*DRAFT*

**SPAWAR SYSTEMS CENTER PACIFIC**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**USERS’ GUIDE**

**FIXED NETWORK ACCESS DEVICE (FNAD)**

**and**

**TEST SUPPORT HARDWARE/SOFTWARE:**

**REFERENCE ELECTRONIC CHAIN OF CUSTODY DEVICE (rECoC)**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*Prepared for*

*Department Of Homeland Security*

*Science and Technology Directory Directorate*

*Secure Transit Corridors Pilot Program*

*Document Control Number: xxxx*

**January 23, 2012**

**REVISIONS**

|  |  |
| --- | --- |
| **Cover Page Date** | **Description** |
| **December 12, 2011** | **Initial Release** |
| **December 14, 2011** | **Updated sections: Hardware jumpers, Secondary Loader Corrected typos.** |
| **December 29, 2011** | **Updated section: Secondary Loader (SL) use** |
| **January 23, 2012** | **Updated INI file section, added SYNTHLOG keyword** |

**CONTENTS**

[FNAD QUICK OVERVIEW (see also *functional description* section) 3](#_Toc311631263)

[TYPICAL FNAD OUTDOOR ENCLOSURES 4](#_Toc311631264)

[FNAD SITE LAN AND FIREWALL CONFIGURATION 5](#_Toc311631265)

[FNAD TO DATA CENTER MESSAGING 6](#_Toc311631266)

[FNAD INSTALLATION AND FIRST USE 7](#_Toc311631267)

[HARDWARE JUMPERS, BUTTONS and INDICATOR LEDs 8](#_Toc311631268)

[HARDWARE JUMPERS WHEN USING PRIMARY BOOTSTRAP LOADER 9](#_Toc311631269)

[SAMPLE CONFIGURATION FILE (.ini) 10](#_Toc311631270)

[OPERATIONAL USE, COMMUNICATIONS-RELATED 14](#_Toc311631271)

[FIRMWARE UPDATE using fnad serial port/PRIMARY BOOTSTRAP 17](#_Toc311631272)

[SECONDARY LOADER (SL) USE 19](#_Toc311631273)

[FUNCTIONAL DESCRIPTION SPECIFICS 20](#_Toc311631274)

| FNAD QUICK OVERVIEW (see also *functional description* section) | |
| --- | --- |
| PHYSICAL | Electronics circuit board housed within varied types of weatherproof enclosures with integral or external antenna. Antenna type is locale-dependent. See photos, next page. |
| POWER | 6-9VDC via Ethernet cat5 cable power inserter or local power transformer |
| ENVIRONMENTAL | For outdoor usage in cold and warm climate locales |
| WIRELESS | 2.4GHz unlicensed band; IEEE 802.15.4 MAC/PHY |
| IEEE 802.15.4 | Configured and operated per DHS ICD specifications. FNADs use one of four channels |
| ANTENNAS | Integral to weatherproof enclosure or is external. Type Varies: chosen during planning for each FNAD/site according to required area of coverage. H/V polarization as needed. |
| LAN INTERFACE | Standard Ethernet IEEE 802.3, 10/100BT. Connect to LAN switch or wireless point to point IP link. Optional use of power inserter/extractor for FNAD power (as above) |
| LAN PROTOCOLS | IP, TCP, UDP, ICMP, ARP. For remote management: RFC SYSLOG and passive FTP |
| DATA CENTER (DC) | Messages per DHS ICD via bi-directional UDP or FNAD-initiated TCP connection to DC |
| MESSAGING | FNAD exchanges (bridges) applications messages formatted per DHS ICD between IEEE 802.15.4 wireless and LAN, then onward to data center via IP networking, and vice-versa. |
| MESSAGE  SECURITY | The FNAD is “transparent to” message security, authentication, or key management/distribution, as are other network transports devices along the end-to-end route. All sensitive messages are AES-encrypted at the message producer (on-container device or data center) and decrypted only at the final recipient. The FNAD and all other network infrastructure/transports between sender/receiver cannot decrypt. |
| NETWORK DISCOVERY | On-container devices passively detect in-coverage conditions (in proximity to one or more FNADs), via FNAD-transmitted network advertisement broadcasts |
| ENABLING POWER MANAGEMENT | FNADs enable on-container devices to “sleep” (power-down) to conserve battery capacity. A “message waiting” mechanism is used by FNADs per DHS’ ICD. |
| DATA PACKET/FRAME BRIDGING | FNADs maintain a list of in-range on-container devices (e.g. ECoCs), their network MAC address, their logical identity (UID), received signal strength, and other items. Ethernet IP packets from the data center are reformed to IEEE 802.15.4 data frames and transmitted wirelessly. Vice-versa, received frames are converted to IP packets and sent to the designated data center. The DHS ICDs for error detection and correction are supported, yielding an end-to-end reliable datagram service irrespective of the LAN/WAN protocol being UDP or TCP. |
| REMOTE MONITORING | During operation, FNAD sends status and detailed communications event logging information to centralized remote monitoring server (RMS). Internet RFC standard “Syslog” protocol used with send-only from FNAD to RMS. Since FNADs cannot decrypt, RMS messaging does not include message secure content. The RMS logs and displays monitoring event data; viewing by other authorized remote users is supported. |
| REMOTE CONFIGURATION MANAGEMENT | At power-up, each FNAD downloads its configuration settings from centralized remote configuration server (RCS). If the RCS is unreachable, the prior settings are used. |
| REMOTE FIRMWARE UPDATE | If enabled, FNAD checks for firmware update from a designated centralized remote configuration server (RCS). New firmware is automatically downloaded and installed. |

# TYPICAL FNAD OUTDOOR ENCLOSURES

****

**LEFT: FNAD’s electronics go within this enclosure. Has integral 14dBi gain antenna.**

**RIGHT: Multiple FNADs w/enclosure for use with external antennas.**

| FNAD SITE LAN AND FIREWALL CONFIGURATION | |
| --- | --- |
| FNAD’s LAN SETTINGS | Per FNAD   * Static IP, private or public address * Subnet mask * Gateway IP address   The above values must be placed in the INI file at the RCS (one per FNAD) |
| FIREWALL TRAVERSAL | The following ports and protocols are used by each FNAD. No inward TCP connections are required. The FNAD initiates all outward connections.   * Port x protocol UDP or TCP, bi-directional; *FNAD to/from Data Center* (SCMS/DCP). If TCP, the FNAD initiates the outward connection. Port no. and protocol are chosen per FNAD by project and site LAN admin in collaboration. Values selected are placed in INI file for FNADs at that site. * Port 514/UDP, *Syslog* per RFC, FNAD send-only, to Remote Monitoring Server (RMS) * Port 21/TCP, *FTP* *passive mode* per RFC, for infrequent use. FNAD initiated outward command/data connections to Remote Configuration Server (RCS) at a primary or one of 2 backup IP addresses. The IP addresses are in the INI file at the RCS for the FNADs. * Port 13/TCP, *NIST Time* protocol, FNAD initiated connection to update date/time. a primary or one of 2 backup IP addresses are in the FNAD’s INI file at the RCS. |
| FIREWALL/ROUTER NETWORK ADDRESS TRANSLATION (NAT) | The FNAD is compatible with NAT with the following clarifications:   * The FNAD initiated data center connection, if UDP, has firewall/router port-forwarding for packets sent and received by the FNAD. * The firewall permits FNAD-initiated TCP connections as listed above. * The firewall supports ordinary FTP passive mode connection to the RCS. The FTP login is done on the standard port number. The passive mode data transfer is FNAD-initiated, outward, per the IETF standard via a TCP connection on a destination port number assigned by the FTP server. |
| LAN SETTING CHANGES DURING THE PROJECT OPERATION PERIOD  (IP, GATEWAY, MASK) | Should a site require changing LAN IP addresses, the Remote Configuration Server (RCS) INI files for affected FNAD can be edited and the FNADs rebooted. The FNAD will reboot due to a power on/off or by briefly dropping the Ethernet Link connection. The latter can be done at the LAN switch to which an FNAD is connected. |
|  |  |

| FNAD TO DATA CENTER MESSAGING | |
| --- | --- |
| WAN CONNECTIVITY | UDP (preferred) or TCP connection initiated by FNAD. The data center’s IP address and port number and protocol to be used by the FNAD are given in the INI file stored at the Remote Configuration Server (RCS). For the TCP option, the FNAD initiates and sustains a connection. |
| DHS ICD MESSAGES | The FNAD supports the DHS ICD defined message formats for:   * Data center to/from on-container ECoC devices * Data center to NAD, set date/time * FNAD initiated status/health heartbeat messages, recurring |
| HEARTBEAT MESSAGES | The INI file item [DC] “DCHEARTBEAT”, if true, causes the FNAD to require the data center to respond to ICD defined heartbeat status messages sent by the FNAD. If responses are not received, the FNAD reports such to the RMS and the FNAD reboots. |
| NON-ICD MESSAGES | The FNAD supports the following non-ICD defined messages   * Unpublished method for remotely initiated FNAD reboot command with password. This would be used after altering the INI file at the RCS in lieu of on-site personnel rebooting the FNAD via a power cycle or briefly interrupting the Ethernet cable connection at the serving Ethernet switch. |
|  |  |

| FNAD INSTALLATION AND FIRST USE | |
| --- | --- |
| FNAD IDENTITY | The FNAD’s identity is the unchanging IEEE 802.15.4 transceiver MAC address. A soft “UID” is given configuration-data (INI) for each FNAD and used in DC messaging. The proper firmware and jumper settings (see Photo 1) should be pre-configured. |
| INSTALLATION | Use deployment plan to place FNAD and provide local or Ethernet based power. |
| ANTENNA | Use deployment plan’s defined antenna type, polarization (H/V) and aiming direction |
| CONFIGURATION DATA FILE (INI) | Each FNAD requires a unique configuration “ini” file stored on the remote configuration server (RCS). A copy of this file should be on a laptop used at installation. |
| OBTAIN LAN IP ADDRESS | The LAN administrator assigns each FNAD a static IP address on the LAN and a gateway address in the subnet. These FNAD-unique value are place in the FNAD’s INI file. |
| LAN FIREWALL CONFIGURATION | The LAN administrator ensures that the LAN firewall is FNAD-compatible, summarized as follows, for each FNAD:   1. FNAD’s send-only UDP packets to remote remote monitoring server, port 514 2. FNAD-initiated FTP (passive mode) connection to remote configuration server 3. FNAD to/from Data center bi-directional traffic, either UDP or FNAD-initiated TCP connection; port number as chosen. Sensitive data is source-encrypted. |
| LAN CONNECTION | The FNAD connects by cat5 Ethernet to the local LAN or to a wireless bridge leading to the local LAN and switch. |
| REMOTE MONITORING SERVER (RMS) ADDRESS | Project network personnel ensure that the RMS server IP address is in the INI file for all FNADs. Note: Once the FNAD can send UDP packets to the RMS, the FNAD’s status and errors in LAN/WAN settings can be observed. Temporarily/durng installation, an on-site laptop-based RMS server could be used. |
| REMOTE CONFIGURATION SERVER ADDRESS | Project network personnel ensure that the RCS server IP address is in the INI file for all FNADs. Once this and the LAN settings are established, all other FNAD configuration settings may be remotely managed. |
| POWER-UP INDICATIONS  (See Photo 1, below) | With the FNAD’s enclosure opened, the visual indications are: 1. The Ethernet connector’s green Link LED should be ON. If not, check LAN cabling.  2. Red small LED on IEEE 802.15.4 radio is on.  3. If installed, the Secondary Loader for remote firmware updates runs at power on. See this document’s *Secondary Loader s* section description on checking for firmware updates.  4. A few seconds after power-on, the larger LED on the main processor board blinks once.  5. The RMS (remote monitoring server), via syslog, should receive a status “STARTUP” including the FNAD’s identity and firmware version. Next, the RMS should show the FNAD connecting to the remote configuration server (RCS) to update the configuration settings. If the RCS is unreachable, the prior configuration settings are used. A later display will show the data center IP address and UDP/TCP link-up status.  5. If the FNAD configuration INI file setting: BOOTLINKDOWN is enabled, the FNAD will repeatedly rest itself (reboot) if and whenever the LAN link LED goes out. The FNAD can be reset by disconnecting the far end (at the switch) cable for a few seconds, or by interrupting power for a few seconds. |
| DATA CENTER (DC) ADDRESS | Project network personnel ensure that the DC server IP address, protocol and port number are in the INI file for all FNADs. |
| FNAD CONFIGURATION SETTINGS DEFAULTS RESET | The FNAD’s configuration settings can be reset to a set of default values as follows.   1. Press and hold the large push-button on the FNAD’s circuit board 2. Apply power to the FNAD or tap the small Reset button. 3. Within 15 seconds, the main-board’s LED should blink TWICE (it blinks ONCE during normal power-up without the large button held down).   The FNAD’s IP address, gateway and RMS/RCS IP addresses are now set to the defaults. |

# HARDWARE JUMPERS, BUTTONS and INDICATOR LEDs

**Ethernet Interface**. Green “link” LED is on when there is connectivity to the device on the cat5 cable. See INI file item “BOOTLINKDOWN”.



**LED:** A few seconds after startup, blinks once for normal startup, twice if reset defaults occurred (see below)

**BSL and JRST jumpers:  
NORMAL operation: OUT  
Use of PRIMARY BOOTSTRAP LOADER: IN**

**802.15.4 Transceiver/radio. Plug-in module.** Red LED should be on. Green LED is on when FNAD receives data or when rECoC senses NADAs while not sleeping.  
A U.FL antenna connector provides a connection for a short “pigtail” coax with an RP-SMA antenna connector for an integral or external antenna.  
  
MAC address: Shown in top side label and imprinted on bottom side of the module. The label shows the least digits of the MAC address **0013A2004061BB85.**

**SYSTEM Button: To reset to default configuration:** Push and hold during rebooting after a power-up or when the RESET button is released. After the secondary loader completes, the LED blinks TWICE indicating the configuration is reset to the default settings shown in this document.   
 Also, in operation, the rECOC uses this button to simulate sensor/lock state changes.

**RESET button.** Press/release to reset/reboot

**Ethernet Jumper:** “in” for FNAD using Ethernet. Optionally OUT for rECoC

**J1 power jumper: Always IN**

**LED JUMPER: Always IN**

**NAD Jumper:** “in” for NAD role; out for rECoC role

**Plug-in Interconnect PC board “daughtercard”.**  I/O and test sensors use connector at top/right edge of board.

**DC Power Input:** 6-9VDC from iontegral cat5 cable power extractor or from locally connected power transformer. The center conductor of the barrel connector *MUST* be the + voltage. Reversing the polarity may damage the ’15.4 radio.  
NOTE: Some wall transformers have reversible polarity settings or plugs with swappable polarity pins. Avoid reverse-polarity errors- when in doubt use DVM.

**RESET Button:** Push to reboot FNAD. Same effect as power off/on. Does not reset configuration.

**RS232 Serial DB9:** Syslog messages are sent here at 57.6Kbaud if the Ethernet link is down. Also used for flash memory loading in lieu of the RCS method. See section “Primary Bootloader Usage”.

# HARDWARE JUMPERS WHEN USING PRIMARY BOOTSTRAP LOADER

See document t section “FIRMWARE UPDATE using fnad serial port/PRIMARY BOOTSTRAP”



**DEBUG jumper  
NORMAL operation: OUT  
Use of PRIMARY BOOTSTRAP LOADER: OUT**

**BSL and JRST jumpers:  
NORMAL operation: OUT  
Use of PRIMARY BOOTSTRAP LOADER: IN**

| SAMPLE CONFIGURATION FILE (.ini) |
| --- |

The configuration files are “.INI” files stored on the Remote Configuration Server (RCS).

The RCS is an FTP server with a passive-mode FTP login for each FNAD and rECoC:  
 username: the letter x followed by the hexadecimal MAC address of the device’s 802.15.4 radio  
 password: (obtain from project personnel)

Each permitted login has a unique file directory (folder), perhaps named the same as the username. In that directory a file named “config1.ini” shall be present. Note: As of this writing, there are likely additions to be made to the INI files’ item types. A sample INI file’s contents is in this document.

**NOTE: The *FNAD CONFIGURATION SETTINGS DEFAULTS RESET action (see prior setting) causes the settings shown below to be applied and used at the next power-up reset. The defaults are identical for all FNADs. Thus the attempt to contact the Remote Configuration Server (RCS) will use these defaults. The FNAD’s LAN address will change – as will the LAN Gateway – and these could become incompatible with the actual local LAN. In this case, a local RCS computer at the [FTP] IP= address and with the correct INI file can be used to get the FNAD back in contact with the normal remote RMS and RCS.***

**CONFIGUATION SETTINGS AFER *RESET TO DEFAULTS* ACTION**

The **reset/default** values listed below allow the FNAD to contact an RCS at the to get FNAD-specific settings. This RCS must be at the [FTP] IP= address resulting from RESET TO DEFAULTS:

[LAN] IP=TBD; GATEW= TBD; MASK= TBD  
[SYSLOG] IP= TBD #RMS server  
[FTP] IP= TBD #RCS server, login is as described earlier (derived from MAC address)

**Important INI file settings, in priority order:**

Normally, the FNAD, after installation, can contact the remote RCS and RMS. This permits all settings to be remotely managed. This would normally be items such as FNAD channel number, NADA timing, Data Center IP/port/protocol. Of course, changing certain configuration settings will disrupt FNAD-to-RCS connectivity and require a RESET TO DEFAULTS and on-site actions as above.

[**VERSION**] ID= is for configuration management. INIFILE= allows the ini file name sought by the FNAD to be changed; use care in changing this. FIRMWAREFILE= is the name of the .hex firmware file sought by the Remote Firmware download/update option in the FNAD/rECoC.

[**FNAD**] section, IP address, gateway address

[**SYSLOG**] server IP address. This is the Remote Monitoring Server (RMS) server. The RMS may temporarily set to be an on-site laptop with a SYSLOG server running. RECURRING=n controls the time interval between routing FNAD reports

[**FTP**] server IP address list. This is the Remote Configuration Server (RCS). The FNAD tries an FTP passive mode connection to each non-zero address in this list.

[**FNAD**] UID\_NAD must agree with that expected by the data center. UID\_DC must be the Data Center for this FNAD.   
 CHANX=n must be the deployment-plan selected IEEE 802.15.4 channel, where n is the index item of [15.4] CHANS, 0..3.   
 PANIDX=n likewise, [15.4] PANIDS, where n is 0 or 1.

[**DC**] IP= is the data center’s IP address; PORT and PROTOCOL must match the data center’s expectations for each FNAD and its installation site. The port number may be the same for all FNADs, according to the DC’s design preferences.

------------------------------

For test purposes:  
[FNAD] TESTUS=b causes the FNAD to transmit to each ECoC a Send Unrestrictred Status message every n seconds, using message waiting. This enables basic testing independent of the Data Center.  
 [rECOC] values, where the same hardware/firmware for the FNAD can operate as a reference/test ECOC.

A sample INI file follows…

[VERSION] # SAMPLE-ONLY – ACTUAL VALUES ARE SITE-SPECIFIC

ID=3 #Config version

INIFILE=config1.ini # 31 chars max; change as needed

FIRMWAREFILE=firmware1.hex # 31 chars max; change as needed

[LAN]

IP=192.168.1.60 #NAD or rECoC LAN IPv4

GATEW=192.168.1.1 #gateway IP if WAN is accessed

MASK=255.255.255.0 #subnet mask

BOOTLINKDOWN=Y #Reboot while Ethernet NIC's Link LED is out

[SYSLOG]

IP=192.168.1.250 #SYSLOG server IP

FILTER=7 #Severity levels > n not sent; 0 to 7

RECURRING=60 #(Secs) Non-event recurring syslog report interval; 0=disable

[FTP]

IP1=192.168.1.250 #Remote Configuration Server (FTP server) IP, primary.

IP2=0.0.0.0 #alternate ; 0.0.0.0 if unused slot

#IP2=166.140.101.226 # lab; 0.0.0.0 if unused slot

IP3=0.0.0.0 #alternate ; 0.0.0.0 if unused slot

[DAYTIME]

IP1=192.43.244.18 #NIST daytime server rotation

IP2=129.6.15.28 #alternate

IP3=129.6.15.29 #alternate

IP4=64.90.182.55 #alternate

[DC]

IP=192.168.1.250 #data center

PORT=11001 #source and destination port no. TCP, UDP differ at DCP

PROTOCOL=UDP #protocol

DCHEARTBEAT=Y # if true, DCmust respond to FNAD heartbeats else FNAD reboots

#PROTOCOL=TCP #protocol 24Oct11 Not yet Supported

[15.4]

HIPOWER=N #Y or N; use highest available transmitter power (60mW for FNAD/rECoC), + antenan gain

CHANS=17,21,23,15 #decimal. List of 4 channels for network discovery; 0 if unused slot

PANIDS=6996,9669 #PAN IDs (two) for network discovery. hexadecimal numbers. 0 if unused slot

[FNAD]

UID\_NAD=0000000000000000 #16 hex digits, used in DCP messages

UID\_DC=0807060504030201 #16 hex digits, Used in NADAs

CHANX=1 #Chooses chan no. in the CHANS list of the "15.4" section, item #0 to 3 for NADAs

PANIDX=0 #Chooses PAN ID in the PANIDS listof the "15.4" section, item #0 to 1 for NADAs

NADAIDQ=20,1000,500 # I=20, D=1000, Q=500 # bursting, 20mSec for 1 sec then 1/2 sec of quiet

#NADAIDQ=100,0,0 # I=100, D=0, Q=0 #non=bursting, constant 100mSec intervals

TESTSUS=0 # Seconds. If non-zero, every n seconds FNAD posts msg waiting with SURS commands to ECoCs. Stimulates RF/data traffic

[rECOC]

REPEATSTATUS=15 # send status every n seconds

DWELLMS=100 #Network discovery, dwell time per channel while expecting NADAs

NADAage=10 #Seconds to tolerate loss of NADAs before redoing network discovery

SLEEPMS=900 #Miliseconds of sleep with radio disabled

WAKEMS=100 #Miliseconds after sleep, radio on, anticipating NADAs

L3UID=0000000000000000 #Level 3 device UID; 16 hex; 16 hex; If 0, use MAC address

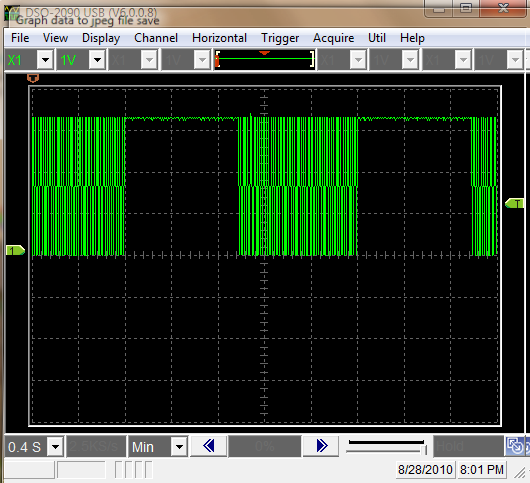
STATICKEYS=Y #Use static key at startup, rather than waiting for rekeying

LOGSYNTH=0 # number of event log records to synthesize for test purposes (w/unique event type code)

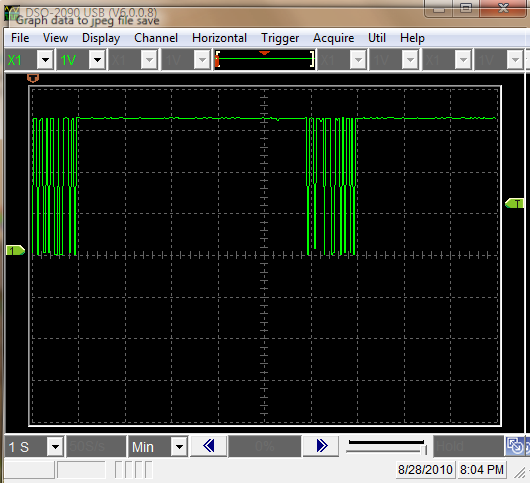
L3LTK=1234567890ABCDEF1234567890ABCDEF #Level 3 long term key if static

L3TCK=1234567890ABCDEF1234567890ABCDEF #Level 3 temporary key if static

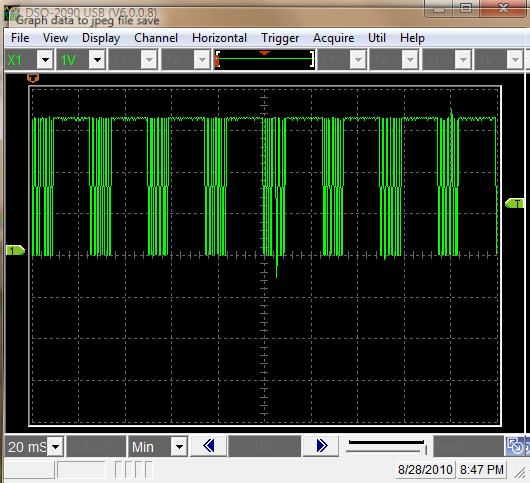
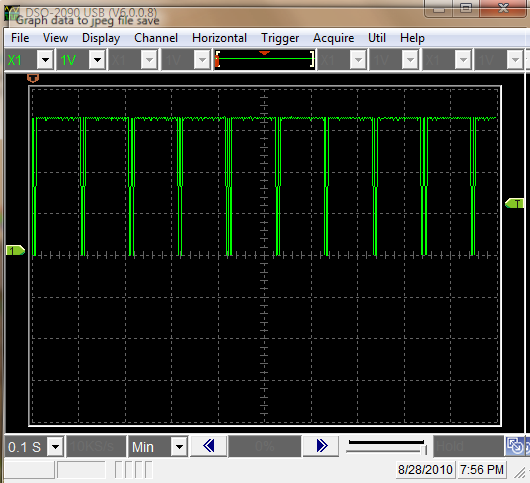
L3RKK=1234567890ABCDEF1234567890ABCDEF #Level 3 rekeying key  
#end



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| I,d,q settings | Inter-NADA | NADA Burst Duration | Quiet Duration | ‘Scope x-Axis |
| 20,1000,1000 | 0.020 Second | 1.0 Second | 1.0 Second | 0.4 Sec/division, 4 sec. total |



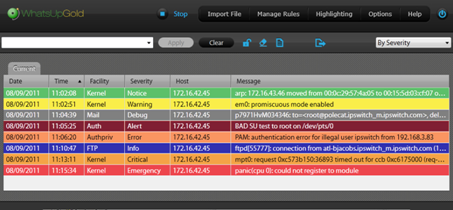
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| I,d,q settings | Inter-NADA | NADA Burst Duration | Quiet Duration | ‘Scope x-Axis |
| 20,1000,5000 | 0.020 Second | 1.0 Second | 5.0 Seconds | 1.0 Sec/division, 10 sec. total |



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Photo** | I,d,q settings | **Inter-NADA** | **NADA Burst Duration** | **Quiet Duration** | **‘Scope x-Axis** |
| Left | 100,100,0 | 0.1 Sec. | 0.1 Second | 0 Seconds | 0.1 Sec/division, 1 sec. total |
| Right | 20,20,0 | 0.02 Sec. | 0.02 Second | 0 Seconds | Sec/division, 0.2 sec total |

**NADA TIMING CHOICE EXAMPLES, AS OSCILLOSCOPE DISPLAYS**

| OPERATIONAL USE, COMMUNICATIONS-RELATED | |
| --- | --- |
| REMOTE MONITORING SERVER (RMS)  SOFTWARE | The RMS server accepts, logs and displays reports from FNADs (and rECoCs). This information is essential in a pilot program phase. An example generic display is shown in the graphic, below. The data format is per the IETF RFC standards RFC 3164, 5424 “SYSLOG”. The SYSLOG server application can be freeware PC software from any of several sources including IP Switch, Inc., downloadable from:  <http://www.whatsupgold.com/free-software/network-tools/syslog-server.aspx>  Add-ons, plug-ins and professional upgrades to this and similar SYSLOG capable software can be used. |
| FNAD REPORTS TO RMS | FNADs report to the RMS with:   * STARTUP information as to firmware version, ID, channel, PAN ID, etc. * Recurring status including number of ECoCs in range and their signal strength, number of NADAs transmitted (ever-increasing number), number of clear channel assessment faults (if too high, indicates sustained inter- or intra-system interference), and other items. * Recurring report of neighbor-FNADs on the same 802.15.4 channel and their received signal strength. Same-channel FNADs must receive and “ignore” NADAs sent by neighbor-FNADs * Newly detected ECoCs and their MAC, UID and received signal strength * Receipt of each message from an ECoC, with received signal strength and the unencrypted message header. (FNADs cannot decrypt message content.) * Receipt of messages from the data center (SCMS/DCP) via Ethernet and wireless forwarding to the addressed ECoC, with receipt verification (MAC ACK). * Notice of to-ECoC message queuing for message waiting * Notice of dequeuing messages-in-waiting and transmission success with receipt verification (MAC ACK). * Notices of MAC ACK failures indicating too-weak signals or ECoCs in power conservation pending future message-in-waiting transmission by FNADs * Errors and anomalies such as timeout retransmissions |
| FNAD NETWORK DISCOVERY CONFIGURATION SETTINGS  AFFECTING  NADA BROADCASTS | Per the DHS ICDs, the FNAD operates on one of four possible channels and one of two possible PAN IDs. Using these, the FNAD produces NADA broadcasts on IEEE 802.15.4. The timing of the NADA messages is in the configuration INI file from the RCS. The timing adjustments are:  “I” interval: Intra-NADA time, 20-100 mSec  “d” duration: For bursts of NADS followed by a “quiet” time, d is 20 to 1000 mSec. For NADAs continuously transmitted, without “quiet” times, d = 0.  “q” quiet time”: Where d is not zero, q is the inter-burst no-transmisions time, 20-500mSec.  NADAs are transmitted after clear channel assessment succeeds though NADAs are broadcast to all in the PAN ID.  Collocated FNADs may but preferably should not use the same channels. Antenna pattern alignment sometimes reduces this “co-channel” intra-system interference. For INTER-system interference reasons, when other wireless services at the site exist, such as 802.11/WiFi, and operates with overlapping frequencies, the chance of clear channel assessment failures increase. If FNADs use a high-rate NADA “I” interval, e.g., 20mSec, the IEEE 802.15.4 MAC layer CCA backof settings may cause MAC ACK timeouts or retransmissions due to CCA faults. The FNADs’ 802.15.4 transmissions occupy 2MHz of spectrum; 802.11 transmissions occupy ten-fold more: 20MHz. Both 802.15.4 and 802.11 are packet/frame based CSMA/CA (listen before transmitting) protocols. Rarely do signals occupy a large percentage of time, i.e., transmissions are sometimes delayed by a few mSec. The details of this inter- and intra-system competition for clear-air time and co-channel interference is beyond the scope of this document. |
| REMOTE CONFIGURATION SERVER (RCS) | The RCS is a standard File Transfer Protocol (FTP) server which supports FTP PASSIVE MODE per the RFCs. For site firewall compatibility, passive mode FTP means the FNAD initiates a TCP connection to the FTP server, requests a file transfer, then the FNAD initiates another TCP connection to the server to do the transfer. The server tells the client (FNAD) which port number to use for the transfer. Therefore, all connections are FNAD-initiated, outward through the site’s firewall, per common policy.  An acceptable server for this is open freeware called Mozilla FileZilla.  The FNAD has a list of one or more RCS (FTP) servers with which to attempt connections. Thus, some FNADs may use one RCS and others are configured to use a different RCS, if desired.  FNADs contact the RCS only at startup initiated by power-up or if enabled, by a certain data center command. The latter is needed after the FNAD’s INI file is changed and needs to be downloaded by the FNAD. |
| FNAD CONFIGURATION DATA AND STORAGE | The FNADs store their latest configuration data in non-volatile “flash” memory. Initially this memory is “blank”, so the FNAD uses the DEFAULT configuration data. This is the same configuration used after the RESET TO DEFAULTS action is invoked on-site by a person pushing the proper button inside the FNAD at startup.  The FNAD obtains from the RCS (FTP) server configuration data. This is stored in the non-volatile flash memory, superseding any prior data.   The IP address of the RCS, when the DEFAULTS are used, is in a default subnet and a default RCS address.  The configuration DEFAULTS (in final form) include an RCS IP address that is unlikely to change. No single default for FNAD IP and gateway is possible among many sites’ LANs.  Thus, going from DEFAULTS to a downloaded-from-RCS configuration INI file would be done once, ideally, only at installation time. After that, the RCS INI files can be altered as needed, with care not to use values that prevent the FNAD from contacting the RCS via the LAN’s subnet gateway. Worse-case, the FNAD with wrong IP/gateway configured values can be RESET to defaults and an on-site RCS (on a laptop) can make available the correct INI file on a one-time basis.  Configuration data is stored in the top 2KB of the second to last 8KB block in flash. The last/highest-address 8KB block contains the primary bootloader. |
| DATA CENTER REPORTS TO RMS | The project’s SCMS and Portable Data Center (PDC) applications may send notices to the RMS. This can help create centralized event histories used in debugging system problems during tests. |
| rECoC REPORTS TO RMS | Reference ECoCs used in testing send RMS reports including   * Network Discovery: Number of NADs per channel, each channel * Best-NAD choice based on signal strength * Loss of coverage, repeating network discovery * Unsolicited and solicited message exchanges with ascension numbers * Errors and anomalies such as timeout retransmissions |
|  |  |



**Example generic SYSLOG display**. Each row is an event received from a device. Severity codes for each record cause differing colors (colors are user-chosen). Users may set filters to see only specific sources (FNADs) or event types, severity, etc. Records are written to disk for use by other display visualization software such as map/image overlays with icons. COTS add-ons to SYSLOG servers enable data mining, trends detection, retrospective reviews, etc.

The event data may be duplicated/forward to and/or viewed by authorized users with access to the RCS.

# FIRMWARE UPDATE using fnad serial port/PRIMARY BOOTSTRAP

The current firmware version (build date/time) is displayed at FNAD startup at the Remote Monitoring Server via the SYSLOG protocol. It is also sent to the FNAD serial port (57.6Kbaud) at startup.

Firmware updates may be *remotely* installed via an Ethernet LAN connection to the Remote Configuration Server (RCS) using the SECONDARY LOADER. The SECONDARY LOADER if installed in the FNAD enables remote firmware updates via the LAN/WAN. The SECONDARY LOADER is project-developed firmware optionally installed once using the PRIMARY BOOTSTRAP LOADER.

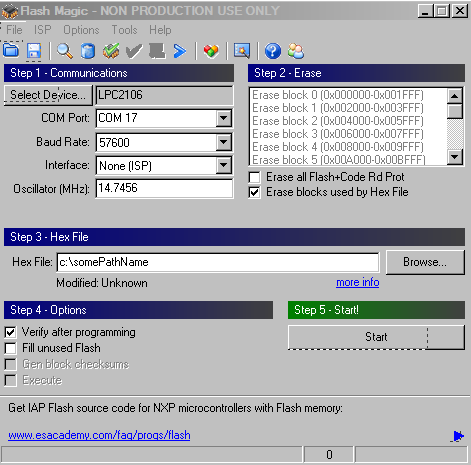
The PRIMARY BOOTSTRAP LOADER may be used by a person with physical access to an FNAD to install FNAD firmware. The PRIMARY BOOTSTRAP LOADER is ever-present firmware in the ARM CPU on the FNAD’s main board.

In normal FNAD operation, the PRIMARY BOOTSTRAP LOADER is *disabled* by the hardware jumper settings. See this document section *HARDWARE JUMPERS WHEN USING PRIMARY BOOTSTRAP LOADER* for the locations of these jumpers. When disabled, no firmware update is possible except by use of the optional SECONDARY LOADER. When the PRIMARY BOOTSTRAP LOADER is jumper-enabled, firmware updates are done on-site only, with a PC connected to the serial port DB9 of the hardware.

Install on a MS Windows PC install the freeware utility “Flash Magic” for Windows PCs. Obtain this program by requesting from teammates or download it: <http://www.flashmagictool.com/>

Obtain new firmware’s “.hex” file via email, etc. Then:

1. Enable the PRIMARY BOOTSTRAP LOADER: Set FNAD board hardware jumpers: BSL “in”; JRST “in”; DEBUG “out”. See document section “HARDWARE JUMPERS…”.
2. Connect PC ‘s serial port or USB-to-serial cable to FNAD’s DB9 connector.
3. Run the Flash Magic program and choose the proper COM serial port number for the real or USB-to-serial port. Set the baud rate to 57600 or lower.
4. Reset the FNAD board (power cycle or press reset button)
5. Use Flash Magic’s menu: ISP/Read Device Signature. Confirm success
6. Ensure Flash Magic’s data entry “Oscillator (MHz) is 14.7456
7. See Flash Magic example display on next page.
8. On flash magic’s Hex File entry: Choose the relevant new firmware file received by email or other means.
9. Click START. Observe success.
10. Disable the PRIMARY BOOTSTRAP LOADER: Set board’s jumpers: BSL “out”; JRST “out”
11. Optional: Follow the RESET TO DEFAULTS procedure at power-on (On FNAD, push/hold larger SYSTEM push button at power on or reset).
12. Observe the onboard LED blinks once at power-up.
13. Use the RMS/Syslog server to confirm proper operation and firmware version.
14. Use the RCS to apply the correct configuration using the RCS’ FTP server and INI file.



**Primary Bootloader, PC side Flash Magic software display.** Some PCs will require a baud rate lower than 115200. The Flash Loader automatically determines the PC’s baud rate.

| SECONDARY LOADER (SL) USE | |
| --- | --- |
| OPTIONAL FIRMWARE | The secondary loader is firmware optionally installed in FNADs and rECoCs. Its purpose is to enable remote FNAD operational firmware updates only from the project’s Remote Configuration Server (RCS) as needed. |
| FIRMWARE FILE NAMES AND RETRIEVAL PROCEDURE | At power-on/reset, the SL uses passive-mode FTP to attempt to retrieve new operational firmware from Remote Configuration Server (RCS) . If attempts fail (i.e., file not found or non-responsive server), the SL runs the previously installed firmware. Progress is reported to the RMS via SYSLOG. If the FTP transfer of new firmware was incomplete, the SL reboots and retries. The FTP username/password is either (a) that given in the INI file for the FNAD’s identity or (b) a default value of *firmwareDefault,*  *firmwareDefaultpass*. The FTP server should have a login enabled for the default, when needed. The default is used if (1) the SYS pushbutton is pressed during power-on or (2) if the non-volatile memory for configuration (INI) data is erased. The default FTP server IP address is used, q.v. For (2) without defaults, the FTP server IP is either of 3 listed in the INI file and the username/password is based on the MAC address of the 802.15.4 radio (but not listed in this document). |
| CONFIGURATION DATA PRESERVATION | The SL preserves the last-saved FNAD configuration data settings as given in the RCS INI file for each FNAD/rECoC based on MAC address. These contain the IP address of the FNAD, the LAN gateway, the RCS server and the RMS server used during the SL processing. As noted above, the INI file also has the file name for firmware dowbnloads. |
| STARTUP WITH SL | At power-up the PRIMARY BOOT LOADER always runs. If it is jumper-disabled, as is the normal condition, control goes to the code beginning at location 0 in flash memory.  Without the SL, the FNAD application firmware runs from location 0.  With the SL, the SL runs at power-up reset from location 0 and when finished, control goes to the application in the memory block above the SL. |
| SIZE OF DOWNLOADED FIRWARE | A full update may take several tens of seconds. Replacement firmware is in Intel .hex format and thus somewhat larger than the binary equivalent as in memory. A typical file size may be 50-75KB. The transfer rate is likely limited not by LAN speeds, but by the time to parse/validate the data then erase and rewrite flash memory block, this being milliseconds per block. |
| SECONDARY LOADER ERROR RECOVERY | The size of the CPU’s flash memory is larger than the size of the RAM in the microprocessor. There is no off-chip memory. Therefore, if a non-recoverable error such as a failure to receive the entire file, the SL resets the CPU causing the SL to run anew. Now, the “Download required” flag is on in the non-volatile memory. Thus the SL repeats the mandatory download to error correct and does so until the operational firmware download is completed successfully. |
| REMOTE MONITORING SERVER (RMS) | The SL reports progress, status and activities to the RMS SYSLOG server. The IP address is that given in the INI file, or the IP address set if defaults are invoked via the SYS push-button. |
|  |  |

| FUNCTIONAL DESCRIPTION SPECIFICS | |
| --- | --- |
| ROLE | The FNAD enables on-conveyance security and monitoring devices to securely communicate with distant data management center(s). The devices are located on or in shipping conveyances such as intermodal shipping containers transported by truck, rail or maritime means. The information exchanged status and device control and may also include other commercial-purposed information. The FNADs are the devices’ access to remote data centers. The FNADs are immobile and are located at points of origin such as manufacturers’ loading docks, and at inspection points such as border crossings, intermodal port facilities, and at consignees’ destination points such as a manufacturing facility. An FNAD implements the “non-secure network access device” as defined in two communications Interface Control Documents (ICDs):   * Communication xxxxxxxxx * NAD to DCP Communications xxx   The term “non-secure” means that sensitive information is encrypted by the on-container device (e.g., ECoC) prior to transmission to an FNAD and onward to a data center. Vice-versa, the data center encrypts prior to transmission. The FNAD is a “data bridge”, and cannot decrypt. Since FNADs are unattended devices located outdoors with the possibility of theft, this transparent bridge role is key. |
| PHYSICAL | The electronics portion of an FNAD is mounted in a variety of suitable types of weatherproof enclosures. These include a simple “box” with an external antenna and an enclosure with an integral antenna. These are depicted below:  [photos here] |
| NETWORK TRANSPORT SECURITY | Sensitive data is AES encrypted by the on-container device and by the data center at the application message level. There is no reliance on security within wireless/wired transport networks between the end points. Authentication, key management and key distribution mechanisms are defined in project ICDs. |
| ANTENNA | The per-FNAD choice of antenna type is made during deployment planning to tailor and shape the wireless coverage to meet the need. The coverage shape and size accommodates the required areas of coverage, e.g., a linear space on a road with/without a curve/turn, etc. Antenna types include low-gain and high-gain omni-directional, narrowed-beamwidth yagii, sector or panel, and parabolic dish. Antennas are installed with either horizontal or vertical polarization according to the requirements and plan, and the characteristics of the on-container devices. |
| WIRELESS FREQUENCY AND FORMAT | The international 2.4GHz unlicensed band is used for wireless access by the on-container devices via the FNAD. Specific frequencies (channels) are used per the ICDs. All wireless transmissions are formatted per the IEEE 802.15.4-2006 standard. The ICD defines the exact format and options used in the standard. These conventions enable co-existence with other on-site 2.4GHz wireless systems and conformance with international regulatory requirements (US FCC equivalents). |
| WIDE AREA NETWORK CONNECTION | The wide area network (WAN) connection is common Ethernet IEEE 802.3 10/100BT via a standard RJ45 connector inside the FNAD’s enclosure. A standard category 5 cable is used. Optionally, power may be via this cat5 cable, as described below. The cat5 cable may lead to a switch/router or to a wireless bridge to reach a switch/router |
| LOCAL AREA NETWORK (LAN) | The FNAD’s Ethernet connects directly or indirectly (e.g., via a wireless bridge) to the facility’s local area network. This LAN leads to a WAN gateway with connectivity for the remote data center(s).  Each FNAD uses the following LAN configuration information: - Static private or public IPv4 address - Gateway IP address - Data Center protocol (UDP/TCP), IP address and port number - Remote Monitoring server (RMS) IP address; FNAD-out only - Network Configuration Download Server IP address (usually same as above) The FNAD obtains these values as explained in the Network Management section below. A default set of values is used when the FNAD is “reset to defaults” by user action (see “Reset to Defaults” section.) |
| SITE FIREWALL/ROUTER COMPATIBILITY | Each FNAD communicates with these remote systems:  - A network time server (NIST) to retrieve date/time UTC - One Data Center (a.k.a. SCMS or DCP) - One Remotre Monitoring computer: FNAD-out; SYSLOG per RFC - One Configuration data management computer (often same IP address as above): FNAD-initiated FTP connection, passive mode dynamic port (SPI) |
| REMOTE COMMUNICATIONS EVENT MONITORING | The Remote Monitoring Server (RMS) computer receives detailed communications status and events from each FNAD. Encrypted message content is not sent, nor does the RCS have the keys to decrypt. The received data is displayed and logged/archived. The RCS’ displays may be remotely viewed by authorized personnel who are at any site. Data analysis automation at the RMS reveals details of anomalies during testing and pilot project operations. The RMS is passive and receive-only. It cannot “command” FNADs. |
| CONFIGUATION SETTINGS MANAGEMENT | Each FNAD’s configuration settings that are stored in non-volatile flash memory of the microprocessor. These settings are established at installation time. Thereafter, each time the NAD is powered-on, it connects to the Network Configuration Server (RCS) computer using an IP address defined in the FNAD configuration settings. This is via the site’s LAN and gateway. Via this connection, the FNAD may obtain revised settings managed remotely. If the settings become invalid due to error or hardware fault, the FNAD may be reset to use configuration default setting values. To do this, see “Reset To Configuration Defaults”, below. Figure ?? shows all settings maintained at the Network Configuration Server (RCS) computer and downloaded by the FNAD at each power-up/reset. Note: If the remotely managed settings (INI file) states an incorrect IP address for the NAD, LAN Gateway or RCS, it is necessary to do the Reset To Configuration Defaults procedure, as below. Meanwhile, the FNAD will continue to send SYSLOG reports on connectivity success to the defined SYSLOG server IP address; this is useful in the process.  Project communications personnel maintain each FNAD’s username/password used by the FNAD to retrieve settings from the Network Configuration computer. |
| RESET TO CONFIGURATION DEFAULTS, PROCEDURE | Rarely needed: To reset the FNAD to a set of pre-defined default values shown in Figure ?? below, do the following:  1. Remove the FNAD’s enclosure cover 2. Refer to Figure ?? below for a visual of the button locations within the FNAD 2. With power applied, press and hold the larger push button on the microprocessor board  3. Holding the button as above, briefly press and then release the RESET button 4. Observe that the LED on the main board flashes twice, about 10 seconds after the RESET button is released.  Note: It is likely that the values for the FNAD IP address and LAN gateway after the reset, are incompatible with those for the site’s LAN. Methods to reinstate the preferred FNAD settings include the following and others:  1. Connect the FNAD’s Ethernet port to a cellular router with Internet access. This router would be configured to be the gateway IP given in the RESET defaults. With this, the FNAD can connect to the remote Network Configuration computer and download/save the managed configuration settings for the LAN/WAN and FNAD operational values.  2. Connect the FNAD’s Ethernet port to a laptop PC whose static IP address is that given in the default values. An FTP server with login and INI file for the FNAD’s MAC address permits the FNAD to download/save settings.  The FNAD should now be reconnected to the site LAN. |
| REMOTE FIRMWARE UPDATES | If this option is installed and enabled, the FNAD will connect to the Network Configuration computer to check for the availability of an update (later version) of the operational firmware used by the FNAD. The firmware for FNADs is all identical. However, each FNAD’s login to the Network Configuration computer enables a unique-per-FNAD firmware file so that FNADs may optionally have differing firmware, e.g., special test uses, etc.  Project communications support personnel maintain each FNAD’s username/password used by the FNAD to retrieve firmware updates from the Network Configuration Server (RCS) computer. |
|  |  |
| ON-SITE FIRMWARE UPDATES | Rarely needed: The FNAD’s built-in bootstrap loader can accept firmware loading via the RS232 serial port connected to a laptop computer. Another scenario for on-site updates is explained in the “Reset To Defaults” section. |
| FNAD HARDWARE DESCRIPTION | Commercial off-the-shelf (COTS) microprocessor circuit board: Industry Standard multi-vendor ARM CPU, 128KB flash RAM, 64KB RAM. The project firmware runs on the ARM under the open-source FreeRTOS operating system for small unattended/embedded processors. The Ethernet interface is a COTS Wiznet 812MJ product module; This module contains, internally, all required IP protocols for four concurrent connections, i.e., independent of the ARM processor’s multi-tasking RTOS and project firmware. The project firmware requires less than half of the 128KB flash – reduced in size from prior FNAD versions as the FNAD HTTP and Telnet servers are removed to meet likely IA requirements for the STC pilot. In their place is the remote monitoring and firmware update mechanism described above. The wireless transceiver is a COTS IEEE 802.15.4 Wireless product Digi XBee Pro series 1 with up to 60mW transmitter power (excluding antenna gain). The ARM CPU interfaces to this transceiver via a standard serial interface at high speed. The IEEE 802.15.4 protocols within the transceiver are certified for compliance by the vendor and are not modified for this project. No project firmware runs on the transceiver nor alters the transceiver’s firmware or timing.  A project-specific passive PC board interconnects the COTS modules. All COTS items are low cost, mature and in long term volume production. |
|  |  |