SNIB3 1.07 Release Notes

Overview

This document describes the new features and enhancements of the Secure Network Interface Board v3 (SNIB3), compared to the previous SNIB2. This document also summarizes the Known Limitations in the 1.07 release of the SNIB3 firmware.

The versions of the SNIB3's firmware components in this release are:

Firmware:	**01.07.0000**
OS:	**01.04.0000**
Driver:	**01.05.0000**

The required versions of associated programs to support the SNIB3 are:

Velocity:	**3.6 SP1**
CCM:	**7.5.37**

If the SNIB3 is on the same network subnet as the Velocity host, then you will configure it using Velocity. If the SNIB3 is on a different subnet, then you will begin to configure it using the SNIB Configuration Tool. While trying to discover SNIB3s, you should temporarily disable port monitoring tools (such as Norton Antivirus and Windows firewall) or add **velocity.exe** and **SNIBConfigTool.exe** to the exceptions list.

Upgrading the firmware of downstream SNIB3s must be done one at a time. In a master-slave configuration, you must upgrade the master SNIB3 board's firmware first, and then upgrade each slave SNIB3 board's firmware in sequence. Don't start the download for the next SNIB3 board until the firmware upgrade for the previous SNIB3 board has completed.

Information about installing and configuring the SNIB3 is provided in the **SNIB3 Quick Installation Guide** which is included with each order. Complete information about the SNIB3 is included in the latest version of the **DIGI*TRAC Systems Design and Installation Guide** (dated 6/9/2016).

NOTE: Extreme power surges, such as those caused by nearby lightning strikes, might damage the Ethernet port on the SNIB3 communications board. To prevent damage, surge protection must be provided for the master SNIB3 in each chain of connected controllers, using the Sankosha Guardian Net LAN-CAT5e-P+ surge protection device. For details, see the **Providing Surge Protection for a Master SNIB3** topic in the **DIGI*TRAC Systems Design and Installation Guide**.

New Features and Enhancements (compared to the SNIB2)

☐ Faster Ethernet Speed

The standard RJ-45 Ethernet port included on the SNIB2 enables the connected controller to communicate with the Velocity host using TCP/IP over 10BaseT or 100BaseT Ethernet networks. The SNIB3's RJ-45 Ethernet port is capable of 10BaseT, 100BaseT, or 1000BaseT (gigabit) speeds.

☐ IPv6 for Addressing

The SNIB3 supports version 6 of the Internet Protocol, which uses 128-bit addresses to identify and locate devices on the Internet. (The previous IPv4 used 32-bit addresses.) Although the SNIB3 supports dynamic IP addressing using the Dynamic Host Configuration Protocol (DHCP) for both IPv4 and IPv6, Identiv strongly recommends using static or reserved IP addresses for your SNIB3 boards.

☐ AES Encryption with 256-bit key length

The SNIB3 supports more robust encryption (with a 256-bit key length) through the XNET3 protocol. (If you are using SNIB2 boards in some of your controllers, you cannot use the XNET3 protocol, and those controllers must be downstream slaves to a master SNIB3, connected using the RS-485 port.)

☐ FIPS 140-2 Certification

The SNIB3's cryptographic modules use the OpenSSL library, which has been certified by the National Institute of Standards and Technology (NIST) to meet their Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules. (The Velocity software uses Microsoft's BCRYPTPRIMITIVES library, which also has been certified by NIST to meet FIPS 140-2.)

☐ Hardware Security Authentication Module (SAM)

The SNIB3 has a hardware Security Authentication Module for securely storing keys. One application for this module is to secure firmware downloads, using a TRN format as used on Touch Secure readers. In this method the firmware is first verified for authenticity by using the SAM keys before downloads are allowed.

Deprecated Features

The following features have been deprecated (relative to the SNIB2):

- RS-232 support for connection to the host computer (you must use RJ-45 Ethernet instead)
- Downstream support for an original SNIB on RS-485 serial connections

Note that the SNIB3 is backwards compatible with the SNIB2, but not with the original SNIB. You cannot use the SNIB3 with the M1N controller, because it does not support any expansion boards. To use the SNIB3 with an Mx controller, you must first remove the SNIB2 daughterboard from the Mx controller's main board.

Known Limitations

SNIB3 supports only 16 downstream controllers

Although the SNIB3 (like the SNIB2) is intended to support up to 63 downstream controllers when using NET*MUX4s, this feature is not yet implemented. In this initial release, a SNIB3 can support up to 16 downstream controllers.

Recommended Baud Rate for master/slave communication is 9600

For RS-485 serial connections between a master SNIB3 and downstream SNIB2s or SNIB3s, the SNIB3 works best when the baud rate is set to 9600 bps.

Simultaneous downloads of many credentials can cause the downloads to hang

Occasionally, the simultaneous download of a large number of credentials to a master SNIB3's controller and all of its downstream controllers can cause the downloads to hang. When this occurs, you must either disconnect and reconnect the master SNIB3's network cable or reboot the master SNIB3's controller, after which the download will continue where it left off. For this release, we recommend downloading credentials to one controller at a time.

Time taken by a SNIB3 master controller with address 1 to identify a SNIB3 slave with address 63 is more than the time taken by SNIB2 Master to identify a SNIB2 slave. (FAL-703)

When powering on slave controllers then the master controller, the controller login messages received in Velocity indicate that it takes longer to complete the login process using SNIB3-connected controllers (50-55 seconds) than it takes with SNIB2-connected controllers (25-30 seconds). There is currently no workaround for this problem.

Simultaneous Firmware Download of slave controllers results in firmware download error (FAL-724)

When attempting to download firmware updates simultaneously on two or more downstream SNIB3-attached controllers, a firmware download error will occur. This is a previously documented problem that occurs in both SNIB2- and SNIB3-attached controllers.

Workaround: It is recommended and standard practice to only download firmware to one controller at a time on a given port. Attempting to download firmware updates to more than one controller at a time will result in firmware download errors.

When changing from XNET2 to XNET3 mode, controllers are logged off, but port shutdown does not happen (FAL-729)

If you attempt to change the mode of downstream controllers from XNET2 to XNET3 protocol, the controllers log off but a proper port shutdown does not occur.

Workaround: The port has to be disabled and re-enabled to reconnect it with the controllers.

State-full IPv6 addresses are not supported (FAL-772)

Because state-full IPv6 addresses are not currently supported, if your network uses only state-full IPv6 addresses, a SNIB3 will not be discoverable. (A SNIB3 will be discovered if it is using static IPv6 addressing, stateless IPv6 DHCP addressing, or IPv4 addressing.)

After starting up and synchronizing with the CCM, there is a 5-second delay before the SNIB3's LEDs display normal patterns (FAL-846)

After a controller is powered on, its SNIB2 or SNIB3 board displays a circular pattern on its LEDs while synchronizing with the CCM. Then various other patterns are displayed during normal operations. But with the SNIB3, there is a 5-second delay after synchronization before the LEDs start displaying the patterns for normal operations.