ref-2)
2. Frequency utilization is the user data throughput including Service Data Unit (SDU) protocol overhead divided by the occupied bandwidth. The occupied bandwidth is the maximum bandwidth allowed for use by the applicable regulatory body within the nominal channel bandwidth. [↑](#footnote-ref-2)
3. This may not be applicable to a direct peer to peer link with no base station infrastructure. [↑](#footnote-ref-3)