

HYPER SCADA SERVER

QUICK START GUIDE



MODELS HSS002-1 AND HSS002-2

HSS Serial Number	NFM Serial Number
HSM1 Serial Number	HSM2 Serial Number
NSM1 Serial Number	NSM2 Serial Number
PSM1 Serial Number	PSM2 Serial Number

HSM (1) IP Address: _____

HSM (2) IP Address: _____

Backup Computer IP Address: _____

Shared IP Address: _____

Safe IP Address: _____

NOTICE

Data Flow Systems, Inc. assumes no responsibility for any errors that may appear in this document, nor does it make any commitment to update the information contained herein. However, questions regarding the information contained in this document are welcomed.

Data Flow Systems also reserves the right to make changes to the specifications of the Hyper SCADA Server, Hyper Server Module, Network Interface Module, Fiber Interface Module, Network Fiber Module, Network Switch Module, and the HT3 SCADA software and to the information contained in this document at any time without notice.

© Data Flow Systems, Inc.
605 N. John Rodes Blvd., Melbourne, FL 32934
Phone 321-259-5009
Fax 321-259-4006
www.dataflowsys.com

DFS-00384-011-01

This document last updated June 9, 2010

This document describes the basic procedures for cabling and configuring the Hyper SCADA Server models HSS002-1 and HSS002-2. The instructions provided are for a “typical” setup. A typical setup is one in which:

- User access is via client computers on an Ethernet network; or from a dedicated workstation directly connected to the HSS
- Telemetry system consists of a system of Network RTUs connected to the HSS via a rack-mount media converter; or a Tunnel CTU directly connected to the HSS.

For detailed cabling and installation information and for instructions on “non-typical” setups, see the Hyper SCADA Server Installation and Operation Manual, which is available for download from DFS’ website (www.dataflowsys.com). For detailed information on configuring HT3, see the HT3 User Guide (available from within the HT3 software and also available on the DFS website).

PARTS LIST

- ❖ Hyper SCADA Server (HSS002-1 or HSS002-2), which includes the following components:

HSS002-1

- One Hyper Server Module (HSM001)
- One Power Supply Module (PSM003)
- One Network Fiber Module (NFM001-X); additional NFM may be required if connecting to a network RTU or dedicated master workstation located more than 100 meters from the HSS.
- One Network Switch Module (NSM001)
- One 7.0 AH battery
- One DIN-rail mounted telephone line surge arrester with two jacks (Line In and Line Out)
- One DIN-rail mounted Category 5 network surge arrester

HSS002-2

- Two Hyper Server Modules (HSM001)
- Two Power Supply Modules (PSM003)
- One Network Fiber Module (NFM001-X); additional NFM may be required if connecting to a network RTU or dedicated master workstation located more than 100 meters from the HSS.
- Two Network Switch Modules (NSM001)
- Two 7.0 AH batteries
- One DIN-rail mounted telephone line surge arrester with two jacks (Line In and Line Out)
- One DIN-rail mounted Category 5 network surge arrester

- ❖ 4 (four) mounting brackets
- ❖ 4 (four) mounting screws
- ❖ Hyper SCADA Server Quick Start Guide

WHAT YOU’LL NEED

- One (1) static IP address for *each* HSM
- One (1) static IP address for Tunnel CTU
- One (1) static IP address to be used as Shared IP (HSS002-2 only)

- One (1) designated static IP address to be used as a Safe IP (HSS002-2 only)
- Local Area Network (LAN) or master workstation
- Three (3) to five (5) CAT5 patch cables terminated with RJ-45 connectors
- One (1) CAT5 cable to cover distance from HSS to LAN/master workstation
- Fiber optic cables terminated with ST/SC connectors
- Configuration jumpers (black #16 stranded wire)
- Telephone cable terminated with RJ-11 connectors
- Computer with Windows 2000 or XP operating system installed
- PS-2 Keyboard and VGA monitor (connected to HSM when configuring IP address)
- NIM/FIM for Tunnel CTU or Network RTUs

INSTALLATION CHECKLIST

- ✓ Unpack the HSS002-X
- ✓ Mount HSS002-X to wall
- ✓ Install the HSS002-X's modules
- ✓ Connect to network or dedicated workstation
- ✓ Connect to Tunnel CTU or Network RTU system
- ✓ Connect telephone lines for dial in and dial out
- ✓ Connect audio device (optional)
- ✓ Connect external alarm light/horn/alarm silence button (optional)
- ✓ Connect power
- ✓ Connect keyboard and monitor to HSM and configure HSM's IP address
- ✓ Configure hosts file on workstation
- ✓ Connect to HT3 (modify browser settings; install plug-ins and java policy file; start HT3)
- ✓ Configure redundancy (HSS002-2 only)
- ✓ Configure backup location

WARNING

The HSS should only be installed and serviced by DFS personnel or other qualified technicians.

The HSS must be installed in accordance with all national and local wiring rules.

WORKSTATION SPECIFICATIONS

With the HT3 system, you can use Windows-based computers, or workstations, to access the Hyper SCADA Server (HSS). The HSS is a Linux-based server that runs the HT3 SCADA software and MySQL database. You can have multiple Windows workstations connected to the HSS through a local area network. A Windows-based workstation provides you with access to all HT3 functions.

We recommend that one computer be designated as a dedicated primary workstation. This computer's main function would be to interface with the HSS and would remain on at all times.

Minimum Requirements for a Workstation Computer*

- Windows XP with SP2
- Internet Explorer 8.0
- Java 1.5

*Microphone required for recording voice alarm announcements

PROTECTING AGAINST ELECTROSTATIC DISCHARGE

Static electricity can harm delicate components inside the HSS. To prevent static damage, put on an electrostatic discharge wrist strap before touching any of the HSS' electronic components.

In addition to the preceding precautions, the following steps can be taken to prevent damage from electrostatic discharge (ESD):

- When unpacking a static-sensitive component from its shipping carton, do not remove the component's antistatic packing material until ready to install the component in the HSS. Be sure to put on an electrostatic discharge wrist strap before unwrapping the antistatic packaging.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components in a static-safe area. Place the equipment on a grounded surface. If possible, use antistatic floor pads and workbench pads.

Note: Contact DFS if electrostatic discharge packaging is needed for return shipments. See Return Authorization (RA) Procedure, p. 29 for more information on returning equipment.

UNPACK THE HSS

IMPORTANT: When handling the HSS002-X's components, follow the instructions in "Protecting Against Electrostatic Discharge" (previous section).

The HSS002-X enclosure and modules are shipped separately in two or more boxes.

1. Carefully open all boxes and locate the box that contains the enclosure. Remove the enclosure and visually inspect it.*
2. From the box that contains the modules, carefully remove each module from its packing and visually inspect it for shipping damage.*

* If any equipment appears damaged, read the information in the Return Authorization (RA) Procedure (p. 31) for instructions on having the equipment replaced or repaired.

MOUNT THE HSS

IMPORTANT: The HSS is designed to be mounted to the wall in a vertical position. This ensures proper air flow through the enclosure and provides easy access to the internal devices. Do not install the unit in a horizontal position or lay the unit down on its front, top, back, or sides.

The HSS is designed to operate in an air conditioned, moisture-free, office-type environment [41-86°F (5-30°C)]. When selecting an installation site, make sure that it provides an acceptable environment.

There are four mounting bosses on the back of the unit for attaching the brackets to the enclosure. Attach the 4 (four) mounting brackets to the back of the HSS' enclosure using the supplied screws. Use all four brackets to ensure that the unit will be securely mounted. The mounting brackets may be aligned vertically or horizontally. After attaching the brackets to the enclosure, securely fasten the HSS to the wall in the desired location.

INSTALL THE MODULES

Refer to the diagram in "Internal Connections" (next section) for correct placement of modules. Modules can be identified by their affixed labels.

When inserting modules, line up the module's card edge connector with the slot and apply gentle pressure. Never force a module into a slot. If the module does not snap into place easily, realign the connector to the slot, and try inserting it again.

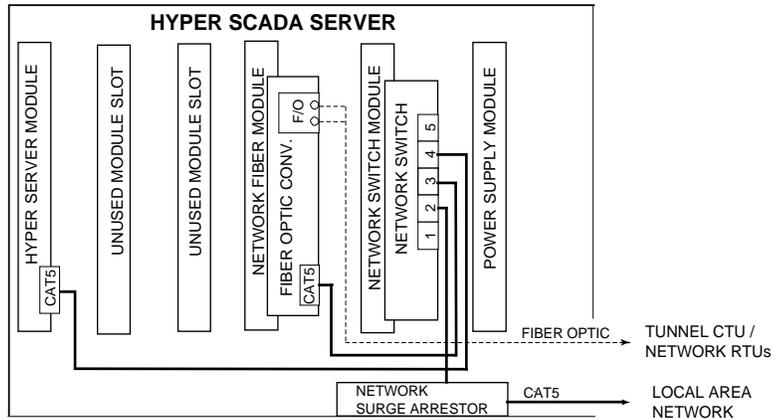
INTERNAL CONNECTIONS

Please follow normal Ethernet wiring practices when installing the HSS.

HSS002-1

The following connections must be made inside the unit:

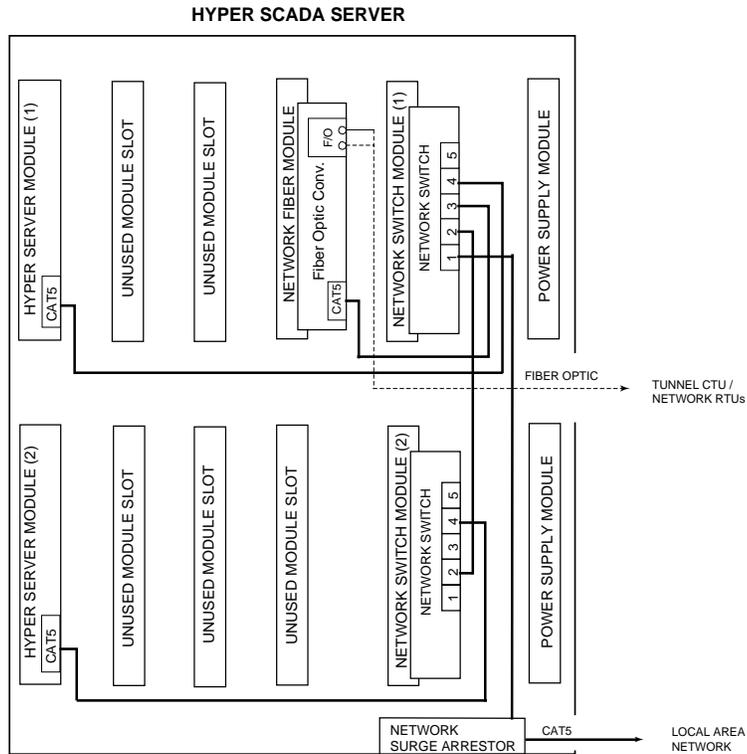
- HSM --> NSM (port4)
- NFM (CAT5) --> NSM (port 3)
- NSM (port 2) --> surge arrester

**HSS002-2**

The following connections must be made inside the unit:

- HSM1 --> NSM1 (port4)
- NFM (CAT5) --> NSM1 (port 3)
- NSM1 (port 2) --> NSM2 (port 2)
- NSM1 (port 1) --> surge arrester
- HSM2 --> NSM2 (port 4)

Refer to diagram on the next page.



CONNECT THE HSS TO LAN OR MASTER WORKSTATION

The HSS can be used in conjunction with either a stand-alone, master workstation or a local area network. A master workstation is one that is directly connected to the HSS. A master workstation is necessary when the HSS is not a part of an existing network. When the HSS is a component of a local area network, users access it from client computers.

If the distance between the main Ethernet backbone/master workstation and the HSS exceeds 100 meters (328 feet), or if the two devices are located in different buildings, an additional Network Fiber Module must be installed in the HSS. This requires that a fiber optic-to-CAT5 converter be placed between the HSS and the master workstation/main Ethernet backbone, and fiber optic cable be used to connect the HSS to this device. For this configuration, follow the instructions provided in HSS Requiring Additional NFM.

The selection of an NFM model is based on network speed and distance between the HSS and the corresponding network device (network card on dedicated workstation; hub, router, or switch connected to main Ethernet backbone; fiber-optic converter installed between HSS and master workstation/main Ethernet backbone). See list below.

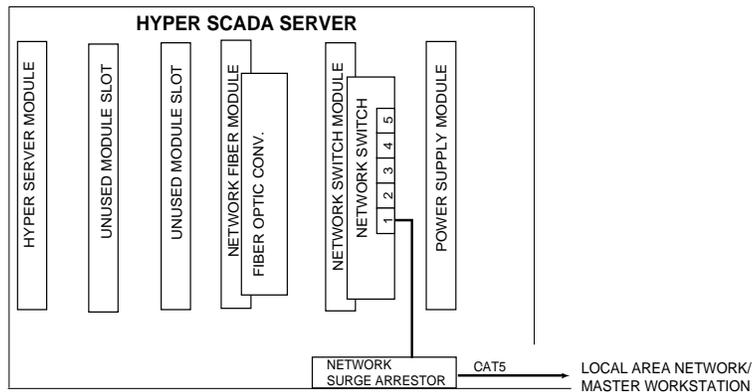
- NFM001: 10 Mbps, multi-mode fiber (up to 2 km)
- NFM001-SM: 10 Mbps, single-mode fiber (2-15 km)
- NFM001-F: 100 Mbps, multi-mode fiber (up to 2 km)
- NFM001-FSM: 100 Mbps, single-mode fiber (2-15 km)

Standard HSS

Although the diagrams below and on the next page show a non-redundant HSS, connections for both the HSS002-1 and HSS002-2 are identical when connecting to an Ethernet network or a master workstation. For the HSS002-2, substitute NSM1 (installed on top backplane) wherever the instructions refer to NSM.

Please follow normal Ethernet wiring practices when installing the HSS.

When connecting the HSS to a local area network via a device (such as a hub, switch, or router), or to a dedicated master workstation, connect any unused port* on the NSM to a port on the other device.



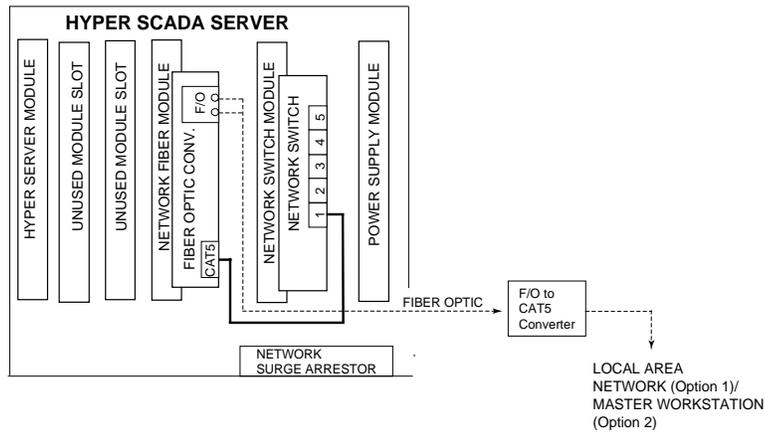
HSS Requiring Additional NFM

Note: In this configuration, the HSS' DIN-rail mounted network surge arrester is unused.

Please follow normal Ethernet wiring practices when installing the HSS.

If the distance from the HSS to the connection point (main Ethernet backbone or master workstation) is more than 100 meters away, or the two devices are located in separate buildings, it is necessary to install an additional NFM in the HSS.

1. Use CAT5 cable to connect any unused port on the NSM to the CAT5 connector on the NFM.
2. Use fiber-optic cable to connect the NFM to the fiber optic-to-CAT5 converter.
3. To complete the connection, use CAT5 cable to connect the fiber optic-to-CAT5 converter to a port on the other device (hub, switch, router, or master workstation).

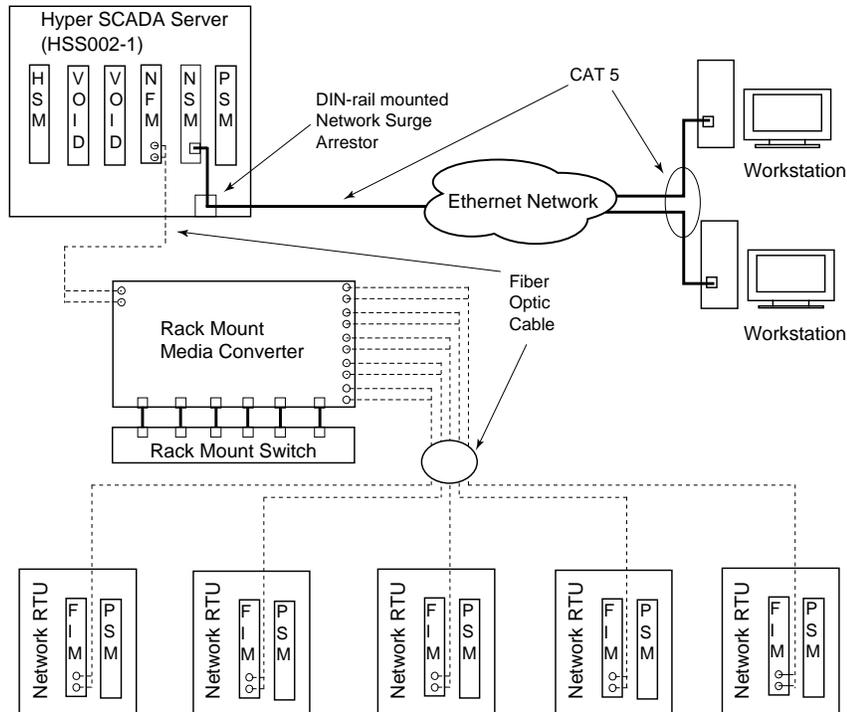


CONNECT THE HSS TO THE TELEMETRY SYSTEM

The HSS can be used in conjunction with a system of Network RTUs (remote terminal units in which Fiber Interface Modules, FIMs, have been installed) or a Tunnel CTU (central terminal unit that utilizes both a FIM and a Radio Interface Module, RIM).

Although the diagrams below and on the next page show a non-redundant HSS, connections for both the HSS002-1 and HSS002-2 are identical when connecting to Tunnel CTU or Network RTU. For an HSS002-2 model, assume that the illustration only shows the unit's top backplane.

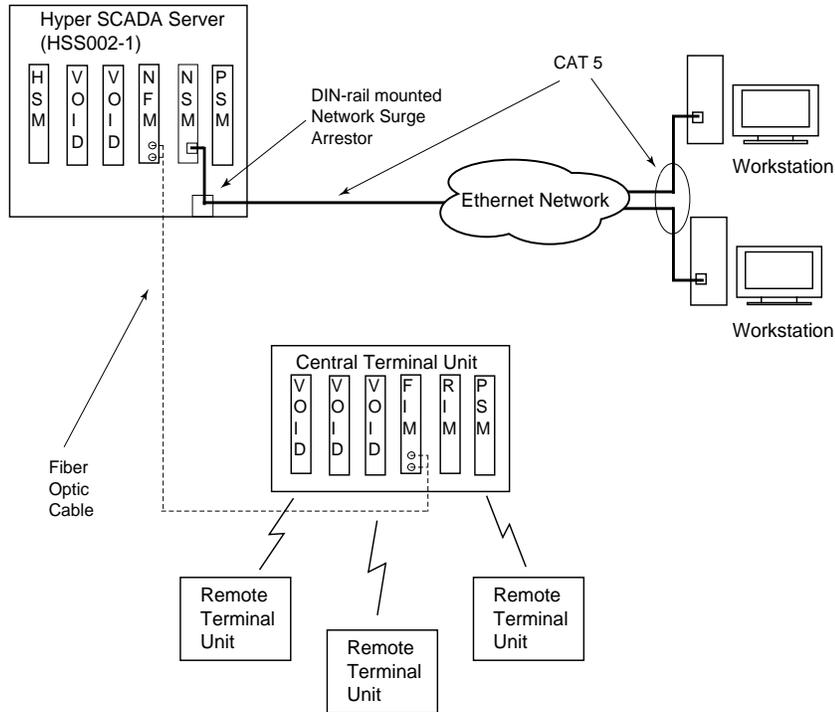
Network RTUs



In this configuration, data is passed between a local area network or a master workstation, and a system of Network (FIM-based) Remote Terminal Units (RTUs). Each RTU contains a Fiber Interface Module (FIM) that is responsible for communications between the primary HSM and the station's function modules. The Network RTUs connect to the HSS via a rack-mount media converter.

Use the appropriate fiber optic cable to connect the HSS' Network Fiber Module to the rack-mount media converter to which the system's Network RTUs are connected.

Tunnel CTU



In this configuration, data is passed between a local area network or a master workstation, and a Tunnel CTU (radio-based CTU that uses a Fiber Interface Module for serial tunneling). Serial tunneling is a process that enables serial (radio) data to be sent over a network. An HSS-Tunnel CTU system utilizes a CTU that includes both a Fiber Interface Module (FIM) and a Radio Interface Module (RIM).

Connect the HSS' Network Fiber Module to the Central Terminal Unit's Fiber Interface Module using the appropriate fiber optic cable.

CONNECT THE HSS TO A TELEPHONE LINE

Each HSM in the Hyper SCADA Server features two voice modems, which enable call in (411), call out (911), and PPP dial-up, and allow alarm annunciation via an audio device (PA system, an amplified speaker, or an amplifier-plus-speaker system).

You can use one or two phone lines to enable these features, although two lines is the preferred method. Instructions for both methods are provided below.

By default, HT3 is configured for two phone lines. If only one phone line is used for the call in and call out functions, HT3's configuration must be changed. See "Call In and Call Out: Configuring 911 & 411" in the HT3 User Guide for more information.

IMPORTANT: If you are using only one line for both functions, call out (911) takes precedence. If you are calling in and a call-out alarm occurs, the system will disconnect your call in order to place the 911 call.

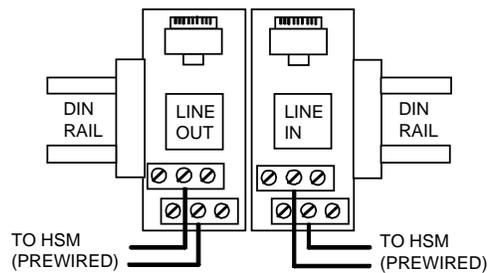


Figure 1: Telephone (911/411) Setup

One Telephone Line Setup

Note: This setup requires a configuration change in HT3

1. From your telephone room or telephone wall jack, locate the telephone line's tip and ring wires and terminate them using an RJ-11 or RJ-12 modular plug.
2. Insert the plug into the LINE IN jack located on the HSS' DIN rail. LINE IN is prewired to the Line 1 termination points on the HSM's card edge.

Two Telephone Line Setup

1. From your telephone room or telephone wall jack, locate line 1's and line 2's tip and ring wires. Terminate each line's tip and ring wires using an RJ-11 or RJ-12 modular telephone connector.
2. Plug the line that will handle call in (411 calls) in the LINE IN jack that is located on the HSS' DIN rail. LINE IN is prewired to the Line 1 termination points on the HSM's card edge.
3. Plug the line that will handle call out (911 calls) in the LINE OUT jack that is located on the HSS' DIN rail. LINE OUT is prewired to the Line 2 termination points on the HSM's card edge.

ALARM NOTIFICATION OPTIONS

The HSS, in conjunction with HT3, allows alarms to be displayed at HT3 client computers. The Hyper Server Module's alarm LED also lights when an alarm occurs.

Additional alarm notification options include.

- Alarms announced through an audio device (for example, a PA system, amplifier-plus-speaker system, or amplified speaker).
- External light illuminating when an alarm occurs.
- Horn sounding when an alarm occurs.
- Alarm silence button

Audio Device

Be sure to match the audio device's polarity (+ / -) to those of the HSS002-X's Hyper Server Module (Audio Output + and Audio Output -). If the polarities don't match, the sound may be distorted.

Ensure that the audio device has its own power source and ground. Do not use the HSS to power or ground the audio device.

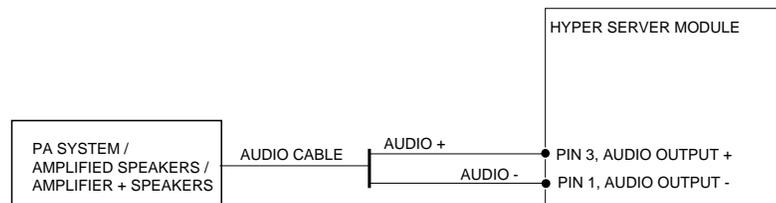


Figure 2: Audio Device Connected to HSS002-1

See additional diagrams on the next page.

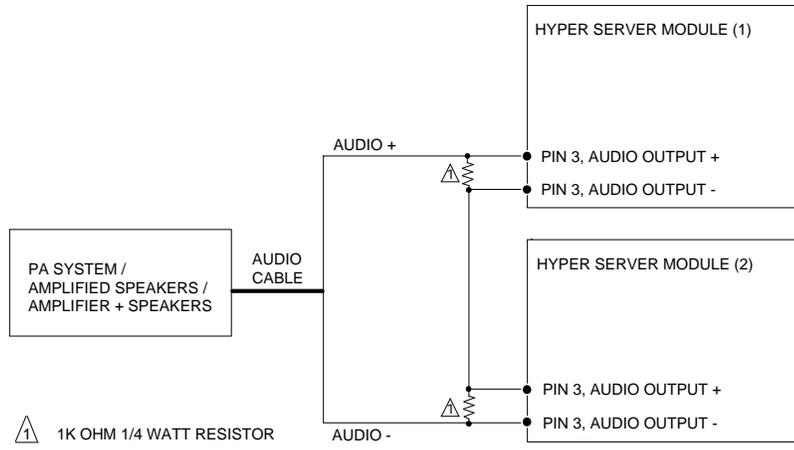


Figure 3: Single-channel Audio Device Connected to HSS002-2

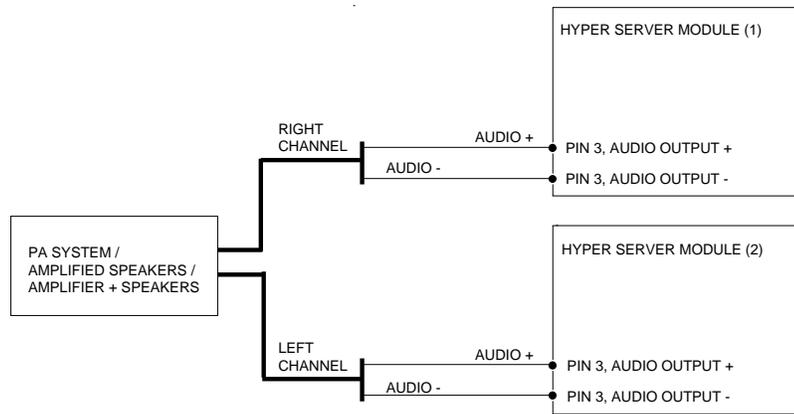


Figure 4: Multi-channel Audio Device Connected to HSS002-2

Alarm Light

Before wiring an alarm light, ensure that:

- Each set of contacts on the relay is rated for the voltage and current it is switching.
- The coil is rated for the +12VDC with which the HSS is driving it.
- The alarm light has its own power source and ground. Do not use the HSS to power or ground the external light.

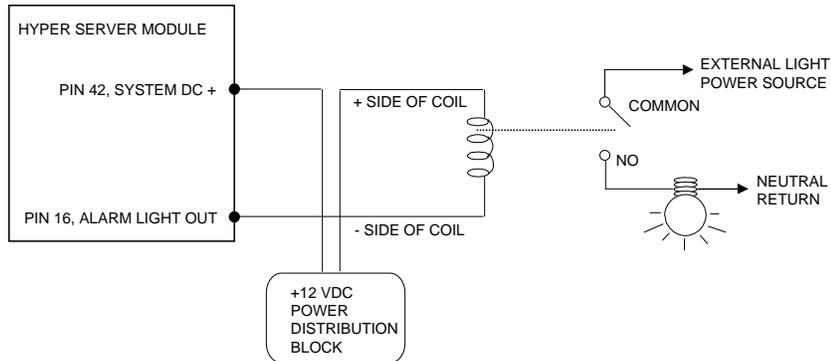


Figure 5: HSS002-1 Alarm Light Wiring

Alarm light wiring for the HSS002-2 is shown on the next page.

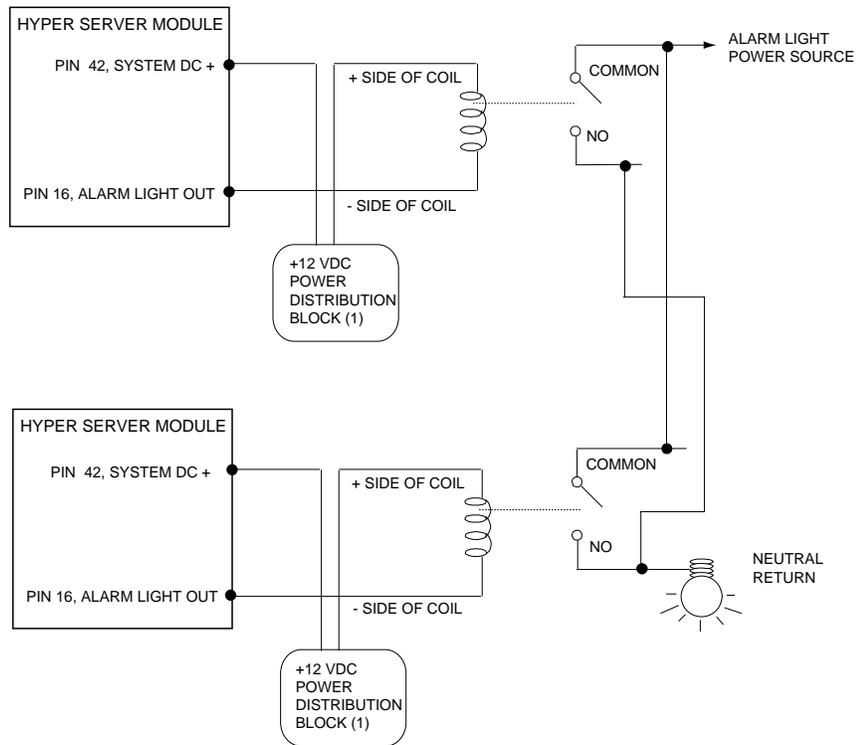


Figure 6: HSS002-2 Alarm Light Wiring

Alarm Horn

Before wiring an alarm horn, ensure that:

- Each set of contacts on the relay is rated for the voltage and current it is switching.
- The coil is rated for the +12VDC with which the HSS is driving it.
- The alarm light has its own power source and ground. Do not use the HSS to power or ground the external light.

See wiring diagrams on next page.

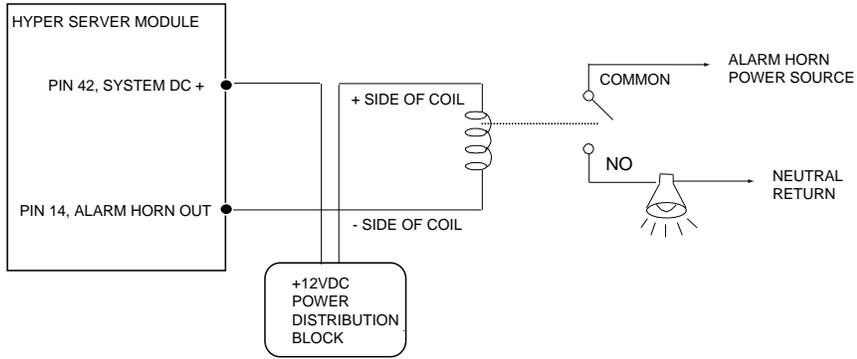


Figure 7: HSS002-1 Alarm Horn Wiring

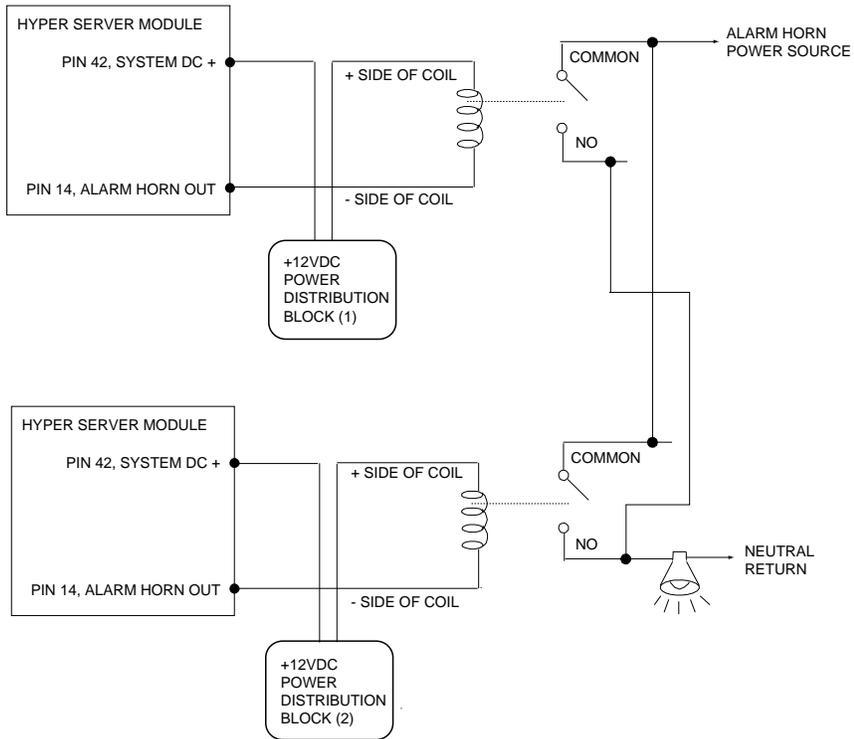


Figure 8: HSS002-2 Alarm Horn Wiring

Alarm Silence Button

Before wiring an alarm silence button, ensure that:

- Contacts on the relay are rated for the voltage and current it is switching.
- The coil is rated for 43.6 mA at 12VDC, and the contact is rated for 8 amps at 250VAC / 8 amps at 30VDC.
- The alarm silence button has its own power source and ground. Do not use the HSS to power or ground the alarm silence.

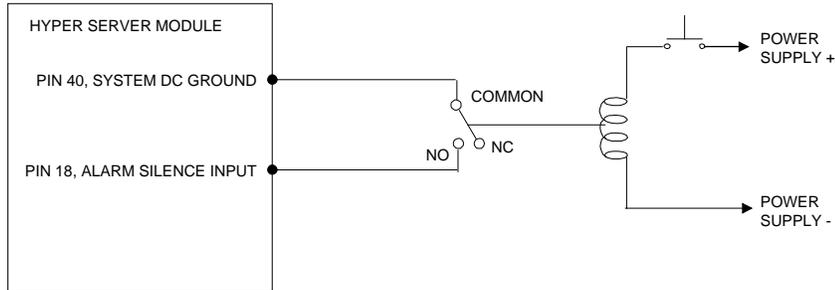


Figure 9: HSS002-1 Alarm Silence Button Wiring

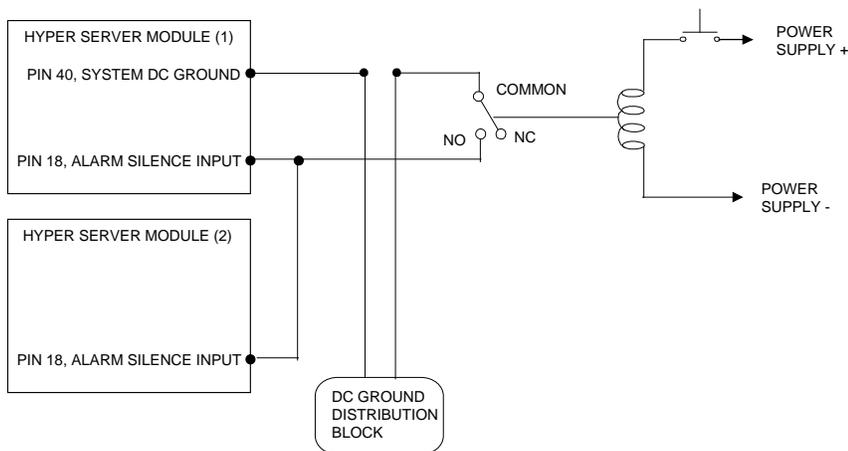


Figure 10: HSS002-2 Alarm Silence Button Wiring

CONNECT THE HSS TO A POWER SOURCE

The HSS uses a 100 watt power supply module (PSM003) to provide 12V DC operating power to all the modules on its backplane and continuous charging to its backup battery. (The HSS002-2 features two power supply modules - one for each backplane.)

The same procedure is used for wiring power to both the HSS002-1 and the HSS002-2. Connections from the backplate to all of the DIN-rail mounted components, including the 10 amp breaker and the neutral terminal block used in this procedure, are prewired at the factory.

Refer to the diagram below when wiring AC power. Note that the diagram shows only the right portion of the DIN rail.

IMPORTANT: A minimum of #16 gage stranded wire must be used in this installation.

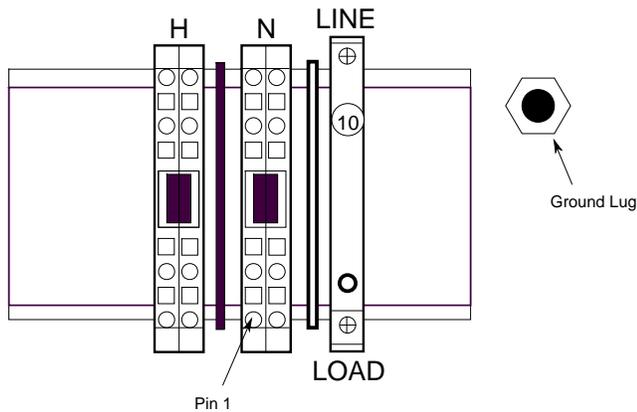


Figure 11: AC Power Wiring

WARNING

Before starting this installation, verify that no power is coming into the HSS or to any device(s) wired to it.

1. Locate the "hot" (black) wire. Strip back approximately 1/4" of the wire's insulation and remove the excess. Connect this wire to the line side of the 10 amp breaker using the breaker's screw-type connection.
2. Locate the "neutral" (white) wire. Strip back approximately 1/4" of the wire's insulation and remove the excess. Connect this wire to pin 1 on the neutral terminal block using the block's Wago compression-type connector.

3. Locate the "ground" (green and yellow) wire. Strip back approximately 1/4" of the wire's insulation, remove the excess, and terminate it with a #10 ring terminal. Connect the grounding wire to the HSS' ground lug.

REDUNDANCY (HSS002-2 ONLY)

A redundant system uses an HSS002-2. The goal of redundancy is to allow the HSS002-2's two HSMs to operate as one. One HSM acts as primary and runs HT3 and the MySQL database server. The other HSM runs in secondary mode and monitors the primary. If the secondary HSM senses a loss of telemetry from the primary HSM, the secondary HSM reboots the primary, assumes the shared IP address, and begins to run the HT3 and MySQL servers. The roles of primary and secondary are not dependent upon the HSM's configured IP address or the backplane in which the HSM is installed. Either can operate as the primary or secondary server.

Details on redundancy can be found in the HT3 User Guide (see "Configuring Your System: Critical Data Redundancy"). The paragraphs below discuss two concepts of redundancy (Shared IP and Safe IP) that must be considered and decided upon before installing and configuring the HSS002-2.

Shared IP

Redundancy uses a function called IP sharing that allows two or more network devices to communicate at one shared IP while retaining their own unique address. In the HSS002-2 application, the primary HSM "masquerades" as the shared IP address. Additionally, client computers are configured to communicate with the primary HSM using the shared IP (not the configured address).

IP sharing makes redundancy virtually transparent to devices on the network, because they communicate with the primary HSM at the shared IP address not its configured address. When the primary and secondary HSMs switch roles, the new primary begins masquerading as the shared IP; there is no need to reconfigure clients to communicate with the new primary HSM. Implementing redundancy requires that you have three (3) unused IP addresses on the same class C network: one for each HSM and one designated as the shared IP.

All clients should access the server using the shared IP address; not the configured IP address for either HSM. Clients should set up their hosts file to associate the name *ht3* with the shared IP address.

Safe IP

A Safe IP is the IP address of a device that is always "up" and is on the same network as the HSS. The secondary HSM uses this IP to determine if it should take over as primary after not getting a response from the acting primary. When it pings the Safe IP, it is trying to determine where the communication problem originated: with the primary HSM or with itself. If a gateway is configured on the HSMs, it should be the Safe IP

address. Examples of other Safe IPs are the addresses of routers, print servers, and voice-over-DSL devices. A workstation computer, although valid, is not the best selection since it can be easily turned off. A workstation computer can be used if no other devices are available, but it is important that it remain on at all times.

CONFIGURE/CHANGE THE HSM'S IP ADDRESS

If the Hyper Server Module's network settings were not preconfigured at the factory, you will need to provide the HSM with its correct IP address.

Follow this same procedure if it becomes necessary to change the HSM's IP address.

1. Connect a PS-2 keyboard and VGA monitor to the HSM. Ports for connecting a keyboard and monitor are easily accessible and clearly marked.
2. Power up the HSS following the procedure outlined in the section "HSM Start Up and Shutdown Procedures," p. 27-28.
3. When the HSM is fully powered and booted up, a login prompt appears on the monitor. Login as MGR.
4. At the command prompt, type *change_ip xxx.xxx.xxx.xxx* (where xxx.xxx.xxx.xxx represents the IP address of the HSM). Enter Y or N to confirm the IP change.
5. If you are configuring an HSS002-2, disconnect the keyboard and monitor from the first HSM and connect it to the second HSM. The login prompt should be displayed on the screen. If it isn't, press the space bar to refresh the video display. After the keyboard and monitor are connected, repeat steps 3 and 4 to configure the second HSM's IP address.
6. Reboot the HSM(s)

For an HSS002-2, reboot the HSMs one at a time. The order that the HSMs are rebooted is not important.

 - A. Press the power down button on the HSM and watch the HSM's LEDs. When the +CPU LED goes off, the HSM is fully powered down. After the HSM has been powered down, it cannot be restarted for 10 seconds. All inputs are ignored until 10 seconds have passed.
 - B. After 10 seconds have passed, press the power up button on the HSM and watch the HSM's LEDs. When the ACT LED begins to blink, the HSM is fully powered up.

We recommend that you keep the keyboard and monitor attached to the HSM until you verify that you can communicate with the HSM from a Windows workstation.

CONFIGURE HOSTS FILE ON WINDOWS WORKSTATION

The hosts file allows you to associate a name with an IP address. After the hosts file has been configured, you can launch Internet Explorer and simply type *ht3* in the Address box to connect to HT3.

1. On the Window's taskbar, click the **Start** button, and then click **Run**.
2. In the **Run** box, type one of the following (depending on your OS level):

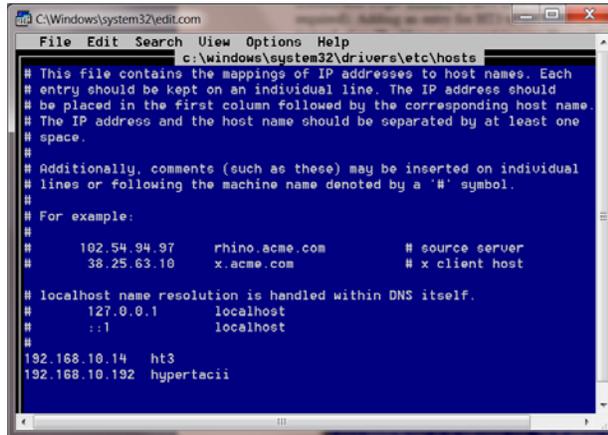
For Windows XP or newer, type:

```
edit c:\windows\system32\drivers\etc\hosts
```

For Windows 2000/NT, type:

```
edit c:\winnt\system32\drivers\etc\hosts
```

3. In the hosts file, place your cursor on a line below the file's comments [lines preceded by a pound sign (#)] and do the following:
 - A. Type *xxx.xxx.xxx.xxx* (where *xxx.xxx.xxx.xxx* represents the Hyper SCADA Server's IP address).
 - B. Press the Tab key
 - C. Type *ht3*



```
C:\Windows\system32\edit.com
File Edit Search View Options Help
c:\windows\system32\drivers\etc\hosts
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
#
# localhost name resolution is handled within DNS itself.
# 127.0.0.1 localhost
# ::1 localhost
#
192.168.10.14 ht3
192.168.10.192 hypertacii
```

4. Select **Save As** from the **File** menu. Verify that the name **hosts** appears in the **File Name** field and click **OK**.

VERIFY CONNECTION TO HSM

After the hosts file has been created and saved, use the ping command to verify that your computer can connect to the Hyper SCADA Server using the assigned host name.

1. On the Windows taskbar, click the **Start** button, and then click **Run**.
2. Type *ping ht3* in the **Run** dialog box and click **OK**.
3. A DOS window appears on screen and indicates if a reply has been received from the Hyper SCADA Server. A message similar to "Reply from xxx.xxx.xxx.xxx: bytes = 32 time < 1 ms TTL = 64" (where xxx.xxx.xxx.xxx represents the Hyper SCADA Server's IP address) indicates that the HSS responded.

CONNECT TO HT3

Modify Browser Settings

Several changes must be made to Internet Explorer's security settings before you can successfully run HT3.

1. Start Internet Explorer.
2. Select **Internet Options** from the **Tools** menu.
3. Click the **Security** tab and select the **Local intranet zone**.
4. Click **Custom Level**.
5. In the **Security Settings** dialog box, enable the following:
 - All of the options listed under **ActiveX controls and plug-ins**.
 - All of the options listed under **Cookies**.
6. Click **OK** at the **Security Settings** dialog box.
7. Click **OK** at the **Internet Options** dialog box.

Install Plug-Ins and Java Policy File

1. Start Internet Explorer and type *ht3* in the **Address** box.
2. If the necessary plug-ins are not already installed, the HT3 Plug-Ins page is loaded. (**Note:** If the HT3 Plug-Ins page does not automatically load, type *http://ht3/ht3/plugins/index.html* in Internet Explorer's Address box.)
3. Follow the instructions on the page to install the required HT3 files and plug-ins.

Start HT3

1. When installation of the plug-ins and the Java policy file is complete, type *ht3* in Internet Explorer's Address box.
2. On the HT3 login page, enter your Login and Password and click **OK**.
3. Bookmark HT3 in your browser or create a shortcut to HT3 on your desktop.

CONFIGURE REMOTE SYSTEM BACKUP

HT3 features an automated backup routine that protects your system from critical data loss. Data is copied and stored locally in a designated backup folder on the Hyper Server Module (HSM).

As an additional protection against data loss, a Windows workstation can be configured as a remote backup location. A remote backup site protects you from loss of data in the event of an HSM hardware failure (the HSM itself stops functioning). The designated backup workstation should be equipped with a hard drive large enough to hold all of the system's backup data and must be configured as a remote backup location. (We recommend that the remote Windows backup machine have at least 5 gigabytes of free disk space.)

Backup is performed daily at a few minutes after midnight. The system first makes a local copy of the data (stored on the Hyper Server Module). It then attempts to locate the remote backup computer.

For remote backup to occur, the designated Windows workstation must be on and running. It is recommended that all power management be disabled (i.e., the network card is not allowed to sleep).

If HT3 does not find the remote location, it skips the creation of a remote copy. It will not attempt another remote backup until the following midnight. An entry is made in the current day's Access Log to indicate if the previous day's backup succeeded or failed.

More information on critical data redundancy, including data recovery, can be found in the Hyper SCADA Server Installation & Operation Manual.

1. If the backup directory is to be on a Windows NT/2000, or Windows XP or newer machine, it is recommended that a new user account be created on the machine.
2. Create a backup folder, or directory, on the Windows workstation that has been designated as the remote backup.
3. Share the backup folder. (Refer to your Windows Help for information on sharing folders.)

Windows 98/ME:

- A. Select Full for Access Type.
- B. Enter *HSU* for the **Shared as** name.
- C. Enter a password in the **Full Access Password** box.

Windows 2000/NT or XP or newer

- A. Change the share name of the folder to HSS.
 - B. Set all shared folder permissions to **Full Control**.
 - C. Give the user account created in step 1, above, full access to the shared drive.
4. Login to HT3 and open the System Backup tool by clicking **Configure** on the HT3 main menu and then clicking **Backup** on the Configure submenu.

The screenshot shows a dialog box with three tabs: 'Backup', 'Redundancy', and 'Purge'. The 'Backup' tab is active. It contains a checked checkbox for 'Enable Remote Backup'. Below it are five text input fields: 'Remote Machine Name' (192.168.10.75), 'Remote Share Name' (HSS), 'Remote User Name' (Bob), and 'Remote Share Password' (telemetry). At the bottom are 'Ok' and 'Reset' buttons.

5. Configure the following:
 - **Enable Remote Backup** - Select this option to turn on automated backup.
 - **Remote Machine Name** - Enter the IP address of the Windows workstation that has been designated the remote backup location.
 - **Remote Share Name** - Enter the share name of the backup folder. This should be HSS.
 - **Remote User Name** - Enter the name of the user account created in step 1, above (Windows 2000/NT or Windows XP or newer machines only).
 - **Remote Share Password**

Windows 98/ME: Enter the Full Access Password assigned to the shared backup folder.

Windows 2000/NT or XP or newer: Enter the password of the user account created in step 1, above.
6. Verify that all of the above information is correct and click **OK**.

HT3 OVERVIEW

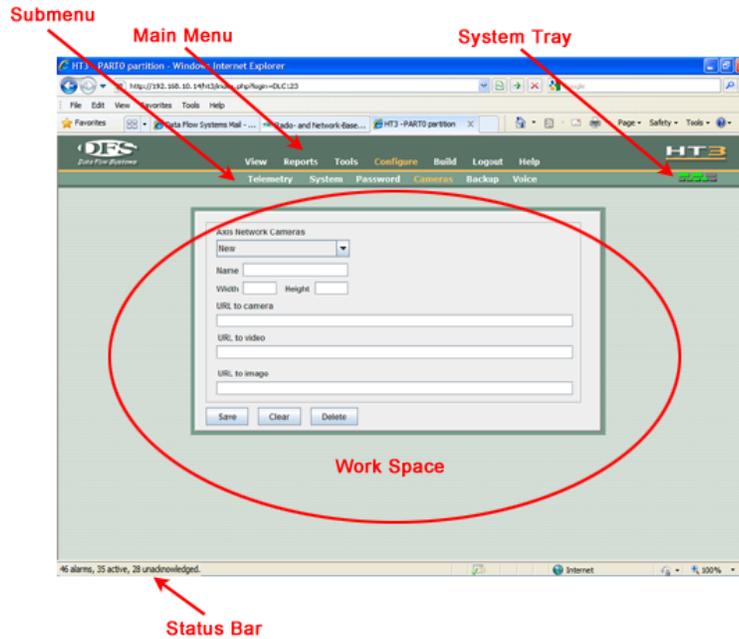
After the necessary hardware and software has been installed and the system is up and running, you can begin configuring HT3 to interface with your system's components (e.g., PLCs, surveillance cameras); set up user accounts; configure alarms for call out; and record alarm announcements. Once the basics are in place, you can begin using HT3's more advanced features, including canned reports, Screen Builder, and Virtual Logic Builder.

The sections below provide a brief overview of HT3's interface and its many features and tools. For more in-depth information, refer to the HT3 User Guide. To open the User Guide, click **Help** on the HT3 main menu and then click **Online Help** or **PDF Version**.

HT3's Interface

HT3's user interface is made up of the following components:

- Menus (main and submenus)
- Work space
- System tray
- Status bar



Menus

When you click an item on the HT3 main menu, the submenu for that item opens and the main menu item changes color. If you click another item on the main menu, the submenu changes to reflect the choices for that item.

When you click an item on the submenu, the submenu item changes color and the work space displays the interface for the chosen item except if Screen Builder, Logic Builder, or PCU Editor is selected. These applications open up in a new window.

Work Space

The work space, located in the center of the user interface, displays the item you selected from the menu.

System Tray

The system tray is located in the top right corner of the GUI (to the right of the submenu and below the HT3 logo). The system tray consists of three colored bars with a flashing line below them. When you place your mouse pointer over one of these items, information is displayed in the status bar.

- **Current User** - Place your pointer over the left bar to view the login name of the user currently logged in.
- **System Time and Date** - Place your pointer over the middle bar to view the current system time and date.
- **Alarm Information** - Place your pointer over the right bar to view total number of alarms, total number of active alarms, and total number of unacknowledged alarms. Click the right bar to open Alarm Viewer.
- **Server Connection** - Place your pointer over the flashing line to view server information (i.e., "server is online" or "server is offline").

HT3's Applications

Brief descriptions of HT3's applications are provided below. For detailed information, refer to the HT3 User Guide.

Status Viewing Tools

HT3 provides you with several methods for examining and analyzing - and from certain viewers, controlling - the status of your telemetry equipment. To access these tools, select **View** from HT3's main menu.

System Statistics displays information on the current status of important system-level points, including driver loop time, Hyper SCADA Server (HSS) AC power and battery voltage, active Hyper Server Module (HSM) CPU usage, and length of time active HSM has been running since its last reboot. This screen (which comes with your system and is built with Screen Builder) uses built-in external status points that monitor the health of your system.

Custom Screen Viewer displays the custom screens (graphical representations of telemetry) that you create using HT3's Screen Builder application. When you click the Screens link, your base, or initial, screen is loaded. If you have not created your own custom base screen, the default HT3 base screen (an example of a custom screen) is loaded.

The *Station Status Viewer* allows you to quickly view the status of each point for a specific station. From this viewer, you can also perform a control for any control point configured at the station. By default, the station listing is sorted in ascending order by

station address, or number. You can also have the list sorted alphabetically according to station name by clicking the "Station Listing" heading. Clicking "Station Listing" again resorts the list by address.

With *Alarm Viewer*, you can view and/or acknowledge alarm activity. The alarm list can be sorted by several different variables, including time, address, and description, and is color coded for quick alarm status identification.

Camera Viewer provides you with a means of viewing the video feed of your network surveillance cameras. With HT3 you can install an unlimited number of surveillance cameras on your network, which can be used to visually monitor important equipment or entrances to your plant.

With *Trender* you can view and analyze historical information for any telemetry point in your system. A trend can contain data from a single point or multiple points. Multiple points can be displayed in separate panels in the same window, or they can be combined to display in the same panel. Trender features tools for zooming in and out (to see more detail or more data) and for panning backward and forward in time. Any user can create and view a trend, but only users with "Configure Telemetry" permission can save a trend

Reports

HT3 provides you with a variety of reports that allow you to monitor the activity and performance of your telemetry equipment.

To access these reports, select **Reports** from HT3's main menu.

The reports include those for:

- Averaging and totalizing analog flow meters.
- Creating an electronic journal of events that affect your utility's operation.
- Calculating the flow at sewage lift stations that aren't equipped with analog flow meters.
- Generating a chronological listing of all events that occurred at the requested telemetry addresses for the specified time period.
- Listing all DFS stations that are digipeating and providing their relay paths.
- Listing information on each DFS point that is emulating Modbus.
- Providing daily pulse count totals for equipment, such as rain gauges or flow totalizers.
- Reviewing data on the activity of a digital point.
- Viewing information on a selected station, including its partition, polling priority, volume, each module configured at the station, and the module's associated I/O points.

An Advanced Reporting Tool for creating access, alarm and control logs and radio error reports, and using advanced features to create analog flow, derived flow, detail, pulse, and pump activity reports is also available.

System Troubleshooting and Maintenance Tools

HT3 includes tools to aid you in troubleshooting and maintaining your system. Although these tools are most effective in the hands of experienced DFS service technicians, system administrators and end users can benefit from their proper use.

To access HT3's troubleshooting and maintenance tools, select **Tools** from HT3's main menu.

The *Telemetry Traffic Tool* lets you monitor radio and network communications between your radio- and network-telemetry drivers, and the field hardware. You can also control the value of digital and analog points, set polling priority, and create a communications log. The Inject feature allows DFS Technicians to troubleshoot communication and other system errors from a remote location.

The *Server Control Center* allows users with "Shutdown System" permission to: stop and start telemetry; reboot the Hyper Server Module (HSM); test the Hyper SCADA Server's (HSS) battery power; reset hardware in the HSS; check the status of the MySQL database and repair any errors that exist in the database tables.

The *File Upload Utility* easy-to-use tool that enables you to browse your Windows workstation or network and upload one of the following types of files to your Hyper Server Module: custom screen image; HT3 update; HTML image; custom HTML file

HT3's easy-to-use File *Download (and Delete) Utility* allows you to download the following files from the Hyper Server Module (HSM) to your local Windows workstation: report .csv files; report .txt files; driver log files. You can also use this utility to delete files (.csv and .txt report files) from the server.

HT3's *Module Patching Utility* is designed to help maintain the latest patch levels (updates to the original program) on all DFS function modules. This tool can also be used to ensure that all network interface modules are running the latest program.

Configuration Tools

HT3's configuration tools provide you with the means necessary to configure all aspects of your telemetry system.

To access HT3's configuration tools, select **Configure** from HT3's main menu.

Configuration Editor's many options let you set up your system to perform tasks and divide workflows in ways that are unique and meaningful to your operation. You can view and configure partitions, users, drivers, alarms, auto controls, and other telemetry items. These tasks can be completed from any configured Windows workstation.

From the *Registry Editor*, you can change your system's time zone and update the system's time and date.

Use HT3's *Password Maintenance* tool to change the password for your user account.

From the *Configure Cameras* utility, you configure the settings for your network surveillance cameras so that their video feed can be viewed from HT3.

HT3 features an automated backup routine that protects your system from critical data loss. From the *Backup* utility, you designate and configure the Windows workstation that is to be used as a data backup location. This utility is also used to configure a redundant system (HSS002-2 required) and set purge schedules for HT3's logs and journals.

HT3's *Voice Recording* tool enables you to create custom alarm announcement call-out (911) and call-in (411) recordings and command prompts.

Building Tools

HT3 includes four applications that can be used to enhance and further automate your telemetry system.

To access HT3's building tools, select **Build** from HT3's main menu.

HT3's *Screen Builder* application lets you create a graphical representation of your telemetry system using text, images, objects, and animation. The screen's components can be linked to actual telemetry points; providing you with a quick, real-time view of your operation.

Virtual Logic Builder is a user-friendly application that enables you to construct "ladder logic"-style programs that run on the HT3 central computer.

PCU Editor enables you to modify the operational set points of a Pump Control Unit (PCU) from a Windows workstation.

With *PLC Editor*, you can transfer set point values to and from the PLC's non-volatile memory locations via telemetry.

Exit HT3

The *Logout* tool (Portal) should be used to log out of the HT3 system.

HT3 Help

HT3's release notes and user guide is available from HT3's Help menu.

Select *About* to view HT3's release notes and to view version information.

The HT3 User Guide is available in an HTML-based version and a PDF book-style version (select *Online Help* or *PDF Version*).

HSM START UP AND SHUT DOWN PROCEDURES

Start Up

1. Turn on the PSM.

2. Connect the battery. The HSS is now activated.
3. It is not necessary to use the HSM's CPU Power up button. The HSM will automatically power up when it senses power has been applied. LED sequence during power up is as follows:
 - A. The ACT LED is constant. The SDN LED blinks slowly and then more quickly. +CPU and +5V LEDs are constant and remain constant during and after power up.
 - B. The SDN LED goes off and the ACT LED is constant.
 - C. The ACT LED begins to blink indicating that the HSM is fully powered up.

Shut Down

1. Press the HSM's CPU Power down button. The shutdown LED (SDN) begins to flash indicating that the shut down process has begun.
2. SDN then goes constant indicating that services to the HSM have been turned off.
3. After a few moments, the CPU power LED (+CPU) goes out indicating that it is now safe to remove power.
4. Disconnect the battery.
5. Turn off the PSM. The HSS is now deactivated.

BACKUP BATTERY

Operating run times for a typical application running on battery power:

- HSS002-1 (single 7.0 AH battery) - approximately 60 minutes.
- HSS002-2 (two 7.0 AH batteries) - approximately 26 minutes.

CARE AND MAINTENANCE

- Do not put any objects on top of the HSS. The enclosure, although strong, is not made to support extra weight.
- When transporting the HSS, we recommend that you put it in the original packaging materials.
- Avoid subjecting the HSS to extreme temperature changes, which can damage the HSS' internal components.
- Avoid dusty or dirty work environments. Dust and dirt can clog and possibly damage the HSS' internal components
- Keep all liquids away from the HSS. Liquids, when spilled onto the HSS' components, can result in severe damage and costly repairs.
- Do not walk on the power, phone, or network cables or allow anything to rest on them.

Cleaning the HSS

WARNING

Even when all of the HSS' modules are powered down, a small amount of electrical current may still be present. To avoid electrical shock, always unplug all power, phone, and network cables and disconnect the battery before cleaning the unit.

Use a damp, lint-free cloth to clean the exterior of the HSS. Do not use abrasive or solvent cleaners.

To clean the interior of the HSS, use a dry, lint-free cloth, a mini computer vacuum, soft brush, or an aerosol can of compressed air.

REPLACEMENT PARTS

Parts should only be replaced with parts recommended and approved by Data Flow Systems. Placing unapproved parts in the HSS002 voids the safety certification. See the Return Authorization (RA) Procedure (below) for instructions on obtaining replacement parts.

RETURN AUTHORIZATION (RA) PROCEDURE

In the event that a function module fails, during or after the warranty period, it may be returned to Data Flow Systems to be repaired or replaced.

All RA's will be subject to standard shipping and handling charges. Minimum handling charge will be assessed, in most cases, for work such as Radio Tuning, Backplanes, "No Problem Found," and other minor repairs. Handling charges will be waived on warranty equipment. Standard shipping and charges will be based on UPS ground, please advise if other arrangements are needed (UPS Red, FedEx, Pickup, Freight...). Standard cost of repairs and shipping charges can be obtained by contacting our RA Department by phone or e-mail.

STEP 1: Replace the failed module with a spare module of the same type, if one is available.

STEP 2: Contact Data Flow Systems Inc. in one of the following ways to receive an RA#:

- Email DFS at rma@dataflowsys.com.
- Call DFS at 321-259-5009 ext. 1142 during normal operating hours.

The following information must be provided.

- Customer/Utility Name and Ship to Address
- Contact Name and Phone Number
- Products to be returned and Serial Numbers
- Detailed description of failure
- PO#

Note: The lack of "Detailed description of failure" could result in a bench test fee and equipment returned due to the inability to properly determine the nature of the failure or testing resulting in "No Problem Found."

STEP 3: Place the function module(s) individually in an electrostatic discharge bag and then wrap with foam or bubble wrap. Pack the wrapped module(s) in a sturdy box filled with popcorn-type or bubble wrap packing material. Include a packing slip with the following information:

- Module(s) model, serial number, probable cause of failure, and the RA number
- Shipping address
- Shipping instructions (shipping costs greater than UPS ground are charged to the customer)

STEP 4: Address the box to:

RA Department # {the RA number you received here}

Data Flow Systems, Inc.
605 N. John Rodes Blvd.
Melbourne, FL 32934-9105

STEP 5: Ship the box to DFS using any typical shipping carrier (for example, UPS, FedEx, etc.). NOTE: DFS employees are not permitted to hand carry RMA materials.

Modules are typically repaired and shipped back to the customer within a 2-week period starting at the time the module reaches the RA Department. If additional information is required during the repair of the module(s), the DFS service department will contact you.

To get information on the progress of any of your equipment in for repair, contact the DFS - RA Department at rma@dataflowsys.com or 321-259-5009 ext. 1142.

Replacement of equipment may be necessary in the event that the equipment and/or parts are unreparable. Warranty equipment will be replaced with out prior notification as warranty replacement. The customer will be notified by phone, if equipment not under warranty cannot be repaired, with information of available options.

DFS reserve the right to return any material received without an RA# or not conforming to the requirements of this RA process.

WARRANTY

The warranty details Data Flow System's commitment to repairing or replacing parts and providing support during the warranty period. Refer to your Warranty Certificate, or the Warranty Statement included with your contract, for details on the terms of your warranty. If you lose your Warranty Certificate/Statement, contact Data Flow Systems' Sales Department to obtain the warranty terms and to replace your Warranty Certificate/Statement.

- Call 321-259-5009
- Email sales@dataflowsys.com



Data Flow Systems, Inc.
605 N. John Rodes Blvd.
Melbourne, FL 32934
321-259-5009
www.dataflowsys.com