

**Please note that Cypress is an Infineon Technologies Company.**

The document following this cover page is marked as “Cypress” document as this is the company that originally developed the product. Please note that Infineon will continue to offer the product to new and existing customers as part of the Infineon product portfolio.

**Continuity of document content**

The fact that Infineon offers the following product as part of the Infineon product portfolio does not lead to any changes to this document. Future revisions will occur when appropriate, and any changes will be set out on the document history page.

**Continuity of ordering part numbers**

Infineon continues to support existing part numbers. Please continue to use the ordering part numbers listed in the datasheet for ordering.



THIS SPEC IS OBSOLETE

**Spec No:** 001-15083

**Spec Title:** WIRELESSUSB(TM) 2-WAY HID SYSTEMS -  
AN4003

**Replaced by:** NONE

## AN4003

### WirelessUSB™ 2-Way HID Systems

**Author:** Sai Prashanth Chinnapalli

**Associated Project:** No

**Associated Part Family:** WirelessUSB

**Software Version:** NA

**Related Application Notes:** None

To get the latest version of this application note, or the associated project file, please visit <http://www.cypress.com/go/AN4003>.

The WirelessUSB™ 2-Way Human Interface Device (HID) protocol is designed for reliable 2-Way communication between a wireless bridge and target HID applications in 1:1 (one HID and one bridge) and 2:1 (two HID's and one bridge) systems. The WirelessUSB 2-Way HID protocol allows HID applications to establish a connection to the bridge and receive ACK, NAK and DATA packets from the bridge.

### Contents

WirelessUSB 2-Way HID Protocol Overview.....	1
Radio Channel Management.....	1
Pseudo-noise Codes .....	2
Chip Error Correction .....	2
Network ID.....	3
Manufacturing ID.....	3
Network Checksum Seed (NCS) .....	3
Bit Error Correction.....	3
Channel Selection Algorithm .....	4
Protocol Modes .....	4
Packet Structures .....	10
Summary.....	12
Appendix A: Complete WirelessUSB 2-Way HID State Machine.....	13
Appendix B: Complete WirelessUSB 2-Way Bridge State Machine.....	14
Appendix C: Sequence Diagrams .....	15
PING Sequence .....	15
Connect Sequence.....	16
BIND Sequence.....	17
Interference Avoidance Sequence .....	18
Worldwide Sales and Design Support.....	20

### WirelessUSB 2-Way HID Protocol Overview

The 2-way HID protocol will ensure that the packets that are transmitted from keyboard and mouse reach the bridge safely and reliably. The host PC is not aware of the wireless connection, since the interface to the host acts like a normal wired USB HID connection. Therefore, there is no special software required on the host PC in order to support WirelessUSB. WirelessUSB 2-Way devices all contain a WirelessUSB transceiver, as opposed to the WirelessUSB transmitter used in WirelessUSB 1-way HID devices.

### Radio Channel Management

WirelessUSB utilizes the unlicensed 2.4 GHz Industrial, Scientific, and Medical (ISM) band for wireless connectivity. WirelessUSB splits the band into 78 distinct frequency channels. Subsets of 13 channels are used by each network to minimize the probability of interference from other WirelessUSB systems (see the Channel Selection Algorithm section for more details). A designated channel subset is used during Bind Mode (along with an associated pseudo-noise code) in order to enable all WirelessUSB devices to effectively communicate during this procedure.

Host PC or Laptop

USB

WirelessUSB Bridge (Transceiver)

WirelessUSB Keyboard (Transceiver)

WirelessUSB Mouse (Transceiver)

Pseudo-noise codes (PN codes) are the codes used to achieve the special matched filter characteristics of DSSS communication. Certain codes referred to as Gold codes are used for WirelessUSB 2-Way communication. These codes have minimal cross-correlation properties, meaning they are less susceptible to interference caused by overlapping transmissions on the same channel. The length of the PN code results in different communication characteristics. Higher data rates are achieved with 32-chips/bit PN codes, while 64chips/bit PN codes allow longer range. The number of frequency/code pairs is large enough to comfortably accommodate hundreds of WirelessUSB devices in the same space. Each bridge/HID pair must use the same PN code and channel in order to communicate.

In the presence of interference (or near the limits of range), the transmitted PN code will often be received with some PN-code chips corrupted. DSSS receivers use a data correlator to decode the incoming data stream. If the number of chip errors is less than the correlator error threshold, the data will be correctly received. Figure 2 shows a WirelessUSB 64chips/bit PN code example.

## Chip Error Correction



## Network ID

The Network ID contains the parameters for the Channel Selection Algorithm as well as the PN code to be used. Bridges typically store their Network IDs in nonvolatile memory. HID's retrieve the Network ID from the bridge during the Bind Procedure. A special Network ID is reserved for Bind Mode, known as the Bind ID. The Bind ID gives a common channel subset so that any two devices can communicate with each other during Bind Mode. The Network ID is composed of the following fields:

- PIN – This is a random number used in the Channel Selection Algorithm to determine the ordering of channels within the channel subset.
- Base Channel – This is the first channel to be used in the channel selection algorithm, which determines which channels are contained in the channel subset.
- PN Code – This is the PN code to be used.

## Manufacturing ID

Each WirelessUSB radio contains a 4-byte manufacturing ID, which has been laser fused into registers 0x3C–0x3F during manufacturing. The bridge uses its Manufacturing ID to help randomize channel subsets, PN codes and checksum seeds. HID's also send their Manufacturing ID to the bridge when binding and connecting. The bridge stores the HID's Manufacturing ID in non-volatile memory after binding, allowing the bridge to verify the identity of the HID when establishing a connection.

## Network Checksum Seed (NCS)

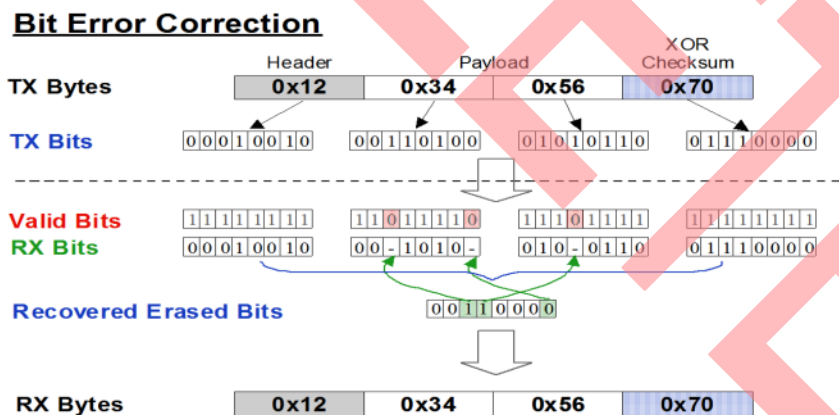
The Network Checksum Seed allows more WirelessUSB systems to be co-located. The Network Checksum Seed is determined by the bridge and sent to HID during the bind procedure. The Network Checksum Seed is then XORed with each data byte (See Bit Error Correction.) when determining the checksum value for all multi-byte packets sent between bound devices (Connect Request, DATA and ACK/DATA packets). All packets sent between non-bound devices use the default checksum seed of 0x00.

## Bit Error Correction

If the correlator threshold is exceeded, the received data bit is not corrupted; it is “erased,” or in other words invalid. There is a negligible probability of data being corrupted rather than erased, because this would require interference to corrupt the majority of chips in such a way that the incoming data stream correlated with the PN code corresponding to the opposite logic state.

Erasures are much easier to correct than errors. By XORing each data byte and the Network Checksum Seed (see the Network Checksum Seed (NCS) section for more details), and transmitting the resulting checksum as the last byte of each packet, it is possible to use this checksum to correct one error in each bit position in a received packet (see Figure 3). It is therefore possible for WirelessUSB systems to successfully receive data without error on frequencies suffering from interference causing chip error rates in excess of 10%.

Figure 3. Bit Error Correction



## Channel Selection Algorithm

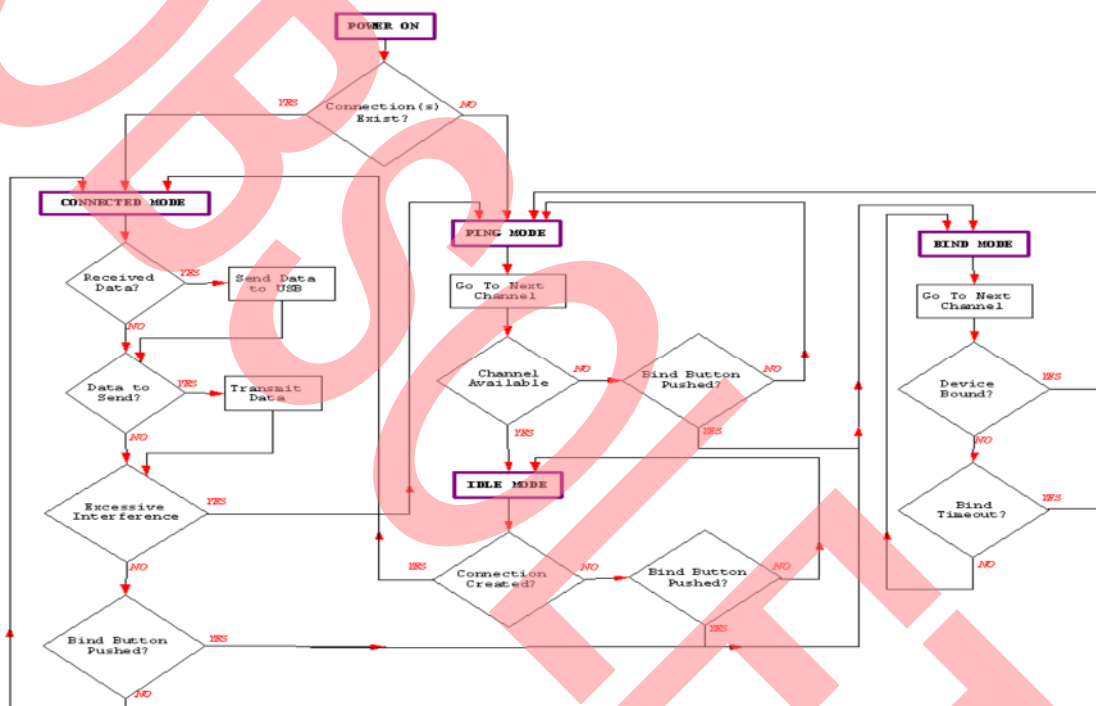
The channel selection algorithm produces a subset containing 13 of the possible 78 channels. The channel selection algorithm is based on the Network ID, with each channel in the subset six MHz from the nearest neighboring channels in the subset. This algorithm reduces the possibility of multiple bridges selecting the same channels in the same order at the same time.

## Protocol Modes

### HID

WirelessUSB HIDs operate in one of five modes. Figure 4 shows a simplified WirelessUSB HID state machine showing all modes except for Sleep Mode. For the complete state machine please refer to Appendix A: Complete WirelessUSB 2-Way HID State Machine.

Figure 4. Simplified WirelessUSB 2-Way HID State Machine



## Bridge

WirelessUSB bridges operate in one of four modes. Figure 5 shows a simplified WirelessUSB bridge state machine. For the complete state machine please refer to Appendix B: Complete WirelessUSB 2-Way Bridge State Machine.

### Ping Mode (Bridge only)

Ping Mode is used by the bridge to find an available channel; channels are unavailable if they are being used by another network with the same PN code, or if there is excessive noise on the channel. The bridge first listens for activity on the selected channel. If the channel is inactive the bridge alternately transmits Pings and listens for Ping Responses for a defined <sup>[1]</sup> period of time. During Ping Mode the bridge also checks the receive signal strength indicator (RSSI) of the radio in order to determine if a non-WirelessUSB device is using this channel (or a WirelessUSB device on the same channel using a different PN code). If a Ping Response is received, indicating that another bridge is using this channel the bridge will select the next channel using the channel selection algorithm and repeat this procedure. The bridge selects another channel using the channel selection algorithm if the RSSI is high, which indicates that there is a lot of traffic on the channel. If a Ping Response is not received and the RSSI is low, the bridge assumes the channel is available and moves to Idle Mode. Bridges send Ping Responses in response to all received Pings if the bridge is in Idle or Connected Mode. HIDs never respond to Pings.

---

<sup>1</sup> The timeout values are configurable.

Figure 5. Simplified WirelessUSB 2-Way Bridge State Machine

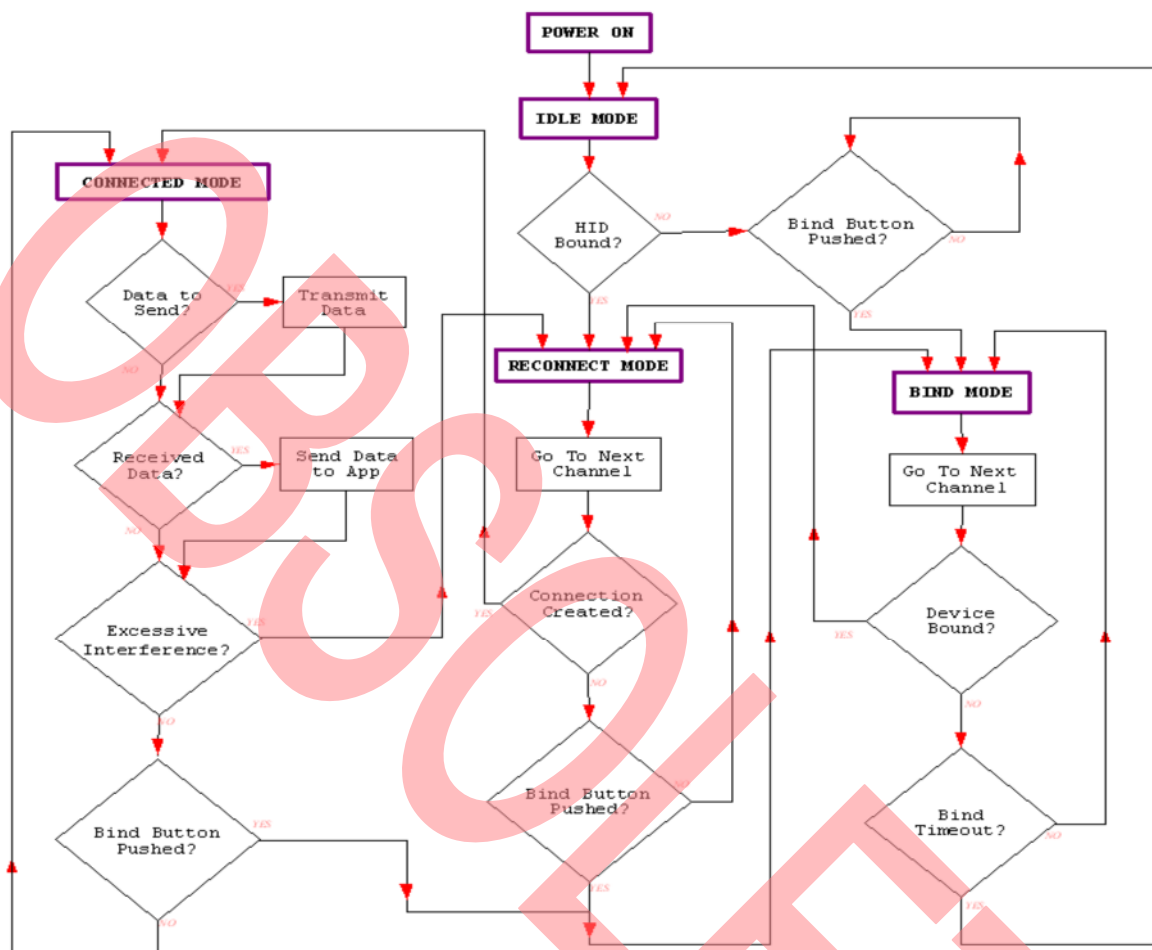




Figure 6. Ping Sequence Diagram

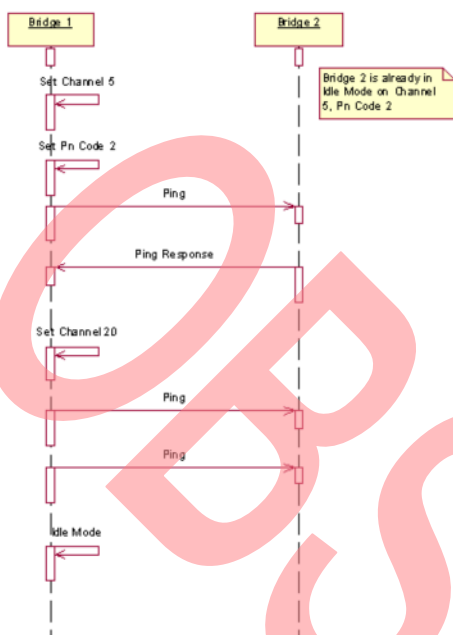
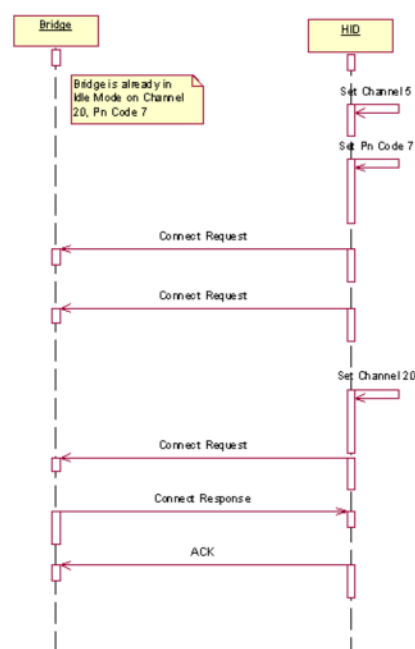


Figure 7. Connect Sequence Diagram



## Idle Mode

### HID

This is the state of a HID at power-up before it has had any communication with the WirelessUSB bridge. If the Network ID is stored in nonvolatile memory the HID retrieves the Network ID and move to Reconnect Mode. If the Network ID is not stored in nonvolatile memory the HID will wait in Idle Mode until a user-initiated event causes the HID to enter Bind Mode. After a defined period of time in Init Mode the HID enters Sleep Mode in order to conserve power. When the HID wakes up due to a user action, it reenters Idle Mode.

### Bridge

In Idle Mode the bridge waits for a connection to be initiated by the HID. If a bridge receives a Connect Request containing its Network ID and a Manufacturing ID of a bound HID, it sends a positive Connect Response to the HID, and moves to Connected Mode. If the bridge receives DATA packets or ACKs while in Idle Mode it assumes the channel is being used by another network and moves to Ping Mode in order to find an available channel. If a bridge receives a Ping Request from another bridge it will respond with a Ping Response to notify the other bridge that the channel is unavailable.

## Reconnect Mode (HID only)

Reconnect Mode is used by the HID to discover the current channel used by the bridge and to establish a connection with the bridge. Upon entering Reconnect Mode the HID uses the Network ID to select a channel using the channel selection algorithm. The HID alternately transmits Connect Requests containing the HID's Manufacturing ID and the Network ID of the desired bridge and listens for a Connect Response. If a bridge in Idle Mode or Connected Mode receives a Connect Request containing its Network ID and the Manufacturing ID of a bound HID, it sends a positive Connect Response to the HID and the devices move to Connected Mode. If a HID does not receive a positive Connect Response in a defined <sup>[2]</sup> period of time, it selects the next channel using the channel selection algorithm and repeats the procedure. If the HID does not receive a positive Connect Response on any of the channels in the subset it enters Sleep Mode in order to conserve power. When the HID wakes up due to a user action it will reenter Reconnect Mode.

<sup>2</sup> The timeout values are configurable.

## Bind Mode

### HID

Bind Mode allows the HID to send its Manufacturing ID to the bridge and receive the Network ID from the bridge. Upon entering Bind Mode the HID sets the current channel and PN code to the channel and PN code specified in the Bind ID. The HID then alternately transmits Bind Requests (containing its device type and Manufacturing ID) and listens for Bind Responses (containing the Network ID) from the bridge. The HID transmits a defined <sup>[3]</sup> number of Bind Request on each channel. If a Bind Response is not received the HID moves to the next channel. If a Bind Response is received the HID stores the Network ID for later use and moves to Reconnect Mode. If a defined <sup>[4]</sup> period of time has elapsed while in Bind Mode without receiving a Bind Response, the HID assumes the bridge is not available and switches to Init Mode. Bind Mode should last long enough for the user to locate and push the button on both the bridge and the HID. A user-initiated event can cause the HID to enter Bind Mode from any other mode.

### Bridge

Upon entering Bind Mode the bridge sets the current channel and PN code to the channel and PN code specified in the Bind ID. The bridge listens for a defined <sup>[5]</sup> period of time for Bind Request on each channel before selecting the next channel using the channel selection algorithm. This reduces the possibility of the bridge not receiving the Bind Request from the HID in the event of channel interference. If the bridge receives a Bind Request from the HID containing a supported device type it stores the HID's Manufacturing ID, sends a Bind Response and then switches to Ping Mode. The bridge also switches to Ping Mode if the defined <sup>[6]</sup> time period has elapsed while in Bind Mode. The channel selection algorithm uses the Bind ID to produce the channel subset for Bind Mode.

<sup>3</sup> The timeout values and number of packet transmissions are configurable.

<sup>4</sup> The timeout values and number of packet transmissions are configurable.

<sup>5</sup> The timeout values and number of packet transmissions are configurable.

<sup>6</sup> The timeout values and number of packet transmissions are configurable.

## Connected Mode

### HID

Connected Mode allows application data to be transmitted from the bridge to the HID. When the HID application has data to send to the bridge the HID creates a DATA packet and listens for a response (either an ACK or ACK/DATA packet). If no response is received, the HID retransmits <sup>[7]</sup> the packet. In WirelessUSB HID systems application data sent from the bridge to the HID is referred to as back channel data. There are three methods for handling the back channel as described as follows:

#### *No Back Channel*

If application data is only sent from the HID to the bridge (1-way data) the HID does not need to listen for data from the bridge. When the HID has application data to send it transmits a DATA packet to the bridge and then listen for an ACK. If the bridge does not respond with an ACK (either no response or a NAK) the HID repeats the procedure. If the HID does not receive an ACK after a defined <sup>[8]</sup> number of transmissions of the DATA packet it may continue in Connected Mode or assume the channel has become unavailable due to excessive interference and move to Reconnect Mode.

#### *Polled Back Channel*

If the bridge sends application data to the HID and the HID is power-sensitive the bridge may combine an ACK with a DATA packet in order to reduce the protocol overhead and minimize the length of time the HID is in receive mode. The HID processes the ACK and DATA portions of the ACK/DATA packet just like it would separate ACK and DATA packets. If all back channel data is sent using ACK/DATA packets the HID must poll the bridge periodically by sending NULL packets if the HID does not have application data to send to the bridge, thus allowing the bridge to respond with an ACK/DATA packet. If the bridge does not have data to send to the HID it will send a normal ACK instead of an ACK/DATA packet. If the bridge does not respond with a ACK (or ACK/DATA) (either no response or a NAK) the HID repeats the procedure. If the HID does not receive a ACK after a defined <sup>[9]</sup> number of transmissions of the DATA packet it may continue in Connected Mode or assume the channel has become unavailable due to excessive interference and move to Reconnect Mode.

<sup>7</sup> The number of packet transmissions and interference threshold are configurable.

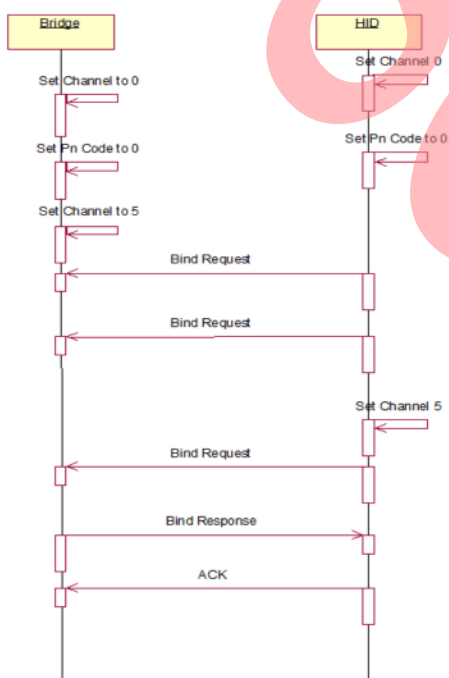
<sup>8</sup> The number of packet transmissions and interference threshold are configurable.

<sup>9</sup> The number of packet transmissions and interference threshold are configurable.

### Asynchronous Back Channel

If the HID is not power-sensitive it may listen for asynchronous DATA packets from the bridge. This method requires the HID to always be in receive mode when not transmitting instead of only being in receive mode for a short period of time after transmitting (as in the other two methods), but allows the bridge to send application data without being polled by the HID. When the HID has application data to send it will transmit a DATA packet to the bridge and then listen for a ACK. If the bridge does not respond with an ACK packet (either no response or a NAK packet) the HID repeats the procedure. If the HID does not receive a ACK after a defined <sup>[10]</sup> number of transmissions of the DATA packet it may continue in Connected Mode or assume the channel has become unavailable due to excessive interference and move to Reconnect Mode. When the HID does not have application data to send it listens for DATA packets from the bridge and responds with an ACK or NAK.

Figure 8. Bind Sequence Diagram



<sup>10</sup> The number of packet transmissions and interference threshold are configurable.

### Bridge

Connected Mode allows application data to be transmitted between the bridge and HID. The bridge should continuously listen for DATA packets from the HID. When valid data is received from the HID the bridge sends an ACK to the HID and sends the data to the USB host. If invalid data is received the bridge will send a NAK to the HID and listen for the HID to retransmit the data. The bridge monitors the interference level and moves to Ping Mode if the defined <sup>[11]</sup> interference threshold is reached, in order to find an available channel. There are three methods for handling application data being sent to the HID as described below:

#### No Back Channel

If application data is not sent from the bridge to the HID the bridge always sends ACK in response to HID DATA packets and never sends DATA or ACK/DATA packets to the HID.

#### Polled Back Channel

If a polled back channel is used the bridge must store application data to be sent to the HID until a DATA packet or a NULL packet is received from the HID. The bridge will send an ACK/DATA packet to the HID and then listen for an ACK. If the HID does not respond with an ACK (either no response or a NAK) the bridge repeats the procedure. If the bridge does not receive an ACK after a defined <sup>[12]</sup> number of transmissions of the ACK/DATA packet it assumes the channel has become unavailable due to excessive interference and moves to Ping Mode in order to find an available channel.

#### Asynchronous Back Channel

When the bridge has data to send it will send a DATA packet to the HID and then listen for a n ACK. If the HID does not respond with an ACK (either no response or a NAK packet) the bridge repeats the procedure. If the bridge does not receive an ACK after a defined <sup>[13]</sup> number of transmissions of the DATA packet it assumes the channel has become unavailable due to excessive interference and moves to Ping Mode in order to find an available channel.

<sup>11</sup> The number of packet transmissions and interference threshold are configurable.

<sup>12</sup> The number of packet transmissions and interference threshold are configurable.

<sup>13</sup> The number of packet transmissions and interference threshold are configurable.

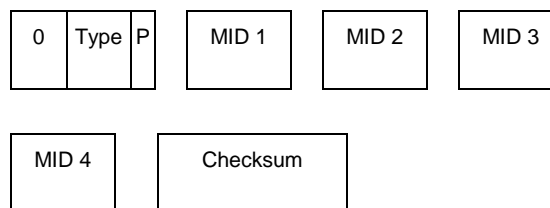
In Sleep Mode the radio and microcontroller are in low-power mode. An external event (i.e. mouse movement or key press) is required to return the HID to its previous mode. The protocol library controls radio power management; the application controls the microcontroller power management.

The most significant nibble of the first byte contains the packet type. Packet types 0x0–0x8 are defined below, packet types 0x9–0xF are reserved. All unused bit fields in the Packet Header are set to 0. The Packet Header byte uses odd parity (an odd number of high bits in the byte).

```

sequenceDiagram
    participant Bridge
    participant DS
    Note over Bridge, DS: HID is connected to Channel 0, Pin Code 2
    Bridge->>DS: Data
    DS->>Bridge: ACK
    Note over Bridge: Interference Threshold Reached
    Bridge->>Bridge: Ping Mode
    Bridge->>Bridge: Set Channel to 28
    Bridge->>DS: Ping
    DS->>Bridge: Ping
    Bridge->>Bridge: Idle Mode
    DS->>Bridge: Data
    Note over DS: ACK Timeout
    DS->>DS: ACK Timeout
    DS->>DS: Reconnect Mode
    DS->>Bridge: Connect Request
    Note over DS: Set Channel to 28
    DS->>DS: Set Channel to 28
    DS->>Bridge: Connect Request
    Bridge->>DS: Connect Response
    DS->>Bridge: ACK
  
```

Bind Requests are sent from the HID to the bridge during Bind Mode.



- **Device Type (Type)** – This is a 3-bit field specifying a vendor-defined device type. This allows the bridge to determine what type of device the HID is and thus determine the length of data packets, which PN code to assign, etc.

- **Parity (P)** – This is a 1-bit parity field for the header byte using odd parity.

**Manufacturing ID (MID 1–MID 4)** – This is the 4-byte Manufacturing ID retrieved from the WirelessUSB radio. MID 1 is register 0x3C, MID 2 is register 0x3D, MID 3 is register 0x3E and MID 4 is register 0x3F.

**Checksum** – This is an 8-bit field containing an XOR checksum of all previous bytes in the packet. The default checksum seed of 0x00 is used for Bind Request Packets.

Bind Response Packets are sent from the bridge to the HID during Bind Mode in response to valid Bind Requests.



- **PIN** – This is a 3-bit field specifying the PIN element of the Network ID.

- **Parity (P)** – This is a 1-bit parity field for the header byte using odd parity.

**Channel** – This is an 8-bit field specifying the first channel to be used in the Channel Selection Algorithm. (Only channels 0-75 are valid)

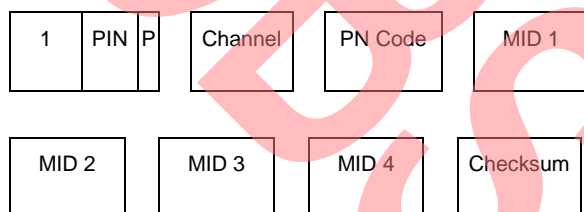
**PN Code** – This is an 8-bit field specifying the PN code to be used.

**Network Checksum Seed (NCS)** – This is an 8-bit field specifying the seed to be used for calculating the checksum on all Connect Request, Connect Response, DATA, ACK, ACK/DATA and NULL packets (Bind Request, Bind Response and Ping packets use the default checksum seed of 0x00)

**Checksum** – This is an 8-bit field containing an XOR checksum of all previous bytes in the packet. The default checksum seed of 0x00 is used for Bind Response Packets.

### Connect Request Packet (HID)

Connect Request Packets are sent from the HID to the Bridge during Reconnect Mode.



#### Packet Header

- **PIN** – This is a 3-bit field specifying the PIN element of the Network ID.
- **Parity (P)** – This is a 1-bit parity field for the header byte using odd parity.

**Channel** – This is an 8-bit field specifying the first channel to be used in the Channel Selection Algorithm as returned by the Bind Response Packet or stored in nonvolatile memory (only channels 0–77 are valid channels).

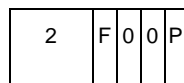
**PN Code** – This is an 8-bit field specifying the PN code to be used as returned by the Bind Response Packet or stored in nonvolatile memory.

**Manufacturing ID (MID 1–MID 4)** – This is the 4-byte Manufacturing ID retrieved from the WirelessUSB radio. MID 1 is register 0x3C, MID 2 is register 0x3D, MID 3 is register 0x3E and MID 4 is register 0x3F.

**Checksum** – This is an 8-bit field containing an XOR checksum of all previous bytes in the packet. The Network Checksum Seed is used for Connect Request Packets.

### Connect Response Packet (Bridge)

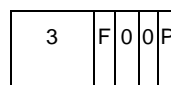
Connect Response Packets are sent from the Bridge to the HID in Idle and Connected Mode in response to valid Connect Requests.



#### Packet Header

- **Flag (F)** – This is a 1-bit field specifying a positive or negative Connect Response Packet (1 = positive, 0 = negative).
- **Parity (P)** – This is a 1-bit parity field for the header byte using odd parity.

### Ping Packet (Bridge)

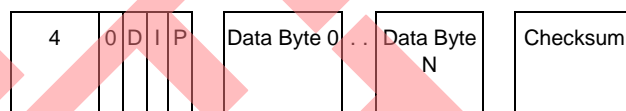


#### Packet Header

- **Flag (F)** – This is a 1-bit field specifying a Ping or Ping Response (0 = Ping, 1 = Ping Response).
- **Parity (P)** – This is a 1-bit parity field for the header byte using odd parity.

### DATA Packet (Bridge and HID)

DATA Packets are sent from the HID to the bridge in Connected Mode. They are also sent from the bridge to the HID in Connected Mode if there is an asynchronous back channel. The order of fields in the packet header of DATA, ACK and ACK/DATA packets is such that the fields in the ACK/DATA packet headers are in the same positions as the corresponding fields in the DATA and ACK packets.



#### Packet Header

- **Data Toggle Bit (D)** – This is a 1-bit field that is toggled for each new DATA Packet. It is used to distinguish between new and retransmitted packets.
- **Device ID (I)** – This is a 1-bit field containing the least significant bit of the Device Type. The Device ID field is used in 2:1 systems to distinguish between the HID devices.
- **Parity (P)** – This is a 1-bit parity field for the header byte using odd parity.

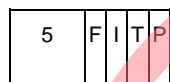
**Data Byte 0–N** – This is byte-aligned application data.

**Checksum** – This is an 8-bit field containing an XOR checksum of all previous bytes in the packet. The Network Checksum Seed is used for DATA Packets.



### ACK Packet (Bridge and HID)

ACK Packets are sent from the bridge and HID in Connected Mode in response to valid DATA Packets. They are also sent from the HID to the bridge in response to valid Bind Responses during Bind Mode and valid Connect Responses during Reconnect Mode.

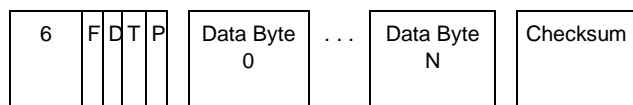


#### Packet Header

- **Flag (F)** – This is a 1-bit field specifying a positive or negative ACK Packet (1 = ACK, 0 = NAK).
- **Device ID (I)** – This is 1-bit field containing the least significant bit of the Device Type. The Device ID field is used in 2:1 systems to distinguish between the HID devices.
- **Data Toggle Bit (T)** – This is a 1-bit field matching the Data Toggle Bit of the Data Packet being acknowledged.
- **Parity (P)** – This is a 1-bit parity field for the header byte using odd parity.

### ACK/DATA Packet (Bridge)

ACK/Data Packets are sent from the bridge to the HID during Connected Mode in response to a valid DATA Packet if there is a polled back channel and the bridge has application data to send to the HID (otherwise a normal ACK is used). ACK/DATA Packets cannot be used in 2:1 systems that use the Device ID Bit to identify the HID, because there is no room in the packet header for the Device ID field.



#### Packet Header

- **Flag (F)** – This is a 1-bit field specifying a positive or negative ACK Packet (1 = ACK, 0 = NAK).
- **Data Toggle Bit (D)** – This is a 1-bit field that is toggled for each new DATA Packet. It is used to distinguish between new and retransmitted data packets.
- **Data Toggle Bit (T)** – This is a 1-bit field matching the Data Toggle Bit of the DATA Packet being acknowledged.

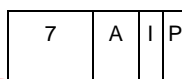
- **Parity (P)** – This is a 1-bit parity field for the header byte using odd parity.

**Data Byte 0–N** – This is byte-aligned application data.

**Checksum** – This is an 8-bit field containing an XOR checksum of all previous bytes in the packet. The Network Checksum Seed is used for ACK/DATA Packets.

### NULL Packet (Bridge and HID)

NULL Packets are sent from the HID to the bridge during Connected Mode instead of DATA Packets if there are two bits or less of application data to be sent. NULL Packets can be used to poll the bridge for back channel data if there is a polled back channel; they may also be used to replace frequently transmitted packets such as a key up event on keyboards in order to reduce the amount of data that is transmitted.



#### Packet Header

- **Data (A)** – This is a 2-bit field containing application data.
- **Device ID (I)** – This is 1-bit field containing the least significant bit of the Device Type. The Device ID field is used in 2:1 systems to distinguish between the HID devices.
- **Parity (P)** – This is a 1-bit parity field for the header byte using odd parity.

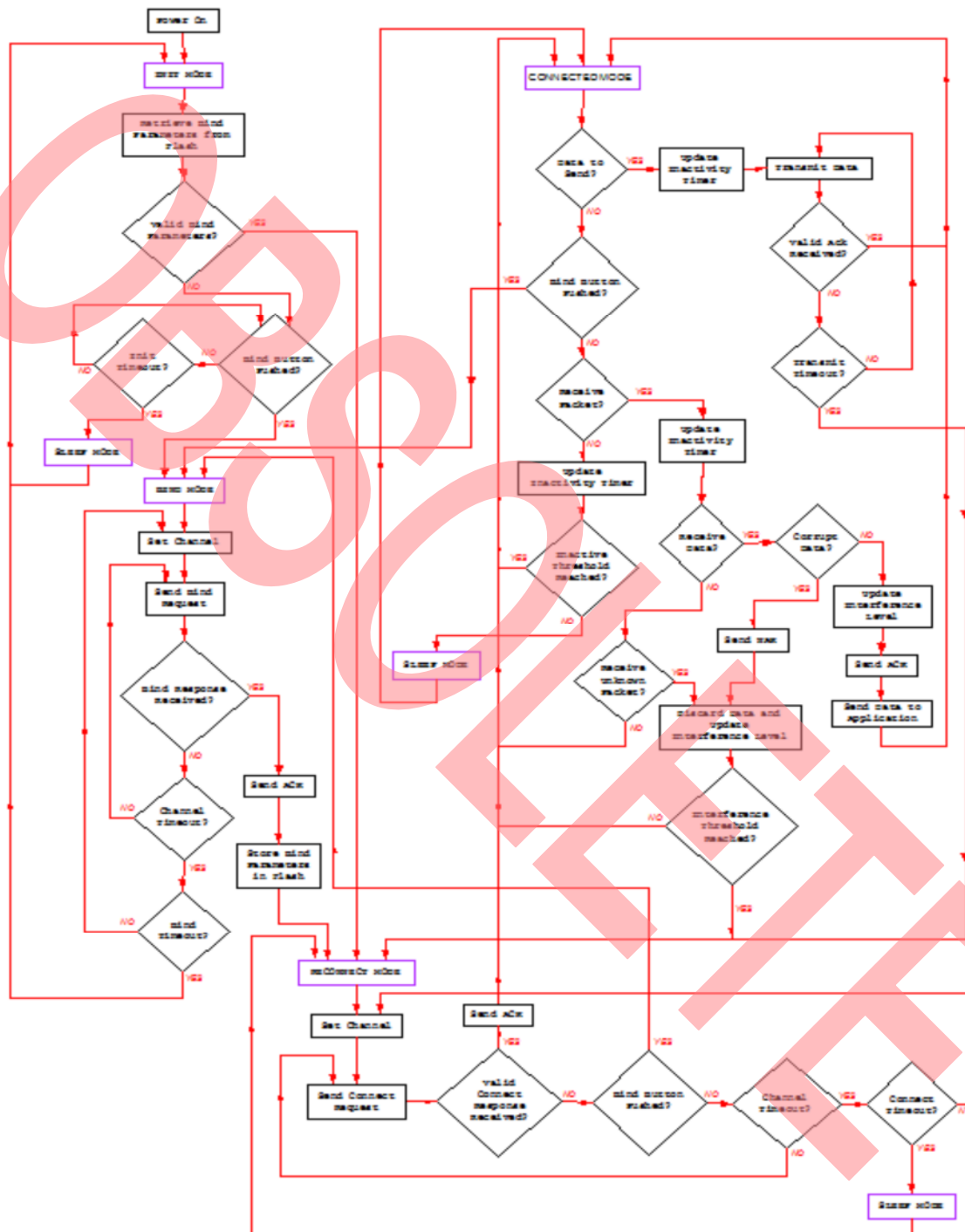
## Summary

The WirelessUSB™ 2-Way Human Interface Device (HID) protocol is designed for reliable 2-Way communication between a wireless bridge and target HID applications in 1:1 (one HID and one bridge) and 2:1 (two HIDs and one bridge) systems. The WirelessUSB 2-Way HID protocol allows HID applications to establish a connection to the bridge and receive ACK, NAK and DATA packets from the bridge.

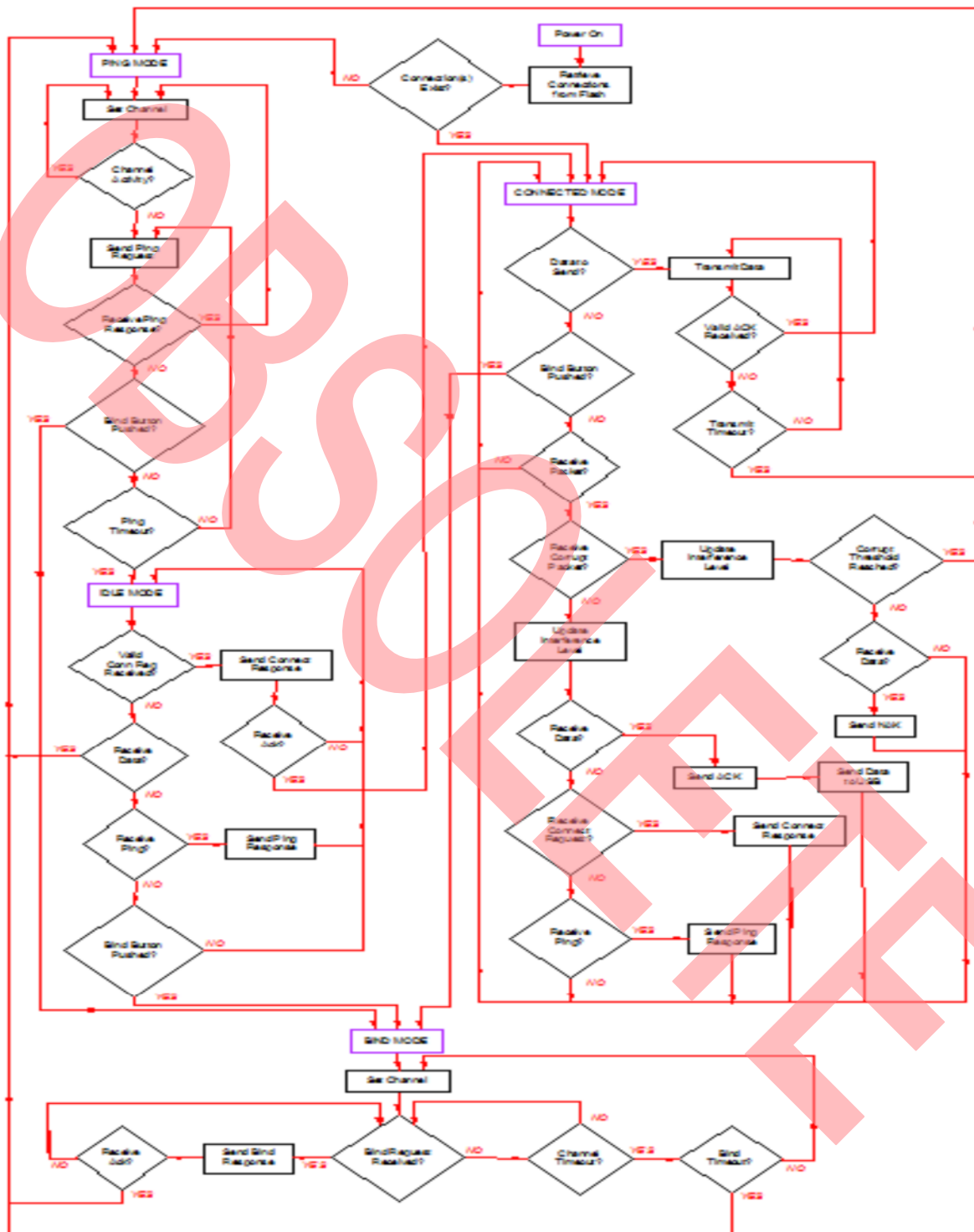
## About the Author

Name: Sai Prashanth Chinnappalli.  
Title: Applications Engineer Staff

## Appendix A: Complete WirelessUSB 2-Way HID State Machine



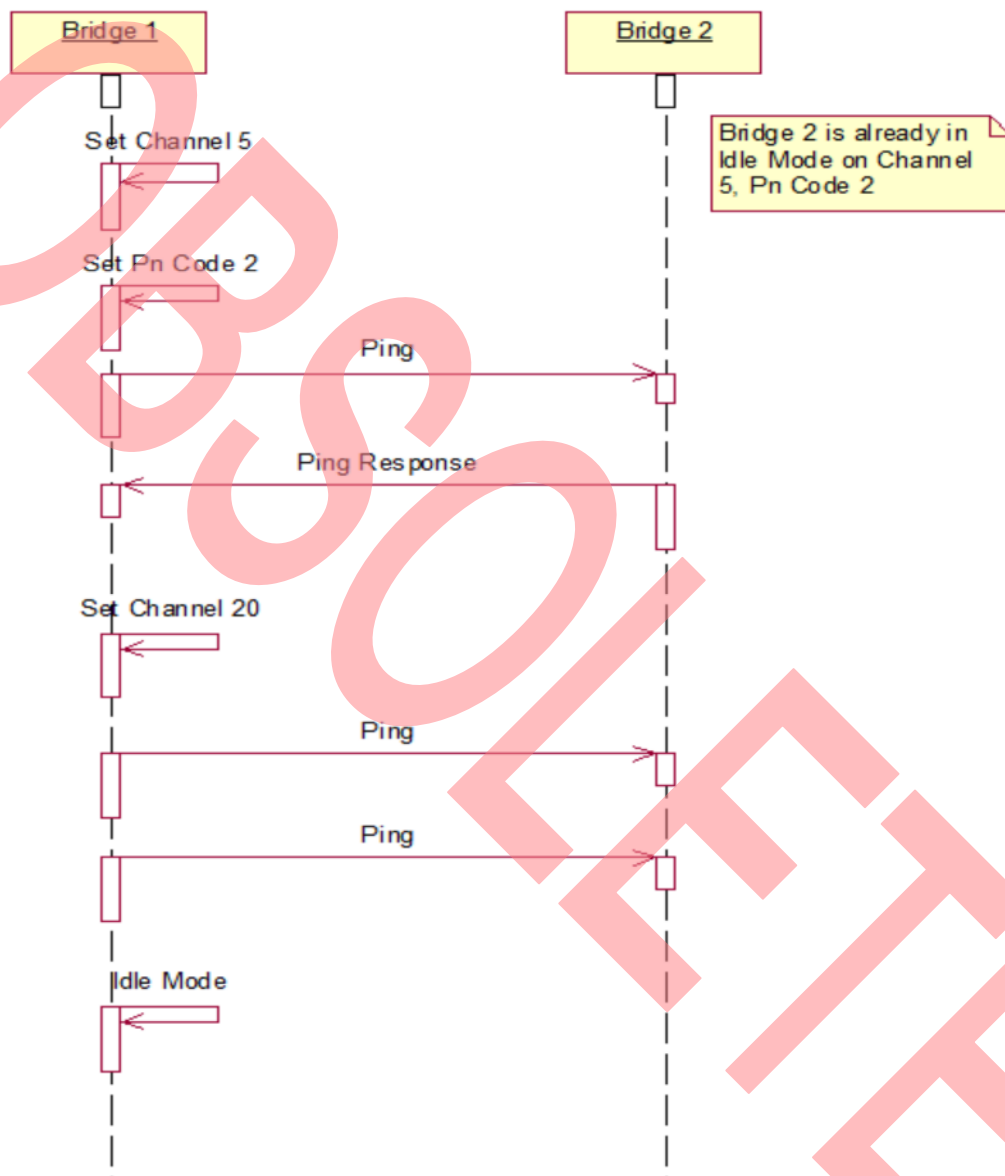
## Appendix B: Complete WirelessUSB 2-Way Bridge State Machine



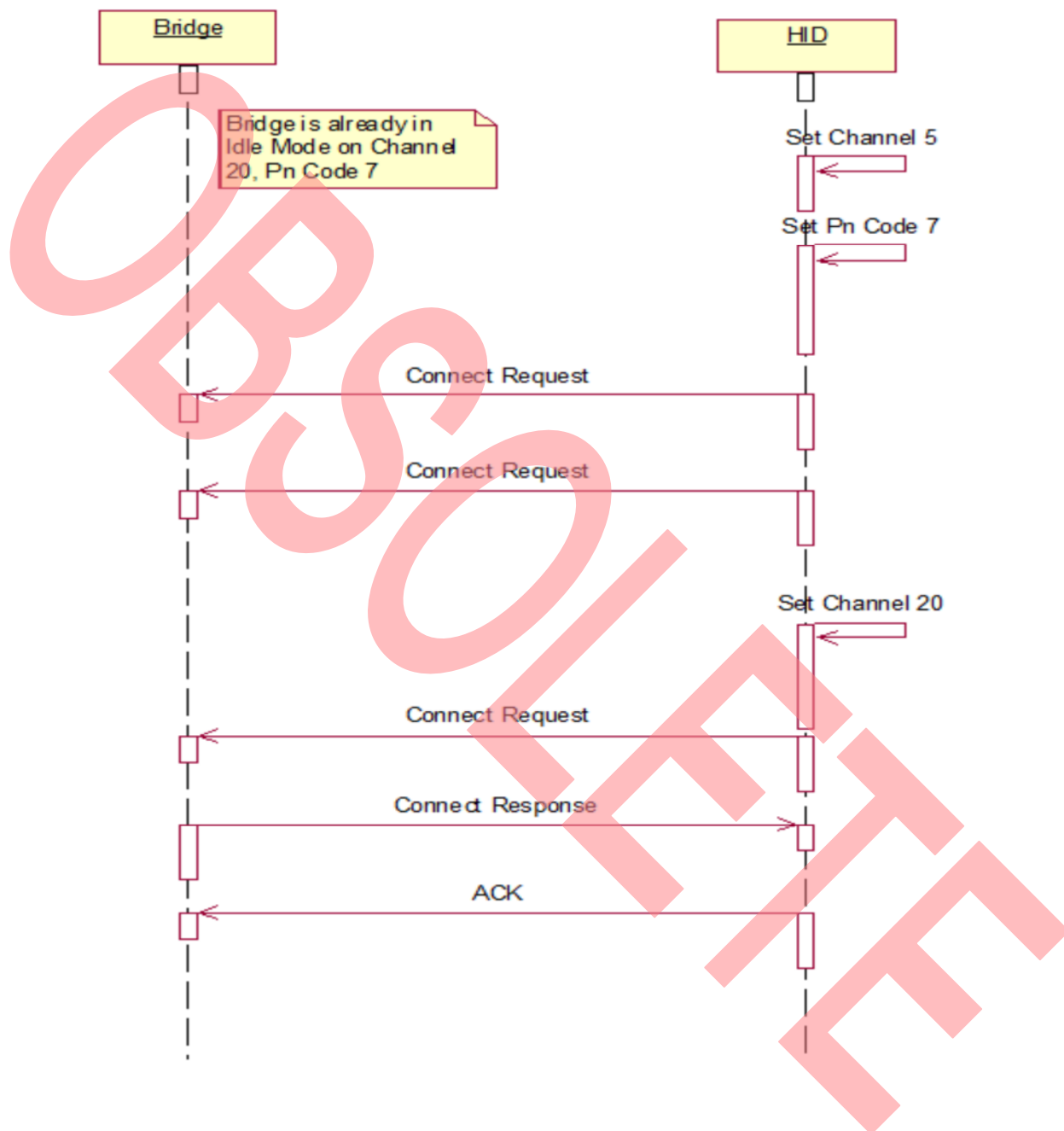


## Appendix C: Sequence Diagrams

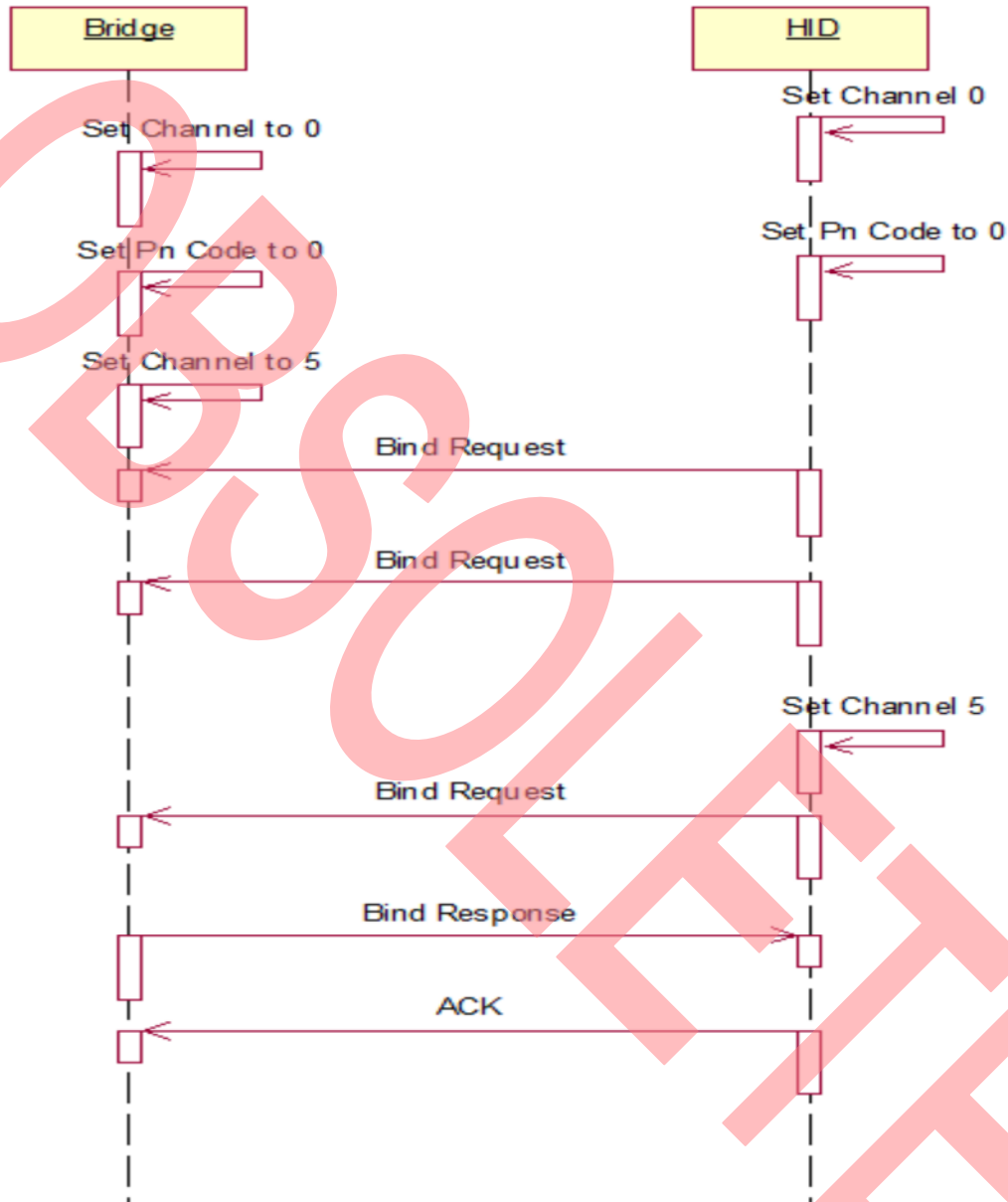
### PING Sequence



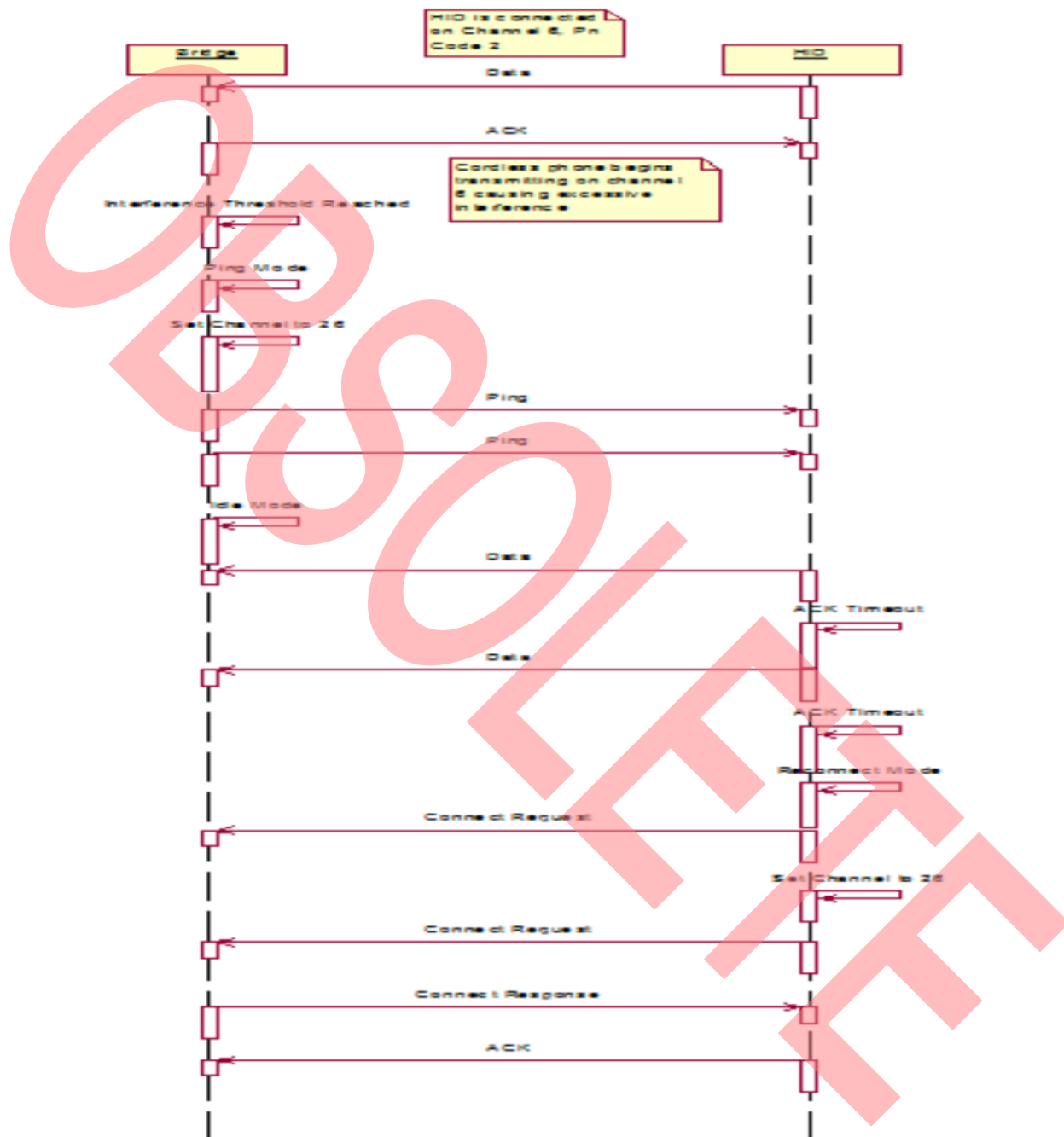
## Connect Sequence



## BIND Sequence



## Interference Avoidance Sequence



## Document History

Document Title: WirelessUSB™ 2-Way HID Systems - AN4003

Document Number: 001-15083

Revision	ECN	Orig. of Change	Submission Date	Description of Change
**	1013540	SFV	04/24/2007	Added Spec No. and new disclaimer and also updated the copyright date
*A	1767565	CSAI	11/23/2007	Copyright updated, Source Disclaimer and Revision Disclaimer added. Applied new template.
*B	3256630	CSAI	05/13/2011	Added abstract. Modified introduction. Updated as per new template.
*C	4395183	CSAI	05/31/2014	Updated in new template. Completing Sunset Review.
*D	5740123	ANKC	05/23/2016	Obsoleting the AN

## Worldwide Sales and Design Support

Cypress maintains a worldwide network of offices, solution centers, manufacturer's representatives, and distributors. To find the office closest to you, visit us at [Cypress Locations](#).

### Products

Automotive	<a href="http://cypress.com/go/automotive">cypress.com/go/automotive</a>
Clocks & Buffers	<a href="http://cypress.com/go/clocks">cypress.com/go/clocks</a>
Interface	<a href="http://cypress.com/go/interface">cypress.com/go/interface</a>
Lighting & Power Control	<a href="http://cypress.com/go/powerpsoc">cypress.com/go/powerpsoc</a> <a href="http://cypress.com/go/plc">cypress.com/go/plc</a>
Memory	<a href="http://cypress.com/go/memory">cypress.com/go/memory</a>
PSoC	<a href="http://cypress.com/go/psoc">cypress.com/go/psoc</a>
Touch Sensing	<a href="http://cypress.com/go/touch">cypress.com/go/touch</a>
USB Controllers	<a href="http://cypress.com/go/usb">cypress.com/go/usb</a>
Wireless/Rf	<a href="http://cypress.com/go/wireless">cypress.com/go/wireless</a>

### PSoC® Solutions

[psoc.cypress.com/solutions](http://psoc.cypress.com/solutions)

PSoC 1 | PSoC 3 | PSoC 4 | PSoC 5LP

### Cypress Developer Community

[Community](#) | [Forums](#) | [Blogs](#) | [Video](#) | [Training](#)

### Technical Support

[cypress.com/go/support](http://cypress.com/go/support)

WirelessUSB is a trademark of Cypress Semiconductor. All other trademarks or registered trademarks referenced herein are the property of their respective owners.



Cypress Semiconductor  
198 Champion Court  
San Jose, CA 95134-1709

Phone : 408-943-2600  
Fax : 408-943-4730  
Website : [www.cypress.com](http://www.cypress.com)

© Cypress Semiconductor Corporation, 2007-2017. The information contained herein is subject to change without notice. Cypress Semiconductor Corporation assumes no responsibility for the use of any circuitry other than circuitry embodied in a Cypress product. Nor does it convey or imply any license under patent or other rights. Cypress products are not warranted nor intended to be used for medical, life support, life saving, critical control or safety applications, unless pursuant to an express written agreement with Cypress. Furthermore, Cypress does not authorize its products for use as critical components in life-support systems where a malfunction or failure may reasonably be expected to result in significant injury to the user. The inclusion of Cypress products in life-support systems application implies that the manufacturer assumes all risk of such use and in doing so indemnifies Cypress against all charges.

This Source Code (software and/or firmware) is owned by Cypress Semiconductor Corporation (Cypress) and is protected by and subject to worldwide patent protection (United States and foreign), United States copyright laws and international treaty provisions. Cypress hereby grants to licensee a personal, non-exclusive, non-transferable license to copy, use, modify, create derivative works of, and compile the Cypress Source Code and derivative works for the sole purpose of creating custom software and or firmware in support of licensee product to be used only in conjunction with a Cypress integrated circuit as specified in the applicable agreement. Any reproduction, modification, translation, compilation, or representation of this Source Code except as specified above is prohibited without the express written permission of Cypress.

Disclaimer: CYPRESS MAKES NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Cypress reserves the right to make changes without further notice to the materials described herein. Cypress does not assume any liability arising out of the application or use of any product or circuit described herein. Cypress does not authorize its products for use as critical components in life-support systems where a malfunction or failure may reasonably be expected to result in significant injury to the user. The inclusion of Cypress' product in a life-support systems application implies that the manufacturer assumes all risk of such use and in doing so indemnifies Cypress against all charges.

Use may be limited by and subject to the applicable Cypress software license agreement.