EndRun TECHNOLOGIES
"Smarter Timing Solutions"

FDC3300e

Frequency Distribution Chassis

User Manual

USM3300-0800-000 Revision 2
March 2019

FDC3300e

Frequency Distribution Chassis User Manual

Preface

Thank you for purchasing the Frequency Distribution Chassis. Our goal in developing this product is to bring you a distribution chassis that will quickly, easily and reliably meet or exceed your system requirements. Your new FDC3300e is fabricated using the highest quality materials and manufacturing processes available today, and will give you years of trouble-free service.

About EndRun Technologies

EndRun Technologies is dedicated to the development and refinement of the technologies required to fulfill the demanding needs of the time and frequency community.

The instruments produced by EndRun Technologies have been selected as the timing reference for a variety of industries and applications - computer networks, satellite earth stations, power utilities, test ranges, broadcast and telecommunications systems and more.

EndRun Technologies is committed to fulfilling your precision timing needs by providing the most advanced, reliable and cost-effective time and frequency equipment available in the market today.

Trademark Acknowledgements

IBM-PC, UNIX, Windows NT are registered trademarks of the respective holders.

Part No. USM3300-0800-000 Revision 2
March 2019

About This Manual

This manual will guide you through simple installation and set up procedures.

Introduction – The Frequency Distribution Chassis, how it works, where to use it, its main features.
Basic Installation – How to connect, configure and test your distribution chassis.
Console Port – Description of the console commands for use over the serial port or optional network port.

If you detect any inaccuracies or omissions, please inform us. EndRun Technologies cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice.

Warranty

This product, manufactured by EndRun Technologies, is warranted against defects in material and workmanship for a period of two years from date of shipment, under normal use and service. During the warranty period, EndRun Technologies will repair or replace products which prove to be defective.

For warranty service or repair, this product must be returned to EndRun Technologies. Buyer shall prepay shipping charges to send product to EndRun Technologies and EndRun Technologies shall pay shipping charges to return product to Buyer. However, if returned product proves to be operating normally (not defective) then Buyer shall pay for all shipping charges. If Buyer is located outside the U.S.A. then Buyer shall pay all duties and taxes, if any.

Products not manufactured by EndRun Technologies but included as an integral part of a system (e.g. peripherals, options) are warranted for ninety days, or longer as provided by the original equipment manufacturer, from date of shipment.

Limitation of Warranty

The foregoing express warranty shall not apply to defects resulting from improper or inadequate maintenance by Buyer or User, Buyer-supplied software or interfacing, unauthorized modification or misuse, operation outside of the environmental specifications for the product, or improper site preparation or maintenance.

TO THE EXTENT PERMITTED BY LAW, THIS WARRANTY AND REMEMDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, REMEDIES AND CONDITIONS WHETHER ORAL OR WRITTEN, STATUTORY, EXPRESS, OR IMPLIED. AS PERMITTED BY APPLICABLE LAW, ENDRUN SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Warranty Repair

If you believe your equipment is in need of repair, call EndRun Technologies and ask for a customer service agent. It is important to contact us first as many problems may be resolved with a phone call. Please have the serial number of the unit and the nature of the problem available before you call. If it is determined that your equipment will require service, we will issue an RMA number. You will be asked for contact information, including your name, address, phone number and e-mail address.

Ship the unit prepaid in the original container or a container of sufficient strength and protection to EndRun Technologies. EndRun will not be responsible for damage incurred during shipping to us. Be sure the RMA number is clearly identified on the shipping container. Our policy is to fix or repair the unit within 5 business days. If it is necessary to order parts or if other circumstances arise that require more than 5 days, an EndRun service technician will contact you.

Loaner units are not included as part of the standard warranty.

Repair After Warranty Expiration

If the warranty period has expired, we offer repair services for equipment you have purchased from EndRun. Call and ask for a customer service agent. It is important to contact us first as many problems may be resolved with a phone call. Please have the serial number of the unit and the nature of the problem available before you call. If it is determined that the equipment has failed and you want EndRun to perform the repairs, we will issue you an RMA number. Ship the unit prepaid in the original container or a container of sufficient strength and protection to EndRun Technologies. EndRun will not be responsible for damage incurred during shipping to us. Customer is responsible for shipping costs to and from EndRun Technologies. Be sure the RMA number is clearly identified on the shipping container. After the equipment has been received we will evaluate the nature of the problem and contact you with the cost to repair (parts and labor) and an estimate of the time necessary to complete the work.

Limitation of Liability

The remedies provided herein are Buyer's sole and exclusive remedies. EndRun Technologies shall not be liable for any direct, indirect, special, incidental or consequential damages, whether based on contract, tort or any other legal theory.

EndRun Contact Information

Address:	EndRun Technologies 2270 Northpoint Parkway Santa Rosa, California 95407 U.S.A.
Phone:	(707)573-8633
Fax:	(707)573-8619
Sales:	1-877-749-3878 or (707)573-8633 sales@endruntechnologies.com
Support:	1-877-749-3878 or (707)573-8633 support@endruntechnologies.com

This page intentionally left blank.

Table of Contents

Preface i
About EndRun Technologies i
Trademark Acknowledgements i
About This Manual ii
Warranty ii
Limitation of Warranty ii
Warranty Repair iii
Repair After Warranty Expiration iii
Limitation of Liability iii
EndRun Contact Information iii

Chapter One - Introduction 1
Main Features 1
Overview 1
Performance, Reliability and Reasonable Cost 1
Flexibility 1
Easy Installation 1
Free FLASH Upgrades 2
Theory of Operation 2
Overview 2
Distribution Subsystem and Linux Subsystem 2
System Status Log Files 2

Chapter Two - Basic Installation 5
Checking and Identifying the Hardware 5
Physical Description 6
Installing the FDC 7
Mount the FDC 7
Connecting the DC Power Option 7
Connect the RS-232 Serial I/O Port 8
Test the Serial Port 9

Connecting and Configuring Ethernet 10
Configuring Ethernet with the Serial Port 10
Using netconfig to Set Up Your IP 11
Verify Network Configuration 11
Check Network Operation 13
Using Telnet 13
Using SSH 14
Using HTTPS 14
Connecting Instruments to the FDC 15
Connect Signal Inputs and Outputs 15
Connect Disable Inputs (External Alarm Inputs) 15
Connect Alarm Output 15

Chapter Three - Console Port Control and Status 17
Console Ports 17
General Linux Operation 17
Available User Commands 18
Detailed Command Descriptions 19
accessconfig 19
alarmstat 19
dcreset 20
dcreturn 20
dcversion 21
disablemode 21
disablestat 22
faultstat 22
help 22
inetdconfig 23
netconfig 23
ntpconfig 23
ntpstat 24
pwrstat 24
selectedin 24
serialnumber 25

settings 25
siginstat 25
sigoutstat 25
status 25
switchmode 25
syskernel 26
sysrootfs 26
sysversion 26
updatekernelflag 26
updaterootflag 27
upgradekernel 27
upgradekerneldtb 27
upgraderootfs 27
upgradesubsys 28

Chapter Four - Simple Network Management Protocol (SNMP) 29
SNMPv3 Security 29
Enterprise Management Information Base (MIB) 30
Invocation of the SNMP daemon 30
Quick Start Configuration -- SNMPv1/v2c 30
Change Default Community Strings (Passwords) 31
Configuring SNMPv1 Trap Generation 31
Configuring SNMPv2c Notifications and Informs 31
Configuration of SNMPv3 32
Disable or Restrict Access 33

Chapter Five - Security 35
Linux Operating System 36
Restrict Access 36
Restrict Access - Telnet, SSH and SNMP 36
Disable Protocols 37
Disable Telnet, Time and Daytime 37
Disable SNMP, SSH and HTTPS 37

Re-Enable SNMP, SSH and HTTPS 38
Is the Protocol Disabled? 38
OpenSSH 39
Configure Keys 39
Network Security Vulnerabilities 40

Chapter Six - Hyper Text Transport Protocol (HTTP/HTTPS) 41
Interface Description 41
Navigation 42
Configure HTTPS 43
Configure HTTPS only for IPv4 43
Configure HTTP for IPv6 44
Configure HTTPS only for IPv6 44
Security 44
Restrict Access 44
Configure Certificate and Key 44

Chapter Seven - Network Time Protocol (NTP) 47
Configuring FDC as a Stratum 2 Client/Server 47
Security 49
Restrict Query Access - NTP 49

Chapter Eight - IPv6 Information 51
IPv6 Capabilities 51
OpenSSH 51
Hiawatha HTTPS 51
Net-SNMP 51
NTP 51
IPv4-Only Protocols 52

Chapter Nine - System Log Files 53
Distribution Subsystem 53
Status 53
NTP Status 54

Appendix A - LED Indicators 55
Power LEDs 55
Input LEDs 55
Output LEDs 56
Alarm LED 56

Appendix B - Upgrading the Firmware 57
Performing the Linux RFS Upgrade 57
Transfer File to FDC 58
Recovering from a Failed RFS Upgrade 59
Performing the Linux Kernel Upgrade 60
Transfer File to FDC 60
Recovering from a Failed Kernel Upgrade 61
Performing the Distribution Subsystem Upgrade 62
Problems with the Distribution Subsystem Upgrade 63

Appendix C - Helpful Linux Information 65
Linux Users 65
Linux Commands 65
Detailed Information Is Available 65
Change Password 66
List Active Processes 66
NTP Monitoring and Troubleshooting 66
Text Editors 67
Change Log-In Banners 67
Query and Change Ethernet Port 67
Redirect Syslog Files to Remote Host 68

Appendix D - Third-Party Software 69
GNU General Public License 69
NTP Software License 74

Appendix E - Specifications 75

Special Modifications - Changes for Customer Requirements 81

This page intentionally left blank.

Chapter *One*

Introduction

The FDC3300e Frequency Distribution Chassis is a 19" rack-mounted, dual-input, ten-output device for 10 kHz to 10 MHz analog signal distribution with intelligent input fault detection and failover switching. In addition to reproducing the input signal with very low distortion and propagation delay, the unit features excellent input-to-input, output-to-output and output-to-input isolation. It adds very low phase noise and spurious components to the distributed signal, making it suitable for demanding applications where high spectral purity is required. Status is locally observable on a cleanly-designed front panel with LED indicators, and it is fully manageable via the full-featured Ethernet port or RS-232 serial port. Redundant AC, DC or AC/DC power inputs are optionally available.

Visit http://www.endruntechnologies.com/support.htm *to download firmware upgrades and get the latest manuals and other documentation.*

Main Features

Overview

The FDC3300e (FDC) may be employed either as a simple, single-input, ten-output signal distributor for non-critical applications, or, by making use of its intelligent dual-input failover switching and redundant power supply capabilities, high-availability signal distribution systems for top tier commercial and military applications may be efficiently implemented. The unit will accept a TTL or Open-Collector Alarm output signal from the upstream signal source on each of its two external alarm inputs so that bank switching of multiple FDC units may be efficiently and synchronously implemented.

Performance, Reliability and Reasonable Cost

It provides high performance and reliability combined with reasonable cost. Its internal sub-assemblies are fabricated with state-of-the-art components and processes and are integrated in a solid, high-quality chassis.

Flexibility

It supports full user configuration of the input switching strategy and complete remote monitoring and control via multiple industry-standard interfaces.

Easy Installation

FDC's standard 1U high, 19" rack-mountable chassis makes installation simple. It may be mounted in any convenient location. All signal input and output connectors are standard BNC female connectors. AC power input is via IEC-320 standard power cord. Connect it to your host computer using the standard RS-232 serial cable provided, or use the rear panel mounted 10/100Base-T RJ-45 connector and CAT-5 patch cable provided to connect it to your network. Initial network configuration

is automatic on networks using the Dynamic Host Configuration Protocol (DHCP). Manual network configuration is via the RS-232 serial I/O port.

Free FLASH Upgrades

Firmware is stored in non-volatile FLASH memory, so the FDC can be easily upgraded in the field using the Ethernet port or local RS-232 port. We make all firmware upgrades for our products available to our customers free of charge.

Theory of Operation

Overview

The diagram below illustrates the FDC architecture. Single or dual power supply operation is supported with any combination of AC or DC input voltages. (Installation of the second power supply is an option for the FDC.) The presence of proper voltage at the output of each of the two internal DC-DC converters is detected and monitored by the alarm logic and Distribution Subsystem CPU. The outputs of these two power supplies are diode "OR'd" to power the FDC. When both power supplies are good, Power Supply A is active while Power Supply B remains on standby.

Single or dual signal inputs are detected and monitored by the alarm logic and Distribution sub-sysem CPU. In addition, single or dual TTL level disable inputs are monitored to allow switching based on the alarm output from the upstream signal source. This external alarm signal can be connected to rear-panel BNC connectors labeled "DISABLE IN". These disable inputs are pulled up with 10k ohm resistors so that they may be connected to an open-collector output signal. Based on the status of the signal input level detection and the disable inputs, the alarm logic and Distribution Subsystem CPU control the signal input switch. You can configure a variety of automatic switching strategies and also manually force the selection of either input.

The output signal from the switch is buffered and drives ten broadband output amplifiers. Output signal level detectors for each of the ten channels are monitored by the alarm logic and Distribution Subsytem CPU so that output amplifier failure or interconnect cable short circuits may be observed.

All status information is reported via the front-panel LEDs and the serial I/O port or Ethernet TCP-IP interface. A summary open-collector alarm output is provided. System status information is also kept in log files. See below for details.

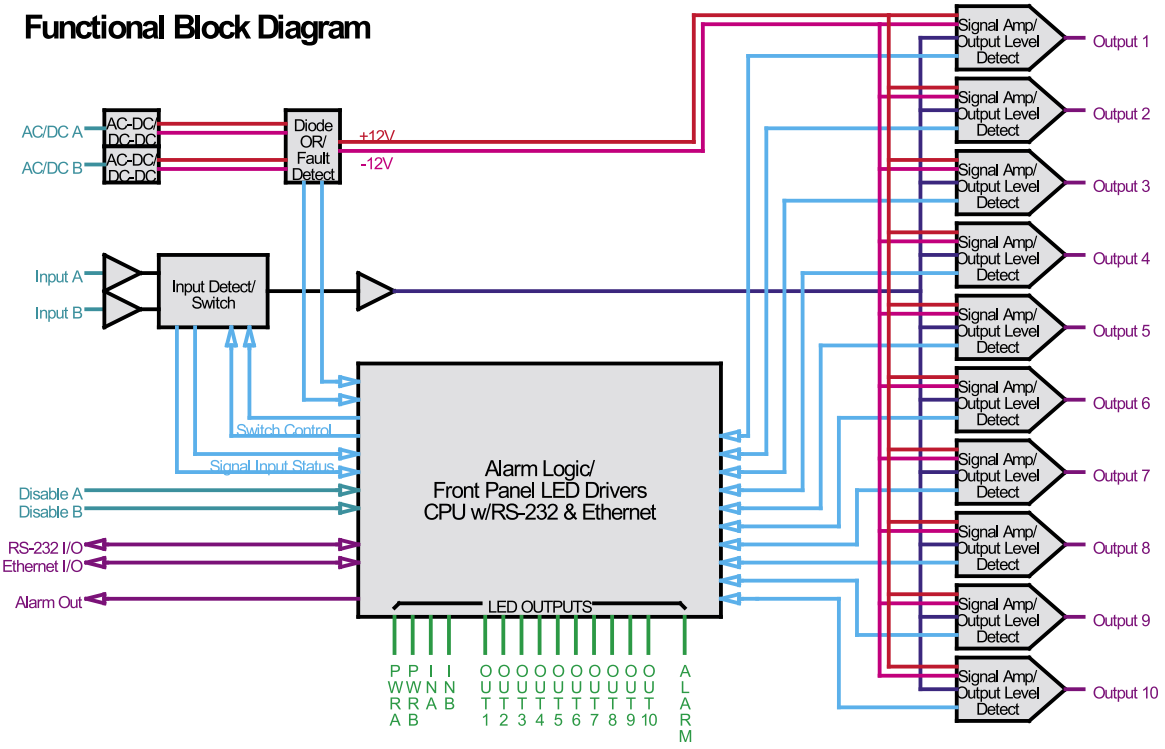
Distribution Subsystem and Linux Subsystem

The FDC is a dual-CPU system comprised of a Distribution Subsystem processor and a Linux Subsystem processor. The Distribution Subsystem provides all of the essential features of the FDC and controls and monitors all hardware functions. The Linux Subsystem interfaces with the Distribution Subsystem to make all status and control available via the ethernet TCP-IP interface. In addition, the Linux Subsystem synchronizes its system clock to a user-configured network time source via NTP. This allows it to maintain meaningfully timestamped log files.

System Status Log Files

Log files are for Distribution Subsystem status and for NTP status. See ***Chapter 9 - System Log Files*** for details.

Functional Block Diagram



This page intentionally left blank.

Chapter *Two*

Basic Installation

This chapter will guide you through the most basic checkout and physical installation of your FDC3300e Frequency Distribution Chassis. Subsequent chapters and appendices will give you the information needed to configure your installation for the maximum performance in your operating environment.

Checking and Identifying the Hardware

Unpack and check all the items using the shipment packing list. Contact the factory if anything is missing or damaged. The FDC3300e (FDC) shipment typically contains:

- FDC3300e (part # 3300-0801-000 or #3300- variant)
- FDC3300e User Manual (part #USM3300-0800-000)
- IEC 320 AC Power Cord (part #0501-0003-000)
  (This part will not be present if using the DC power option.)
- DB9F-to-DB9F Null Modem Serial I/O Cable (part #0501-0002-000)
- RJ-45 to RJ-45 CAT-5 patch cable, 2 meters (part #0501-0000-000)

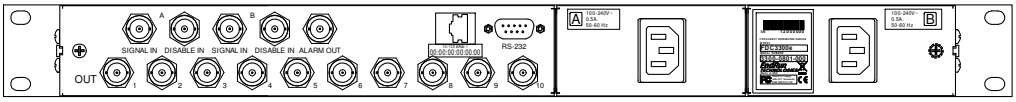
Physical Description

Power A/B LEDs — These red/green LEDs indicate power input status. Green means the power supply is good. Red means the power supply is installed but has failed. Off means the optional power supply is not installed. Power B is on standby when both supplies are good.

Input A/B LEDs — These red/green/yellow LEDs indicate the signal input status. For a full description see ***Appendix A - LED Indicators***.

Output 1-10 LEDs — These red/green/yellow LEDs indicate the presence or absence of signals at the output connectors. Green means the output is present and red means the output is absent or shorted.

Alarm LED — This red/green/yellow LED indicates the presence of a fault condition. Green means there is no alarm condition. Red means an alarm condition exists. Use the **`alarmstat`** or **`faultstat`** commands for more information (see ***Chapter 3 - Console Port Control and Status***).



RS-232 Connector — This DB-9M connector provides the RS-232 serial I/O interface to the FDC. This allows the user to initialize, monitor and control the FDC. For signal definition, see ***Appendix E - Specifications, RS-232 Serial Port I/O***.

10/100Base-T Jack — This RJ-45 connector mates with the Ethernet twisted pair cable from the network.

Signal Input A/B Jacks — These two BNC connectors accept the A and B analog signal inputs.

Disable Input A/B Jacks — These two BNC connectors accept the A and B logic level external alarm inputs. If properly configured (see **`disablemode`**), a high level on this input will disable the corresponding Signal Input.

Alarm Output Jack — This BNC connector provides the open-collector Alarm output. This output is asserted during the power-on/startup sequence and when an alarm condition exists.

Signal Output 1-10 Jacks	These ten BNC connectors provide the analog signal outputs.
AC Power Input Jack	This IEC 320 standard three-prong connector provides AC power.
DC Power Input Block	This optional 3-position terminal block provides connection to the DC power source, and replaces the AC power input jack. See details in ***Appendix E - Specifications.***

Installing the FDC

FCC NOTICE

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Mount the FDC

Using standard 19" rack mounting hardware, mount the unit in the desired location.

CAUTION

Ground the unit properly with the supplied power cord.

The socket outlet should be installed near the equipment and be easily accessible.

Power cord is used as a disconnection device. To de-energize equipment, disconnect the power cord. If your FDC has dual power supplies, then multiple power cords may be installed. To de-energize this equipment, disconnect all power cords from the device.

Do not install the FDC where the operating ambient temperature might exceed 122°F (50°C).

Connecting the DC Power Option

Connect the safety ground terminal to earth ground. Connect the "+" terminal to the positive output of the DC power source. Connect the "-" terminal to the negative output of the DC power source. Note that the FDC has a "floating" internal power supply, therefore either the positive or negative output of the DC power source can be referenced to earth ground. This unit will not operate if the +/- connections are reversed; however it will not be damaged by a reverse connection.

SHOCK/ENERGY HAZARD

Install in Restricted Access Location.

Use 10-14 AWG copper wire only.

Terminal block screw torque: 9 in-lbs (1 nM).

Branch circuit must have circuit breaker, 15A or less.

Power must be sourced via two-pole disconnect device.

Install terminal block cover after wiring.

Connect the RS-232 Serial I/O Port

If your network *does not* use DHCP, you will need to configure your Ethernet interface using the RS-232 serial I/O port. If your network *does* use DHCP, you may wish to connect the serial port now, since it will help you in debugging any problems you may encounter with automatic configuration via DHCP. But, if you want to skip the RS-232 serial port setup, proceed to ***Verify Network Configuration*** later in this chapter.

To test serial communications with the FDC you will need either a VT100 compatible terminal or a terminal emulation program running on your computer. We will refer to either of these as "terminal" for the remainder of this instruction.

1. Disconnect power from the FDC.

2. Connect one end of the DB9F-to-DB9F null modem adapter cable to the serial I/O jack on the FDC.

3. Connect the other end of the DB9F-to-DB9F null modem adapter cable to the terminal. If the serial I/O port on your terminal does not have a DB9M connector, you may need to use an adapter. Refer to ***Appendix E - Specifications*** for details on the signal wiring. *If you are using a computer for your terminal, remember which port you are using because you will need to know that in order to set up your terminal software.*

NOTE

You must use an RS-232 null-modem cable or adapter if you are connecting the FDC to another computer. The cable included in the shipping kit is a null-modem cable.

If your computer does not have a serial port, you can use a USB port with a USB-RS232 converter similar to Gearmo GM-FTDI-8. First, connect the USB converter to your computer, then connect the converter to the null-modem cable. Finally, connect the null-modem cable to the FDC.

Test the Serial Port

You must configure your terminal to use the serial I/O port you used in ***Connect the RS-232 Serial I/O Port*** above. You must also configure your terminal as shown below:

- Baud Rate: 19200
- Data Bits: 8
- Parity: None
- Stop Bits: 1
- Handshaking / Flow Control: OFF (both hardware and software)
- Terminal Emulation (if any): VT100 (or similar) or Linux

After configuring these parameters in your terminal, apply power to the FDC. After a few seconds, your terminal should display something similar to this:

```
**************************************************************************
* 6010-0084-000 v1.00 XDC330Xe Bootloader Thu Aug  9 21:14:40 UTC 2018  *
**************************************************************************


Current default Kernel/Root File System:  FACTORY/FACTORY

You can:

  Override the default kernel and/or root file system boot configuration,
  and/or
  Reset the root password to the factory password

By typing these commands:

  bootcfg=*#     (* = 0 or 1 to select FACTORY or UPGRADE kernel,
                  # = 0 or 1 to select FACTORY or UPGRADE root file system)

  pwrst=xxxxxxxx (xxxxxxxx is reset code obtained from EndRun Tech Support)

Begin typing within 5 seconds to extend the boot timeout.

Booting current default Kernel/Root File System:  FACTORY/FACTORY
```

These lines are the Linux bootloader boot prompts. The prompt will timeout after five seconds and the factory default Linux kernel and the factory default FDC root file system will be loaded. When the Linux kernel is loaded from FLASH memory into RAM a long list of kernel-generated, informational messages is displayed as the kernel begins execution and the various device drivers are initialized. When the boot process completes, the FDC login prompt is displayed:

```
**************************************************************************
*           Welcome to FDC3300e console on:  FDC3300e.your.domain
*           Tue Aug 21  2018 21:47:03 UTC
**************************************************************************

FDC3300e login:
```

Here you may log in as “sysuser” with password “Praecis” or you may log in as the “root” user with password “endrun_1”. When logged in as “sysuser”, you may check status information and view log

files but you will not be able to modify any system settings or view secure files. In order to perform system setup procedures, which includes configuring the IP network settings, you must log in as the "root" user. After correctly entering the password at this prompt,

```
password:
```

the sign on message is shown. It identifies the host system as FDC3300e and shows the software part number, version and build date. The out-of-the-box hostname is set to "FDC3300e", and the domainname is set to "your.domain".

```
FDC3300e 6010-0083-000 v 1.00 - Mon Aug 13 20:31:37 UTC 2018
FDC3300e (root@FDC3300e:~)->
```

This last line is the standard FDC prompt. After configuring the unit, you should change the passwords using the Linux **`passwd`** command issued from the prompt.

If you do not see characters displayed by your terminal program within 30 seconds after the unit is powered up, you must troubleshoot your setup. An incorrectly wired cable or incorrect port setting in your terminal emulation program are the most common problems. Refer to ***Appendix E - Specifications*** for the signal connections for the FDC.

Connecting and Configuring Ethernet

Connect one end of the CAT-5 patch cable supplied with your FDC to the RJ-45 connector labeled 10/100BASE-T. Connect the other end of the patch cable to your network through a 'straight' port on your switch. Do not connect it to a 'crossover' port on your switch.

By factory default, the FDC will attempt to configure the Ethernet interface automatically via the Dynamic Host Configuration Protocol (DHCP). The FDC will attempt to set the netmask, its IP address, the IP address of the default gateway, the domain name and the IP addresses of any nameservers, if the DHCP server is configured to provide them. You may optionally configure the FDC to also set its hostname via DHCP, if your DHCP server is configured to provide it. You can do this by running a simple script called **`netconfig`** after your unit is up on the network.

If your network *does* use DHCP for host configuration, you may proceed to ***Verify Network Configuration*** to make sure that the network parameters were set up correctly.

If your network *does not* use DHCP, you will need to configure your Ethernet interface using the RS-232 serial I/O port. The following sections assume you have already connected and tested your serial port. If you have not, see the previous section - ***Connect the RS-232 Serial I/O Port.***

Configuring Ethernet with the Serial Port

To configure your Ethernet interface with the serial port, after logging in as the *root* user, you must run a simple script called **`netconfig`**. This script will prompt you for the needed information and perform some syntax checking on your inputs. Then it will create or modify the appropriate files needed to configure the Ethernet interface. The following sections will guide you in setting up communications with the FDC using its RS-232 serial I/O port.

Once you have successfully established communications with the FDC, you may proceed to configure the network parameters using **netconfig** (see below). Then you can communicate with the FDC over the network using **telnet** or **ssh** and synchronize its system clock to your network computers using NTP.

Using netconfig to Set Up Your IP

The following shows the beginning of the **netconfig** interactive script:

```
*****************************************************************************
************   FDC3300e IPV4/IPV6 Network Configuration    ****************
*****************************************************************************
*
*   This script will configure the TCP/IPV4/IPV6 network parameters for
*   your FDC3300e.  We will first configure IPV4 and then IPV6.  Your
*    FDC3300e has one Ethernet interface, called eth0.
*
*   You can also choose to unconfigure IPV4 or IPV6 on eth0.
*   You will be able to reconfigure your system at any time by typing:
*
*   netconfig
*
*   The settings you make now will not take effect until you reboot your
*   FDC3300e, so if you make a mistake, just re-run this script before
*   rebooting.
*
*   You will be prompted to enter your IPV4/IPV6 network parameters now.
*
*****************************************************************************
*****************************************************************************

Configure IPV4 for eth0?
  (Answer yes to continue on and reconfigure eth0 for IPV4.)
  (Answer no to "unconfigure" eth0 for IPV4.  Only the
   IPV4 loopback interface will be setup.) ([y]es, [n]o):
```

After configuring your Ethernet interface, you should shutdown the FDC and reboot it by issuing this command at the prompt:

```
FDC3300e (root@FDC3300e:~)-> reboot
```

Verify Network Configuration

If you are using the RS-232 serial I/O port to communicate with the FDC, you will be able to see the kernel-generated boot messages when the unit reboots. You should note the line

```
Configuring eth0 as 192.168.1.120...
```

if you have set up a static IP address, or this line

```
Attempting to configure eth0 by contacting a DHCP server...
```

if you are using DHCP. These appear near the end of the kernel generated boot messages.

If you are using DHCP and are not using the RS-232 serial I/O port, you will have to check the DHCP configuration information maintained by your DHCP server to determine the expected IP address and log in to the FDC using **telnet** or **ssh** to verify successful DHCP configuration. Refer to the subsequent topics in this section ***Using Telnet*** and ***Using SSH***, for details on logging in to the FDC that way. Once you have logged in, you may perform the following checks.

If you are not using DHCP, the IP address shown should match the static IP address which you entered during the **netconfig** procedure. If so, log in as "root" at the login prompt and check the other configuration parameters using **ifconfig**:

```
FDC3300e(root@FDC3300e:~)-> ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.99  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 00:0e:fe:02:00:00  txqueuelen 1000  (Ethernet)
        RX packets 1063027  bytes 96545722 (92.0 MiB)
        RX errors 0  dropped 80676  overruns 0  frame 0
        TX packets 177680  bytes 13331719 (12.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 25  base 0x8000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 504204  bytes 112820792 (107.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 504204  bytes 112820792 (107.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Pay particular attention to the settings shown for **eth0**, in particular the **Mask**: setting, which should match that which is appropriate for your network. Now check the remaining configuration parameters using **route**:

```
FDC3300e (root@FDC3300e:~)-> route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         192.168.1.1     0.0.0.0         UG    1      0        0 eth0
loopback        *               255.0.0.0       U     0      0        0 lo
localnet        *               255.255.255.0   U     0      0        0 eth0
```

Here you are interested in the default gateway address. It should match the appropriate one for your network. If so, then the Ethernet interface of your FDC has been successfully configured to operate on your network and you are ready to check operation of the FDC over the network. If not, you should recheck your configuration and/or repeat the **netconfig** procedure.

If you have configured a nameserver(s) for your network, you may check that by issuing this command:

```
FDC3300e (root@FDC3300e:~)-> cat /etc/resolv.conf
search your.domain
nameserver 192.168.1.1
nameserver 192.168.1.2
```

Which displays the contents of the */etc/resolv.conf* file containing the domain name you entered previously using **netconfig**, and the nameserver IP address(es) to use for that domain.

Check Network Operation

With your FDC network parameters properly configured, you are ready to test the setup using **ping** from a server or workstation that is able to access the network connected to the FDC. Alternatively, you could **ping** one of your servers or workstations from the FDC prompt to test the setup.

Once you have successfully established network communications with the FDC, you may perform all maintenance and monitoring activities via **telnet** and **ftp**. The FDC provides both client and server operation using **telnet**. For security reasons, only client operation is supported using **ftp**. You may also monitor the FDC via the HTTPS interface (see ***Chapter 6 - HTTP/HTTPS***).

Security conscious users will want to use **ssh**, the secure shell replacement for **telnet**, as the login means. The companion utility, **scp** provides a secure replacement for **ftp** as a means of transferring files to and from the FDC. Both of these protocols are supported in the FDC via the OpenSSH implementations for Linux. Refer to ***Chapter 5 - Security, OpenSSH*** for more information about the secure shell protocol.

Using Telnet

When establishing a **telnet** connection with your FDC, logging in directly as *root* is not permitted. This is a security measure that makes it slightly more difficult to gain access by simply trying passwords, since it is also necessary to know the name of a user. When you initiate a **telnet** session with the FDC, this banner will be displayed:

```
*******************************************************************************
*        Welcome to FDC3300e telnet console on:  host.your.domain
*******************************************************************************

host login:
```

Here you may log in as “sysuser” with password “Praecis”. When logged in as “sysuser”, you may check status information and view log files but you will not be able to modify any system settings or view secure files. After correctly entering the password at this prompt,

```
Password:
```

the sign on message is shown. It identifies the host system as FDC and shows the software part number, version and build date:

```
FDC3300e 6010-0083-000 v 1.00 - Mon Aug 13 20:31:37 UTC 2018
FDC3300e (root@FDC3300e:~)->
```

This last line is the standard FDC prompt. After configuring the unit, you should change the passwords using the Linux **passwd** command issued from the prompt.

To gain *root* access, you must now issue the “super user” command at the prompt:

```
FDC3300e (root@FDC3300e:~)-> su root
```

You will then be prompted for the password, which is “endrun_1”, and be granted *root* access to the system. To leave “super user” mode, issue the command **exit**. Issuing **exit** again will close the **telnet** session.

Using SSH

When establishing a **ssh** connection with your FDC, logging in directly as *root* is permitted. When you log in as *root* via a **ssh** session with the FDC, this banner will be displayed:

```
**************************************************************************
*   Welcome to the FDC3300e SSH console on:  host.your.domain
**************************************************************************

root@192.168.1.120's password:
```

Here you may log in as "root" with password "endrun_1". After correctly entering the password the sign on message is shown. It identifies the host system as FDC and shows the software part number, version and build date:

```
FDC3300e 6010-0083-000 v 1.00 - Mon Aug 13 20:31:37 UTC 2018
FDC3300e (root@FDC3300e:~)->
```

This last line is the standard FDC prompt. After configuring the unit, you should change the passwords using the Linux **passwd** command issued from the prompt.

Issuing **exit** will close the **ssh** session.

Using HTTPS

You may monitor the status of the FDC via the HTTPS interface. For security reasons, you may not change any settings via the HTTPS interface. See ***Chapter 6 - HTTP/HTTPS*** for more information.

IMPORTANT

SSH, Telnet, SNMP and HTTPS are all enabled with default passwords. To ensure security, change the passwords or disable the protocols.

To change the passwords for SSH, Telnet and HTTPS use the Linux **passwd** command. To change the passwords/community strings for SNMP see ***Chapter 4 - SNMP***.

To disable Telnet, SSH, SNMP and HTTPS see ***Chapter 5 - Security, Disable Protocols***.

Connecting Instruments to the FDC

Connect Signal Inputs and Outputs

Using coaxial cables, connect your analog signal(s) to the Signal Input A and/or Signal Input B on the FDC3300e. The factory default for the FDC **`switchmode`** setting is for Signal Input A to be the primary and Signal Input B to be the secondary. You can change this by using the **`switchmode`** command over the serial I/O port.

Connect coaxial cables from each of the FDC signal outputs to your equipment.

Connect Disable Inputs (External Alarm Inputs)

If the source(s) of your reference signal(s) has (have) compatible TTL alarm output(s) that you would like to use to force signal input switching on your FDC, connect these using coaxial cables to the Disable A and/or Disable B input(s) on the FDC. The factory default for the FDC **`disablemode`** setting is to ignore these inputs. If you plan to use them, you will need to use the **`disablemode`** command over the serial I/O port to configure them.

Connect Alarm Output

If you are using the FDC summary alarm output, connect a coaxial cable from the equipment that will be monitoring the FDC to the Alarm output on the FDC.

This page intentionally left blank.

Chapter *Three*

Console Port Control and Status

This chapter describes FDC3300e (FDC) control and status commands used via the Linux console. The console is accessed via the Ethernet port or the RS-232 serial port. FDC supports several application-specific commands for configuration and for monitoring the performance and status of the Linux and Distribution Subsystems.

You do not need knowledge of Linux commands in order to operate the FDC. *However, FDC does support a subset of the standard Linux commands and utilities and it uses the* **`bash`** *shell, which is the Linux standard, full-featured shell. A wealth of information is available from a variety of other sources on Linux.*

FDC-specific commands will be described in this chapter. For a brief description of some of the most useful Unix/Linux commands, see ***Appendix C - Helpful Linux Information***.

Console Ports

Two interface ports are available on FDC. The 10/100 Base-T Ethernet port and the RS-232 serial port. A network cable and serial cable are provided with each FDC shipment. The serial cable is wired as a null-modem adapter and can be used to connect FDC to the serial port on your computer. Detailed specifications on the ports, including the RS-232 pinout, are in ***Appendix E - Specifications***.

General Linux Operation

You do not need to know Linux in order to operate FDC. However, for those interested, the command shell used by FDC is the Linux standard: **`bash`**. All commands and file names are case sensitive, which is standard for Unix-like operating systems. For a brief description of some of the most useful Unix/Linux commands, see ***Appendix C - Helpful Linux Information***.

If you are unfamiliar with Unix-like operating system, and you would like to be able to more closely monitor or customize the operation of your network interface, then you should consult good Linux reference books or the Linux Documentation Project at::

http://www.tldp.org

Available User Commands

COMMAND	FUNCTION
accessconfig	Interactive script that guides you in configuring **`telnet, ssh`** and **`snmpd`** access to FDC that is limited to specific hosts. The resulting */etc/hosts.allow* and */etc/hosts.deny* files are saved to the non-volatile FLASH disk. Factory default configuration allows access by all hosts.
alarmstat	Prints system alarm information as a series of zeros and ones. Where '1' means the alarm is asserted and '0' means it is not. An 'x' means it is not installed.
dcreset	This will cause a system reset of the Distribution Subsystem.
dcreturn	Tells the Distribution Subsystem to return to the primary input.
dcversion	Prints the software and FPGA version information for the Distribution Chassis Subsystem.
disablemode	Configures Disable A and Disable B inputs.
disablestat	Prints the current status of the Disable A and Disable B inputs. A '1' means the input is asserted and '0' means it is not.
faultstat	Prints the summary of all system fault states in a user-friendly format.
help	Prints help for all distribution chassis commands.
inetdconfig	Interactive script that allows you to configure the list of protocol servers which are started by the **`inetd`** superserver daemon running in FDC.
kernelversion	Prints the Linux operating system kernel version.
netconfig	Interactive script that allows you to configure the IP network of the FDC.
ntpconfig	Interactive script that guides you in configuring the NTP Subsystem. Allows configuration of MD5 authentication and broadcast/multicast mode. All parameters are retained in FLASH disk storage.
ntpstat	Prints the values of several key parameters indicating the status of the NTP daemon.
pwrstat	Prints the current status of the power supplies. A '1' means the power supply is operational. A '0' means it is not.
selectedin	Prints the currently selected Signal Input A, B or NONE.
serialnumber	Prints the serial number of the FDC.
settings	Prints all user setting commands which include DISABLEMODE and SWITCHMODE.
siginstat	Prints the current status of Signal Inputs A and B. A '1' means the signal is present and a '0' means it is not.
sigoutstat	Prints the current status of the Signal Outputs 1 through 10 as a sequence of 10 characters. A '1' means the signal is present and a '0' means it is not.

status	Prints all system status commands which include ALARMSTAT, DISABLESTAT, PWRSTAT, SELECTEDIN, SIGINSTAT, and SIGOUTSTAT.
switchmode	Configures the switching mode, AB, BA, A or B.
syskernel	Prints the currently booted linux kernel, either 0 or 1, where 0 is the factory-installed kernel and 1 is the upgraded kernel.
sysrootfs	Prints the currently loaded linux root file system image, either 0 or 1, where 0 is the factory-installed root file system, and 1 is the upgraded root file system.
sysversion	Prints the Linux root file system version information.
updatekernelflag	Command to update the flag stored in FLASH that is read by the Linux bootloader at boot time to select operation with either the factory-installed or upgraded kernel.
updaterootflag	Command to update the flag stored in FLASH that is read by the Linux bootloader at boot time to select operation with either the factory-installed or upgraded root file system.
upgradekernel	Command that performs the Linux Kernel upgrade process.
upgradekerneldtb	Command that upgrades the Linux Kernel Device Tree Blob. It is highly unlikely that it will ever be needed.
upgraderootfs	Command that performs the Linux Root File System upgrade process.
upgradesubsys	Command that performs the Distribution Subsystem upgrade process.

Detailed Command Descriptions

accessconfig

This command starts an interactive script that will allow the root user to configure access limitation via **`telnet`**, **`ssh`** and **`snmp`** to FDC. By default, the unit is configured to allow access by all users. If you need to limit **`telnet`**, **`ssh`** or **`snmp`** access, e.g. for security reasons, you must run this script as root from either the RS-232 serial I/O port or from a **`telnet`** or **`ssh`** session.

This script modifies these files: */etc/hosts.allow* and */etc/hosts.deny*. These are non-volatilely stored in the FLASH disk */boot/etc* directory. You must reboot FDC after running this script for the changes to take effect.

Command: **`accessconfig`**
FDC reply: Interactive script is started.

alarmstat

This query-only command displays the current system alarms as a series of characters, listed left to right. Each character is a ‘0’, a ‘1’ or an ‘X’. A ‘1’ means the corresponding alarm is active. A ‘0’ means it is OK. An ‘X’ means the optional component is not installed in this particular unit.

Group 1 (6 characters)	Group 2 (10 characters)	Group 3 (4 characters)
Signal Input A absent	Output 1 signal absent	System Oscillator error
Signal Input B absent	Output 2 signal absent	Flash error
Disable A asserted	Output 3 signal absent	FPGA error
Disable B asserted	Output 4 signal absent	Dist.Subsystem Comm
Power Supply A failed	Output 5 signal absent	
Power Supply B failed (option)	Output 6 signal absent	
	Output 7 signal absent	
	Output 8 signal absent	
	Output 9 signal absent	
	Output 10 signal absent	

Command: **`alarmstat`**
FDC reply: **`01000X 0000000000 0000`** (An alarm exists on Signal Input B. Also, Power Supply B is not installed.)

NOTE

System alarms will clear automatically once the problem has been corrected.

dcreset

This command will cause a software reset of the Distribution Subsystem. It is similar to a power cycle, but the Linux subsystem is not rebooted.

Command: **`dcreset`**
FDC reply: **`OK`** (The Distribution subsystem will reset.)

dcreturn

After the chassis has switched from the primary to the secondary signal input, this command is used to return to the primary input. After you have restored the signal on primary input, type **`dcreturn`** to force the chassis to switch back to primary. An alternate way to force the chassis to switch back to the primary input is by removing the secondary disable input (provided that **`disablemode`** has been configured properly). It is also possible to accomplish the return by physically disconnecting the secondary input momentarily. However this will cause a brief interruption in the output signal during the switch. For this reason, using **`dcreturn`** or the disable input are the preferred methods.

This command is also used after the chassis has switched from the primary signal input to no signal input (**`selectedin`** is **`NONE`**). This will occur if **`disablemode`** has been configured to allow it. If the selected input is NONE then correct the problem and enter the **`dcreturn`** command to restore the unit to proper operation.

Command: **`dcreturn`**
FDC reply: **`OK`** (The chassis will return to the primary input.)

dcversion

This query-only command will show the current firmware and FPGA version information of the Distribution Subsystem.

Command: **dcversion**
FDC reply:
F/W 6010-0077-000 Ver 1.00 - FPGA 6020-0006-000 Ver 04 - AUG 11 14:08:44 2018

disablemode

This command allows you to select external alarm inputs from the reference source (if any) as specified in Appendix E. (These inputs are labeled "DISABLE IN" on the rear-panel.) When the external alarm input is asserted it will disable the corresponding reference signal input and/or set a system alarm. If you are not using external alarms then set **disablemode** to N,N. Disablemode syntax is:

disablemode a,b,x

where parameter a is Y (yes) or N (no) for whether to use the Disable A input or not. Parameter b is Y or N for whether to use the Disable B input or not. Parameter x tells the chassis what action to take when there is no good input signal to switch to: ON to leave the selected input on, or OFF to switch both reference inputs off when they both have a fault. This parameter can be left blank if both Disable inputs are to be ignored.

If **disablemode** is N,N the chassis will ignore the Disable A and Disable B inputs. If **disablemode** is Y,Y,OFF (or N,Y,OFF or Y,N,OFF) the chassis will turn off the last selected reference input when it sees Disable asserted and there is no good signal present on the other input. For example:

Example 1: If **disablemode** is Y,N,OFF and **switchmode** is A, then there is no secondary reference input and the chassis cannot switch if the Disable A input is asserted. If Disable A is asserted, Signal Input A will be switched off, which will switch off all the outputs.

Example 2: If **disablemode** is Y,Y,OFF and **switchmode** is AB and the Disable A input is asserted, the chassis will switch to Signal Input B. However, if Input B has a problem (input signal goes away or Disable B is asserted) then the chassis will switch off Signal Input A, which will switch off all the outputs.

NOTE: If both Input A and B have been switched off then you must enter the **dcreturn** command after you have corrected the problem.

If **disablemode** is Y,Y,ON (or N,Y,ON or Y,N,ON) then the chassis will switch between the primary and secondary inputs as described above when Disable is asserted, but it will never switch both the inputs off.

Typing **disablemode** with no parameters will display the current setting.

If you change this setting it will be saved in non-volatile memory. *This is a configuration command and if the parameters are changed this will cause a re-initialization of the software.*

Command:	**disablemode y,n,on**	
FDC reply:	**OK**	(Disable A is valid and Disable B is ignored. The chassis will leave the inputs on if Disable A is asserted.)
Command:	**disablemode**	
FDC reply:	**y,n,on**	

disablestat

This query-only command shows the status (signal levels) of the Disable A and Disable B inputs. The first character is for Disable A and the second character is for Disable B. A '0' means the disable input is low, and a '1' means the disable input is high (asserted - a fault condition).

Command:	**disablestat**	
FDC reply:	**01**	(Disable B input is asserted. Disable A is not.)

faultstat

This command returns the summary of all system and distribution subsystem fault states in a user-friendly format. An example is shown below.

Command: **faultstat**

Chassis reply:

```
Group 1 Fault Status:
  Signal Input A---------------------------------> OK
  Signal Input B---------------------------------> OK
  Disable Input A--------------------------------> OK
  Disable Input B--------------------------------> OK

Group 2 Alarm Status:
  Output 1---------------------------------------> OK
  Output 2---------------------------------------> OK
  Output 3---------------------------------------> OK
  Output 4---------------------------------------> *FAULT*
  Output 5---------------------------------------> OK
  Output 6---------------------------------------> OK
  Output 7---------------------------------------> OK
  Output 8---------------------------------------> OK
  Output 9---------------------------------------> OK
  Output 10--------------------------------------> OK

Group 3 Alarm Status:
  System Oscillator------------------------------> OK
  FLASH------------------------------------------> OK
  FPGA-------------------------------------------> OK
  Subsystem Communication------------------------> OK
```

Contact EndRun Customer Support if one of the Group 3 alarms persist.

help

This query-only command displays a list of the distribution chassis commands. To get help on a particular command you would type **help**, followed by the command.

Command: **help**
FDC reply: All commands are displayed.
Command: **help faultstat**
FDC reply: Information specific to the **faultstat** command is displayed.

inetdconfig

This command starts an interactive script that allows you to configure the list of protocol servers which are started by the **inetd** super-server daemon running in FDC. Three protocol servers may be configured: Time, Daytime, and Telnet. By default, the unit is configured to start Telnet. If you need to disable it you must run this script as *root* from either the RS-232 serial I/O port or from a **telnet** or **ssh** session. This script modifies the */etc/inetd.conf* file, which is non-volatilely stored in the FLASH disk */boot/etc* directory. You must reboot FDC after running this script for the changes to take effect.

Command: **inetdconfig**
FDC reply: Interactive script is started.

netconfig

This command starts an interactive script that allows you to configure the IP network subsystem of FDC. By default, the unit is configured to configure itself using the Dynamic Host Configuration Protocol (DHCP). If you need to set up static IP configuration, you must run this script as *root* from the RS-232 serial I/O port during the installation process. Refer to ***Chapter 2 - Basic Installation, Using netconfig to Set Up Your IP*** for details on the use of the command.

This script creates or modifies these files: */etc/HOSTNAME*, */etc/hosts*, */etc/networks, /etc/resolv.conf* and */etc/rc.d/rc.inet1.conf*. All of these are non-volatilely stored in the FLASH disk */boot/etc* directory. You must reboot FDC after running this script for the changes to take effect.

Command: **netconfig**
FDC reply: Interactive script is started.

ntpconfig

This command starts an interactive script that allows you to configure the NTP Subsystem of your FDC. It is highly recommended to configure stratum 2 operation of your FDC so that the system log files will have meaningful timestamps. You must run this script as root. By default, the unit is configured to authenticate with a set of default MD5 keys in the */etc/ntp.keys* file. In addition to setting up stratum 2 operation, this script will allow you to create your own MD5 keys (recommended) or set up broadcast/multicast client operation. Refer to ***Chapter 7 - Configuring FDC as a Stratum 2 Server*** for details on the use of this command.

The two files that are modified are */etc/ntp.keys* and */etc/ntp.conf*. Both of these are non-volatilely stored in the FLASH disk */boot/etc* directory. You must reboot FDC after running this script for the changes to take effect.

Command: **ntpconfig**
FDC reply: Interactive script is started.

ntpstat

This command provides some key information regarding the operation of the NTP daemon. The format of the response shows the current status of the NTP daemon:

YYYY MMM DD HH:MM:SS IPADDR S +S.sssssssss sec +FF.ffffff ppm LI

Where:

YYYY MMM DDD is the UTC year, month and day-of-month.

hh:mm:ss	are the UTC hours, minutes and seconds.
IPADDR	is the reference ID of the NTP server currently being used for synchronization.
S	is the stratum level of the NTP daemon (the reference server stratum + 1).
+S.sssssssss sec	is the offset in seconds between the NTP system clock and the reference server.
+FF.ffffff ppm	is the frequency offset of the Linux Subsystem oscillator in PPM.
LI	are the leap second indicator bits as received from the reference server.

Below is an example of a typical response to this command:

Command: **ntpstat**
FDC reply:

```
2018 Jun 01 15:46:30 192.168.0.241  2 +0.000024560 sec +30.146700 ppm 00
```

pwrstat

This query-only command shows the status of the power supplies and power inputs. The distribution chassis is capable of having two power supplies (for redundancy) but the standard unit has only one. The second is an option. The **pwrstat** response will show two characters - the first is for the standard power supply. The second is for the optional power supply. A '0' means the power input is not present, the power supply has failed, or the power supply is not installed (in the case of the optional supply). A one '1' means the power supply is good. An 'x' means the optional power supply is not installed.

Command: **pwrstat**
FDC reply: **1X** (The first supply (Power A) is good. The second supply (Power B) is not installed.

selectedin

This query-only command shows the currently selected signal input, either A, B or NONE.

Command: **selectedin**
FDC reply: **A** (Currently selected input is Signal Input A.)

serialnumber

This command shows the serial number of the FDC.

Command: **serialnumber**
FDC reply: **18080056**

settings

This query command displays all Distribution Subsystem command settings.

Command: **settings**
FDC reply:
```
disablemode = Y,Y,ON
switchmode = AB
```

siginstat

This query-only command shows the current status of both Signal Inputs A and B. The first character is for Signal Input A and the second character is for Signal Input B. A '0' means a signal is not present and a '1' means a signal is present.

Command: **siginstat**
FDC reply: **10** (Signal Input A is present. Signal Input B is not.)

sigoutstat

This query-only command shows the current status of Output Signals 1 though 10. The first character is for Output 1, the second is for Output 2, and so on. A '0' means there is no input signal, the output driver is bad or a short is connected to it. A one '1' means there is an input signal and the output signal is good.

Command: **sigoutstat**
FDC reply: **1011111111** (A problem exists at Output 2.)

status

This command displays the results of all Distribution Subsystem status query commands.

Command: **status**
FDC reply:
```
alarmstat = 01000X 0000000000 0000
disablestat = 01
pwrstat = 1X
selectedin = A
siginstat = 10
sigoutstat = 1011111111
```

switchmode

This command sets the switching mode in case a fault is detected. A fault is either lack of signal presence or a logic high level on Disable A or Disable B, provided these have been configured properly (see **disablemode**). Syntax is: **switchmode x**

Where **x** is A, B, AB, or BA. If **switchmode** is **ab** then the chassis will use Signal Input A as its primary source and Signal Input B as its secondary source. This means the chassis will switch to Signal Input B if a problem on A occurs. If **switchmode** is **ba** then the reverse is true. If **switchmode** is **a** or **switchmode** is **b** then there is no secondary input. The chassis will either remain on the primary signal input or will switch it off, depending on the **disablemode** setting. Typing **switchmode** with no parameter will display the current **switchmode** setting. The factory default setting is: **ab**

If you change this setting it will be saved in non-volatile memory. *This is a configuration command and if the parameters are changed this will cause a re-initialization of the software.*

Command:	**switchmode ba**	
FDC reply:	**OK**	(B is primary. A secondary.)
Command:	**switchmode**	
FDC reply:	**BA**	

syskernel

This command returns the currently booted linux kernel, either 0 or 1, where 0 is the factory-installed kernel and 1 is the upgraded kernel.

Command:	**syskernel**
FDC reply:	**BOOTED KERNEL IMAGE = 1 (Upgrade)**

sysrootfs

This command returns the currently loaded linux root file system, either 0 or 1, where 0 is the factory-installed root file system and 1 is the upgraded root file system.

Command:	**sysrootfs**
FDC reply:	**BOOTED ROOT FILE SYSTEM IMAGE = 1 (Upgrade)**

sysversion

This command displays the firmware version and build date of the Linux root file system.

Command:	**sysversion**
FDC reply:	**FDC3300e 6010-0083-000 v 1.00 - Aug 16 22:38:21 2018**

updatekernelflag

This command allows you to update the configuration of the Linux bootloader after a new kernel image has been written to the UPGRADE kernel partition of FDC FLASH disk. You may also use it to reset the default back to the FACTORY kernel partition. Refer to ***Appendix B - Upgrading the Firmware, Performing the Linux Kernel Upgrade*** for detailed instructions for performing the upgrade procedure. One argument is accepted, whose value is either 0 or 1, which causes a flag to be set that indicates to the bootloader which kernel image should be loaded by default. If an argument value of 2 is given, then the currently configured default kernel is shown.

Command:	**updatekernelflag 1**
FDC reply:	**Default Kernel now set to: UPGRADE**
Command:	**updatekernelflag 2**
FDC reply:	**Default Kernel = UPGRADE**

updaterootflag

This command allows you to update the configuration of the Linux bootloader after a new root file system image has been written to the UPGRADE root file system partition of FDC FLASH disk. You may also use it to reset the default back to the FACTORY root file system partition. Refer to ***Appendix B - Upgrading the Firmware*** for detailed instructions for performing the upgrade procedure. One argument is accepted, whose value is either 0 or 1, which causes a flag to be set that indicates to the bootloader which root file system image should be loaded by default. If an argument value of 2 is given, then the currently configured default root file system is shown.

Command:	**updaterootflag 1**
FDC reply:	**Default Root File System now set to: UPGRADE**
Command:	**updaterootflag 2**
FDC reply:	**Default Root File System = UPGRADE**

upgradekernel

This utility allows you to upgrade the Linux Kernel. It is run after the *kernel.gz* file has been copied to the */tmp* directory on the system. It performs an erase of the upgrade kernel partition and then writes the */tmp/kernel.gz* file to it. Refer to ***Appendix B - Upgrading the Firmware, Performing the Linux Kernel Upgrade*** for detailed information.

Command:	**upgradekernel**
FDC reply:	Shows progress indicator.

upgradekerneldtb

This utility allows you to upgrade the Linux Kernel Device Tree Blob (DTB), which contains a description of the hardware device information for the kernel. It is run after the *kernel.dtb* file has been copied to the */tmp* directory on the system. It performs an erase of the upgrade kernel DTB partition and then writes the */tmp/kernel.dtb* file to it. Refer to ***Appendix B - Upgrading the Firmware, Performing the Linux Kernel Upgrade*** for detailed information.

Command:	**upgradekerneldtb**
FDC reply:	Shows progress indicator.

upgraderootfs

This utility allows you to upgrade the Linux Root File System. It is run after the *rootfs.gz* file has been copied to the */home* directory on the system. It performs an erase of the upgrade root file system partition and then writes the */home/rootfs.gz* file to it. Refer to ***Appendix B - Upgrading the Firmware, Performing the Linux RFS Upgrade*** for detailed information..

Command: **upgraderootfs**
FDC reply: Shows progress indicator.

upgradesubsys

This utility allows you to upgrade the Distribution Subsystem firmware. Prior to executing this command, you must copy the binary firmware file to be uploaded to the Distribution Subsystem to */tmp/subsys.bin*. It issues the commands over the serial port to the Distribution Subsystem that are needed to start the X-modem file transfer, and then displays progress to the console. See ***Appendix B - Upgrading the Firmware, Performing the Distribution Subsystem Upgrade*** for more information before using this command.

Command: **upgradesubsys**
FDC reply: Upgrade progress is shown.

Chapter *Four*

Simple Network Management Protocol (SNMP)

Your FDC3300e (FDC) includes the NET-SNMP version 5.5.1 implementation of an SNMP agent, **`snmpd`***, and a SNMP notification/trap generation utility,* **`snmptrap`***. It supports all versions of the protocol in use today: SNMPv1 (the original Internet standard), SNMPv2c (never reached standard status, often called "community SNMP") and SNMPv3 (the latest Internet standard).*

The NET-SNMP project has its roots in the Carnegie-Mellon University SNMP implementation. For more detailed information about the NET-SNMP project and to obtain management software and detailed configuration information, you can visit this website:

http://www.net-snmp.org

An excellent book which describes operation and configuration of various SNMP managers and agents, including the NET-SNMP implementations, is available from O'Reilley & Associates:

Essential SNMP, Mauro & Schmidt, O'Reilley & Associates, 2001

If you are planning to operate with SNMPv3, it is highly recommended that you make use of both of these resources to familiarize yourself with the agent configuration concepts.

SNMPv3 Security

Prior to SNMPv3, SNMP had definite security inadequacies due to using two community names in a manner analogous to passwords that were transmitted over the network as clear text. In addition, since no mechanism existed for authenticating or encrypting session data, any number of man-in-the-middle data corruption/replacement exploits were possible in addition to plain old snooping to learn the community names. SNMPv3 implements the User-based Security Model (USM) defined in RFC-2274 which employs modern cryptographic technologies to both authenticate multiple users and to encrypt their session data for privacy, much in the same way that SSH does for remote login shell users.

In addition, it implements the View-based Access Control Model (VACM) defined in RFC-2275. This RFC defines mechanisms for limiting the access of multiple users having various security levels (no authentication, authentication or authentication plus privacy) to specific "views" of the Structure of Management Information (SMI) object tree.

Enterprise Management Information Base (MIB)

In addition to providing the SNMP variables contained in MIB-II as described in RFC-1213, EndRun Technologies has implemented an enterprise MIB using the syntax of the SMI version 2 (SMIv2) as described in RFC-2578. Your FDC will have the MIB listed below:

XDC330X-MIB

Which is located on your FDC in this ASCII file:

/usr/local/share/snmp/mibs/XDC330X-MIB.txt

In addition to a complete set of System and Distribution Subsystem status objects, the MIB defines five SMIv2 notification objects:

- Alarm Group 1 status change
- Alarm Group 2 status change
- Alarm Group 3 status change
- NTP Leap Indicator Bits status change
- NTP Stratum change

Invocation of the SNMP daemon

The SNMP daemon, **`snmpd`** is started from the */etc/rc.d/rc.snmpd* system start-up script. By default, it will listen on port 161 for SNMP queries from the network management system. If you would like to have it listen on another port, you could edit the file and change the port number in the argument list being passed to **`snmpd`** when it is started.

IMPORTANT

After modifying ***/etc/rc.d/rc.snmpd***, you must copy it to the ***/boot/etc/rc.d*** directory and reboot the system. It is very important to retain the access mode for the file, so be sure to use **`cp -p`** when performing the copy. During the boot process, the files contained in the ***/boot/etc/rc.d*** directory are copied to the working ***/etc/rc.d*** directory on the system RAM disk. In this way the factory defaults are overwritten.

Quick Start Configuration -- SNMPv1/v2c

You should be able to compile the MIB file on your SNMP management system and access the variables defined therein. The factory default community names are “XDC330X_0” for the read-only community and “endrun_1” for the read-write community. This is all that is required for operation under v1 and v2c of SNMP.

Change Default Community Strings (Passwords)

You can, and should, change the default community names by editing */etc/snmpd.conf* and modifying these two lines:

```
rwcommunity  endrun_1
rocommunity  XDC330X_0
```

Configuring SNMPv1 Trap Generation

To have your FDC send SNMPv1 traps (RFC-1215) you must configure the community and destination for SNMPv1 traps by uncommenting and editing this line in */etc/snmpd.conf*:

```
trapsink    xxx.xxx.xxx.xxx trapcommunity trapport
```

where **trapcommunity** should be replaced by your community, and **xxx.xxx.xxx.xxx** is the IP address or hostname of the destination host for receiving the traps generated by the FDC. By default, the trap will be sent to port 162. You may optionally add another parameter, **trapport** to the end of the above line to override the default port setting. Otherwise leave it blank.

Note: Though the agent will recognize multiple **trapsink** lines within */etc/snmpd.conf* and send the generic SNMP coldStart or authenticationFailure traps to multiple destinations, the FDC enterprise MIB trap generation mechanism will only send a trap to the last declared **trapsink** in the file.

Configuring SNMPv2c Notifications and Informs

To have your FDC send SNMPv2c notifications (SMIv2, RFC-2578) or informs, you must configure the communities and destinations by uncommenting and editing one or both of these lines in */etc/snmpd.conf*:

```
trap2sink    xxx.xxx.xxx.xxx trap2community trap2port
informsink   xxx.xxx.xxx.xxx informcommunity informport
```

where **trap2community** and **informcommunity** should be replaced by your communities, and **xxx.xxx.xxx.xxx** is the IP address or hostname of the destination host for receiving the notifications or informs generated by the FDC. By default, the v2c trap or inform will be sent to port 162. You may optionally add another parameter, **trap2port** or **informport** to the ends of the above lines to override the default port setting. Otherwise leave it blank.

Note: Though the **snmpd** agent will recognize multiple **trap2sink** or **informsink** lines within */etc/snmpd.conf* and send the generic SNMP coldStart or authenticationFailure notifications and informs to multiple destinations, the FDC enterprise MIB notification/inform generation mechanism will only send a notification to the last declared **trap2sink,** and an inform to the last declared **informsink** in the file.

IMPORTANT

After editing ***/etc/snmpd.conf***, you must copy it to the ***/boot/etc*** directory and reboot the system. It is very important to retain the access mode for the file (readable only by ***root***), so be sure to use **`cp -p`** when performing the copy. During the boot process, the files contained in the ***/boot/etc*** directory are copied to the working ***/etc*** directory on the system RAM disk. In this way the factory defaults are overwritten.

Configuration of SNMPv3

If you are planning to use SNMPv3, you should definitely make use of the two resources mentioned previously (NET-SNMP website and *Essential SNMP*) and study them carefully. There are rather elaborate configuration options available when you are using v3. The instruction presented here will give you the flavor of the configuration but definitely not the full scope of possibilities. To access your FDC via v3 of SNMP, you will have to configure two files:

/etc/snmpd.conf
/boot/net-snmp/snmpd.conf

The first file contains static configuration parameters that the agent uses to control access and to determine where to send notifications/traps. Other aspects of the agent's operation are also configurable in this file, but you should not need to modify those. To use the SNMPv3 capabilities of the FDC, you must first set up user information and access limits for those users in */etc/snmpd.conf*. Uncomment and edit these two lines to define your v3 users and their access parameters:

```
rwuser root    priv .1
rouser sysuser auth .1.3.6.1.4.1.13827
```

The first line defines a SNMPv3 read-write user *root* whose minimum security level will be authenticated and encrypted for privacy (choices are noauth, auth and priv), and who will have read-write access to the entire *iso(1)* branch of the SMI object tree. The second line defines a SNMPv3 read-only user *sysuser* whose minimum security level will be authenticated but not encrypted, and who will have read-only access to the entire *iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).endRunTechnologiesMIB(13827)* branch of the SMI object tree. After adding the user lines to */etc/snmpd.conf*, copy it to the */boot/etc* directory using **`cp -p`**.

The second file is located on the non-volatile FLASH disk and is used by the SNMP agent to store "persistent data" that may be dynamic in nature. This may include the values of the MIB-II variables sysLocation, sysContact and sysName as well as any configured SNMPv3 user crypto keys. In order to use SNMPv3, you must configure user keys in this file for each SNMPv3 user that you have set up in */etc/snmpd.conf*. To do this, you must add lines to */boot/net-snmp/snmpd.conf* like these for each user:

```
createUser root    MD5 endrun_1 DES endrun_1
createUser sysuser SHA XDC330X_0
```

The first line will cause the agent, **`snmpd`** to create a user *root* who may be authenticated via Message Digest Algorithm 5 (MD5) with password *endrun_1* and may use the Data Encryption Standard (DES) to encrypt the session data with passphrase *endrun_1*. The second line will cause a user *sys-*

user to be created who may be authenticated using the Secure Hash Algorithm (SHA) with password X*DC330X_0*. Passwords and passphrases must have a *minimum* of 8 characters, or you will not be able to be authenticated.

IMPORTANT

You must kill the **`snmpd`** daemon prior to editing, ***/boot/net-snmp/snmpd.conf***. Otherwise, the secret key creation may not complete properly. Issue the command **`/etc/rc.d/rc.snmpd stop`** to kill the **`snmpd`** daemon. You can verify that the **`snmpd`** daemon has been killed by issuing the **`ps -e`** command and verifying that it is not present.

After rebooting, the agent will read the */boot/net-snmp/snmpd.conf* configuration file and compute secret key(s) for each of the users and delete the **`createUser`** lines from the file. It will then write the secret key(s) to the file. These lines begin with the string, **`usmUser`**. In this way, un-encrypted passwords are not stored on the system.

IMPORTANT

To generate new keys, stop the **`snmpd`** process, delete the existing **`usmUser`** key lines from the file ***/boot/net-snmp/snmpd.conf*** and then add new **`createUser`** lines. Then reboot the system.

This example gives the simplest configuration to begin using SNMPv3 but doesn't make use of the full capabilities of the VACM in defining groups and views for fine-grained access control. The factory default */etc/snmpd.conf* file contains commented blocks of lines that can be uncommented to give you a basic configuration that uses the User-based Security Model (USM) described in RFC-2274 and the View-based Access Control Model (VACM) described in RFC-2275. The comments included in the file should help you in modifying it for your specific requirements.

Disable or Restrict Access

To disable SNMP, see ***Chapter 5 - Security, Disable SNMP, SSH and HTTPS***. To restrict access to specific hosts see ***Chapter 5 - Security, Restrict Access - Telnet, SSH and SNMP***.

This page intentionally left blank.

Chapter *Five*

Security

Your FDC3300e (FDC) incorporates several important security features to prevent unauthorized tampering with its operation. Many of these are standard multiple-user access control features of the underlying Linux operating system which controls the FDC. Others are provided by the additional protocol servers selected for inclusion in your FDC, and the way that they are configured.

Secure user authentication and session privacy while performing routine monitoring and maintenance tasks are provided by the OpenSSH implementations of the "secure shell" daemon, **`sshd`** and its companion "secure copy" utility, **`scp`**. The default Hiawatha implementation is for HTTP/HTTPS (HTTP encrypted via TLS), but it can be configured for HTTPS only. The NET-SNMP implementation of the Simple Network Management Protocol (SNMP) daemon, **`snmpd`** conforms to the latest Internet standard, known as SNMPv3, which also supports secure user authentication and session privacy. In addition, the Network Time Protocol daemon, **`ntpd`** supports client-server authentication security measures to deter spoofing of NTP clients by rogue NTP servers. This chapter describes these security measures and gives the advanced network administrator information that will allow custom configuration to fit specific security needs.

IMPORTANT

SSH, Telnet, SNMP and HTTPS are all enabled with default passwords. To ensure security, change the passwords or disable the protocols. To change the passwords for SSH, Telnet and HTTPS use the **`passwd`** command. To change the passwords/community strings for SNMP see ***Chapter 4 - SNMP***.

By default all hosts are allowed access via SSH, Telnet, SNMP and HTTPS. To restrict access to specific hosts, see ***Restrict Access - Telnet, SSH and SNMP*** below. To restrict access via HTTPS, see ***Chapter 6 - HTTP/HTTPS Interface, Restrict Access***. To restrict NTP query access see ***Chapter 7 - Network Time Protocol, Restrict Query Access.***

To completely disable any or all of these protocols see ***Disable Protocols*** below.

Linux Operating System

The Linux operating system versions are shown in ***Appendix E - Specifications***. Linux supports a complete set of security provisions:

- System passwords are kept in an encrypted file, */etc/shadow* which is not accessible by users other than *root*.

- Direct *root* logins are only permitted on the local RS-232 console or via SSH.

- The secure copy utility, **`scp`**, eliminates the need to use the insecure FTP protocol for transferring program updates to the FDC.

- Access via HTTPS may be restricted or completely disabled. See ***Disable SNMP, SSH and HTTPS*** in this chapter or ***Chapter 6 - HTTP/HTTPS Interface, Restrict Access***.

- SNMP access for system monitoring only, is configurable to provide the security of the latest version 3 Internet standard which supports both view-based access control and user-based security using modern encryption techniques. Previous versions v1 and v2c supported access control essentially via passwords transmitted over the network in plain text. Refer to ***Chapter 4 - SNMP*** and ***Restrict Access - Telnet, SSH and SNMP*** (below) for details. SNMP may also be completely disabled. See ***Disable SNMP, SSH and HTTPS*** below.

- Individual host access to protocol server daemons **`in.telnetd, snmpd`** or **`sshd`** are controlled by directives contained in the files */etc/hosts.allow* and */etc/hosts.deny*, which are configured using the interactive script **`accessconfig.`** See ***Restrict Access - Telnet, SSH and SNMP*** below.

- Insecure protocols like Time, Daytime and Telnet may be completely disabled by configuration of the **`inetd`** super-server daemon using the interactive script **`inetdconfig`**. See ***Disable Telnet, Time and Daytime*** below.

Restrict Access

The following paragraphs describe how to restrict SNMP, SSH, and Telnet to specific hosts. For instructions on how to restrict HTTPS and NTP access see ***Chapter 6 - HTTP/HTTPS Interface, Restrict Access*** and ***Chapter 7 - NTP, Restrict Query Access***.

Restrict Access - Telnet, SSH and SNMP

By default, the FDC is configured to allow access by all users via Telnet, SSH and SNMP. To ensure security and to protect against denial-of-service attacks, you should restrict access by using the **`accessconfig`** command.

`accessconfig` modifies two files, */etc/hosts.allow* and */etc/hosts/deny*, which are used by **`tcpd`** and the standalone daemons, **`snmpd`** and **`sshd`**, to determine whether or not to grant access to a requesting host. These two files may contain configuration information for a number of protocol servers, but in the FDC only access control to the protocol server daemons **`in.telnetd, sshd`** and **`snmpd`** is configured.

As shipped from the factory, these two files are empty. When you run **accessconfig**, these lines are added to the */etc/hosts.deny* file:

```
in.telnetd:  ALL
sshd:  ALL
snmpd:  ALL
```

This tells **tcpd** to deny access to **in.telnetd, sshd** and **snmpd** to all hosts not listed in the */etc/hosts.allow* file. The **snmpd** and **sshd** daemons also parse this file directly prior to granting access to a requesting host.

Next you will be prompted to enter a list of hosts that will be granted access to **in.telnetd, sshd** and **snmpd**. These appear in the */etc/hosts.allow* as lines like this:

```
in.telnetd:  192.168.1.2, 192.168.1.3
sshd:  192.168.1.2, 192.168.1.3
snmpd:  192.168.1.2, 192.168.1.3
```

This simple shell script handles the needs of most users, however the syntax of these two files supports elaborate configuration possibilities which are beyond the capabilites of this simple shell script. Advanced users who need these capabilities will need to edit these two files directly and then copy them to the */boot/etc* directory. (See ***Appendix C - Helpful Linux Information, Text Editors***.) Be careful to maintain the proper ownership and access permissions by using **cp -p** when copying the files.

Disable Protocols

See below for instructions on how to completely disable the following protocols: Telnet, Time, Daytime, SSH, SNMP, and HTTPS. The Network Time Protocol (NTP) cannot be disabled.

Disable Telnet, Time and Daytime

To disable Telnet, Time and Daytime use the **inetdconfig** command to start an interactive script that will ask you which protocols to disable. Then it will modify the */etc/inetd.conf* file, which is read by the super-server daemon, **inetd**. Requests from remote hosts for protocols not configured in */etc/inetd.conf* will be refused. Currently, three servers are configurable via **inetdconfig**: Time and Daytime (whose protocol servers are contained within the **inetd** daemon itself), and **in.telnetd**. Any one or all of these may be enabled or disabled for start-up.

Disable SNMP, SSH and HTTPS

To disable SNMP, SSH or HTTPS, you only have to modify the file mode of the scripts that control their execution. These are located in the */etc/rc.d* directory.To disable any of these daemons, issue one or more of these commands:

```
chmod -x /etc/rc.d/rc.snmpd
chmod -x /etc/rc.d/rc.sshd
chmod -x /etc/rc.d/rc.hiawatha
```

After issuing these commands, you must copy the modified file(s) to the non-volatile FLASH area using one or more of these commands:

```
cp -p /etc/rc.d/rc.snmpd /boot/etc/rc.d
cp -p /etc/rc.d/rc.sshd /boot/etc/rc.d
cp -p /etc/rc.d/rc.hiawatha /boot/etc/rc.d
```

Re-boot the FDC when done for the changes to take effect.

IMPORTANT

After modifying ***/etc/rc.d/rc.snmpd, rc.sshd or rc.hiawatha***, you must copy them to the ***/boot/etc/rc.d*** directory and reboot the system. It is very important to use the **`-p`** when performing the copy. During the boot process, the files contained in the ***/boot/etc/rc.d*** directory are copied to the working ***/etc/rc.d*** directory on the system RAM disk. In this way the factory defaults are overwritten.

Re-Enable SNMP, SSH and HTTPS

If you have disabled SNMP, SSH or HTTPS, and you want to re-enable it, all you need to do is remove the *rc* file from the */boot/etc/rc.d* directory using one or more of these commands:

```
rm /boot/etc/rc.d/rc.snmpd
rm /boot/etc/rc.d/rc.sshd
rm /boot/etc/rc.d/rc.hiawatha
```

Re-boot the FDC when done for the changes to take effect.

Is the Protocol Disabled?

Telnet, TIME and DAYTIME: To determine if one of these protocols is disabled, use the **`inetdconfig`** command.

SNMP, SSH and HTTPS: To determine if one of these protocols is disabled, issue the following command:

```
ls -l /boot/etc/rc.d
```

If you see one of the following files listed, and there is NOT an '*' after the file name, then the corresponding protocol is disabled:

```
-rw-r--r-- 1 root root 1144 Feb 19 01:52 rc.hiawatha
-rw-r--r-- 1 root root 1168 Oct 26 2012  rc.snmpd
-rw-r--r-- 1 root root 2684 Feb 18 02:16 rc.sshd
```

If **`rc.hiawatha`**, **`rc.snmp`**, or **`rc.ssh`** is not listed, or it is listed and there is an '*' after the file name, then the protocol is enabled. Here is an example:

```
-rwxr-xr-x 1 root root 1168 Oct 26 2012  rc.snmpd*
```

OpenSSH

The secure shell protocol server running in the FDC is based on the portable OpenSSH for Linux. As such it supports both SSH1 and SSH2 protocol versions. By default, only SSH2 is enabled in the FDC due to security issues with SSH1. For more information about OpenSSH, and to obtain client software, refer to the OpenSSH website:

http://www.openssh.com.

An excellent book which describes operation and configuration of the various SSH implementations, including OpenSSH is:

SSH, The Secure Shell, Barrett & Silverman, O'Reilley & Associates, 2001.

NOTE: To disable the SSH protocol see ***Disable SNMP, SSH and HTTPS*** above. To restrict access see ***Restrict Access - Telnet, SSH and SNMP*** above.

Configure Keys

On initial boot-up from out-of-the-box, the SSH start-up script, */etc/rc.d/rc.sshd*, will detect that no keys are present in the */etc/ssh* directory. It will call **`ssh-keygen`** to generate a set of host keys and then it will copy them to the */boot/etc/ssh* directory. These will be copied to */etc/ssh* during each boot up. A complete set of security keys for both SSH1 and SSH2 versions of the protocol are generated. RSA keys are supported by both versions, and DSA keys are supported when using the SSH2 version. Should you need to replace your keys at any time, you can just remove the keys from the */boot/etc/ssh* directory and then reboot the FDC. A new set of host keys will automatically be generated.

To configure root logins to your FDC via passwordless, public key authentication, you must generate a public/private pair of SSH2 keys using your own ssh key generating utility, or you can use the **`ssh-keygen`** that is resident on the FDC file system. You must then append the public key to the */boot/root/.ssh/authorized_keys2* file in the non-volatile FLASH area on your FDC. At boot time, the FDC will copy these to the actual working */root/.ssh* directory of the system ramdisk. To use this capability, the corresponding private key must reside in the */root/.ssh* directory of your remote computer as *id_rsa* or *id_dsa*. If you are unfamilar with this process, refer to the man page for the **`ssh-keygen`** utility for details (issue **`man ssh-keygen`** at the prompt). (Be careful to maintain the proper ownership and access permissions of the private key by using **`cp -p`** when copying the file. It MUST be readable only by *root*.)

Advanced users wishing to modify the overall configuration of the **`sshd`** daemon should edit the */etc/ssh/sshd_config* file and then copy it to the */boot/etc/ssh* directory of the FDC. Be careful to maintain the proper ownership and access permissions by using **`cp -p`** when copying the file. At boot time, it will be copied to the */etc/ssh* directory of the system ramdisk, thereby replacing the factory default configuration file.

Network Security Vulnerabilities

EndRun addresses major network security vulnerabilities that may affect FDC at the top of this web-page:

http://www.endruntechnologies.com/fsb.htm

This paper describes best practices to secure your time server and mitigate many network security vulnerabilities:

http://www.endruntechnologies.com/pdf/AppNoteSecurity.pdf

Chapter *Six*

Hyper Text Transport Protocol (HTTP/HTTPS)

This chapter briefly describes the web interface that resides on the FDC3300e (FDC). This interface is a fast and easy-to-use graphical interface that is compatible with your standard web browser. Simply point your browser to the IP address of the FDC and log in securely with HTTPS. Security-conscious customers may disable this interface entirely (see Chapter 5 for instructions).

NOTE

When the FDC is shipped from the factory, both HTTP and HTTPS are enabled. For security reasons, we recommend that you configure for HTTPS only. See ***Configure HTTPS only for IPv4*** and ***Configure HTTPS only for IPv6*** later in this chapter. We also recommend that you restrict access to specific IP addresses. See ***Security, Restrict Access*** later in this chapter.

The HTTPS implementation uses HTTP encrypted via Transport Layer Security (TLS). HTTPS enhances security because it encrypts and decrypts the requested and returned pages from the server, including any passwords which are transmitted. The HTTPS implementation is built from the standard Hiawatha distribution:

https://www.hiawatha-webserver.org

It uses HTTPS (HTTP via TLS) with MbedTLS (formerly known as PolarSSL). For more information about this protocol, refer to:

https://tls.mbed.org

See later in this chapter for information on changing the default HTTP/HTTPS configuration and TLS certificate and key. To disable the HTTP/HTTPS protocol, see ***Chapter 5 - Security, Disable SNMP, SSH and HTTPS***.

Interface Description

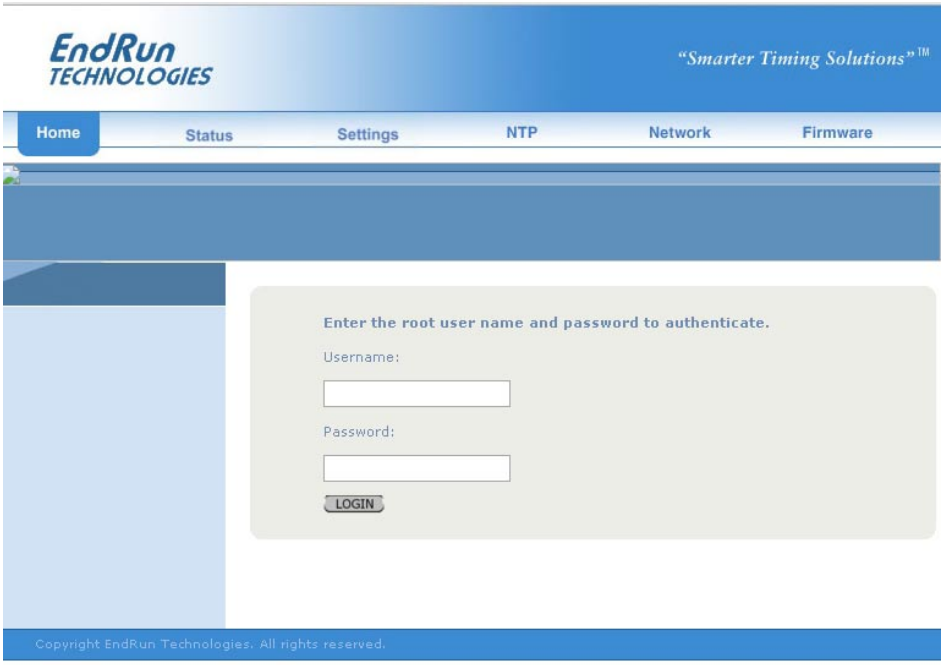
For security reasons the web pages on the FDC show status and configuration information only. You cannot change any operational settings. To make changes to the FDC you will need to use the command line interface via either a network or serial port.

To get started with the web interface simply point your browser to the IP address of the FDC and log in. By default, IPv4 will accept a request for HTTP or HTTPS. The server needs additional configuration for HTTPS only and IPv6. Following are examples for IPv4 and IPv6:

IPv4: 192.168.1.1
IPv6: [fe80:0:0:0:20e:f3ff:fe01:1f] Do not forget the brackets [].

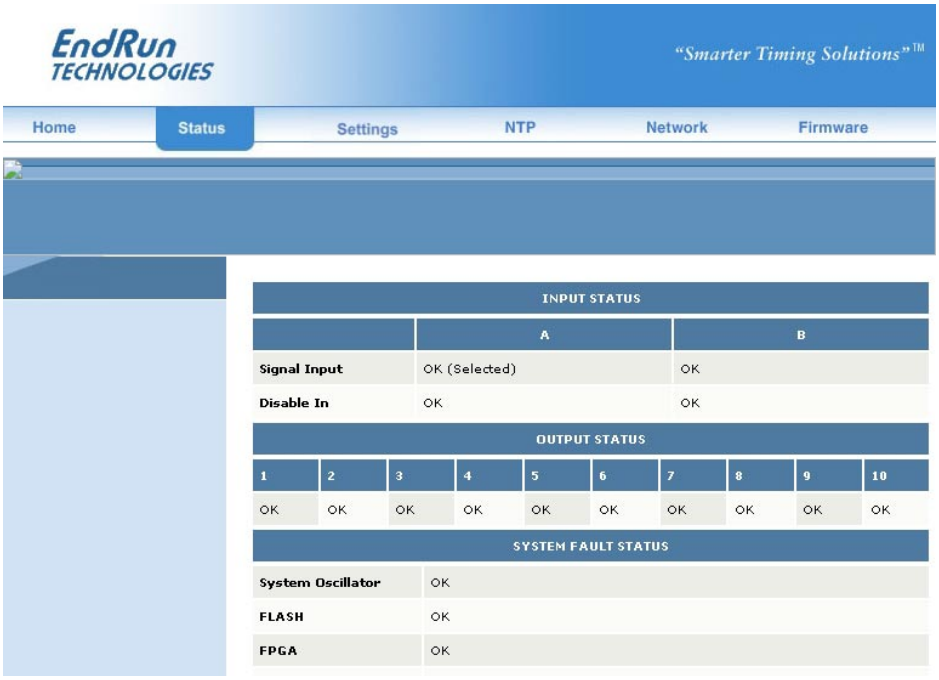
With HTTPS, a warning dialog page will be presented for the certificate. Acknowledge the dialog page and the server will continue to load, protected by TLS. The browser should change from http: to https:, indicating that the page is protected by TLS. To maximize security you should replace the TLS Certificate. See ***Security, Configure Certificate and Key*** later in this chapter for details.

Below is a picture of the login page:



Navigation

The main menu tabs across the top of each webpage allow you to navigate through the status information. These tabs are: ome, Status, Settings, NTP, Network and Firmware.



Configure HTTPS

HTTP/HTTPS use files for the default configuration located in */etc/hiawatha*. Of these, you will typically only need to modify *hiawatha.conf*. Advanced users who need to modify the default configuration will need to edit the file and copy it to the */boot/etc/hiawatha* directory. Do not attempt to change the directives unless you have a real need to do so. (See ***Appendix C - Helpful Linux Information, Text Editors***.)

To configure HTTPS (HTTP encrypted via TLS), you will need to modify *hiawatha.conf*. When configured, a HTTP request will be redirected to HTTPS. You must edit the */etc/hiawatha/hiawatha.conf* file and configure as shown below.

Configure HTTPS only for IPv4

You must edit the */etc/hiawatha/hiawatha.conf* file and set the Hostname in the Virtual Host to the IPv4 address of the server. After making and saving your changes, copy the edited file to the non-volatile FLASH area and reboot the unit:

```
cp -p /etc/hiawatha/hiawatha.conf /boot/etc/hiawatha
reboot
```

Configure HTTP for IPv6

You must edit the */etc/hiawatha/hiawatha.conf* file and edit the Binding for Port 80, add the Interface. After making and saving your changes, you must copy the edited file to the non-volatile FLASH area and reboot the unit:

```
cp -p /etc/hiawatha/hiawatha.conf /boot/etc/hiawatha
reboot
```

Configure HTTPS only for IPv6

You must edit the */etc/hiawatha/hiawatha.conf* file and:

1. Edit the Binding for Port 80, add the Interface.
2. Edit the Binding for Port 443, add the Interface.
3. Edit the Hostname in the Virtual Host to the IPv6 (global) address of the server.

After making and saving your changes, you must copy the edited file to the non-volatile FLASH area and reboot the unit:

```
cp -p /etc/hiawatha/hiawatha.conf /boot/etc/hiawatha
reboot
```

Security

Restricting access and configuring the certificate and key are described below. For information on disabling the HTTP/HTTPS protocol see ***Chapter 5 - Security, Disable SNMP, SSH and HTTPS***.

Restrict Access

To control access via HTTP/HTTPS, you must edit the */etc/hiawatha/hiawatha.conf* file and add the Access List for additional security. Define which IPs have access to the Virtual Host. '**`allow`**' gives access. '**`deny`**' denies access.

The default file contains these lines that must be edited:

```
#Access List allow 192.168.1.1, deny all
```

After making and saving your changes, you must copy the edited file to the non-volatile FLASH area and reboot the unit:

```
cp -p /etc/hiawatha/hiawatha.conf /boot/etc/hiawatha
reboot
```

Configure Certificate and Key

For TLS it is recommended, but not required, that new certificates and keys are generated and installed on the Hiawatha web server. The factory-configured, self-signed certificate is located in */etc/hiawatha/tls*. After creating new certificates, they will need to be saved in */boot/etc/hiawatha/tls/hiawatha.pem*. To generate a new certificate and key, issue these commands:

```
cd /boot/etc/hiawatha/tls
openssl req -new > cert.csr
openssl rsa -in privkey.pem -out key.pem
openssl x509 -in cert.csr -out cert.pem -req -signkey key.pem -days 1001
cat key.pem cert.csr > hiawatha.pem
```

The file will be created in the */boot/etc/hiawatha/tls* directory. You must reboot the FDC for changes to take effect.

NOTE

If you request your X.509 SSL/TLS certificate from a Certificate-Signing Authority (CA) you must have the following order in the ***hiwatha.pem*** file as shown below:

-----BEGIN RSA PRIVATE KEY-------
[webserver private key]
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
[webserver private key]
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
[optional intermediate CA certificate]
-----END CERTIFICATE-----

This page intentionally left blank.

Chapter *Seven*

Network Time Protocol (NTP)

This chapter describes how to configure the FDC3300e (FDC) as an NTP Stratum 2 Client/Server. NTP is primarily used to synchronize the FDC's system clock for accurate time stamping of log files. Setup is simple using the **ntpconfig** *script to configure the ip address of a Stratum 1 NTP server on your network and authentication keys (if used). For advanced users, the FDC can be used as a Stratum 2 NTP server with the full suite of functions provided in the NTP distribution.*

If you are new to NTP, a simple introduction is available here:

http://www.endruntechnologies.com/pdf/NTP-Intro.pdf.

For advanced usage, it would be beneficial to read the on-line documents, especially the Distribution Notes, FAQ and Configuration subject matter at:

http://www.ntp.org

Configuring FDC as a Stratum 2 Client/Server

The **ntpconfig** command allows you to set up NTP operation on your FDC. Below is an example illustrating the general operation of this interactive script:

```
FDC3300e (root@FDC3300e:~)-> ntpconfig

*******************************************************************************
*********************Network Time Protocol Configuration***********************
*******************************************************************************
*                                                                             *
*   This script will allow you to configure the ntp.conf and ntp.keys files   *
*   that control FDC3300e NTP daemon operation.                               *
*                                                                             *
*   You will be able to create new MD5 authentication keys which are stored   *
*   in the ntp.keys file.                                                     *
*                                                                             *
*   You will be able to update the authentication related commands in the     *
*   ntp.conf file.                                                            *
*                                                                             *
*   You will be able to configure the "broadcast/multicast" mode of           *
*   operation, with or without authentication.                                *
*                                                                             *
```

```
*   You will be able to add servers to be polled to ntp.conf, with or        *
*   without authentication.                                                  *
*                                                                            *
*   The changes you make now will not take effect until you re-boot the      *
*   FDC3300e.  If you make a mistake, just re-run ntpconfig prior to         *
*   re-booting.                                                              *
*                                                                            *
*   You will now be prompted for the necessary set up parameters.            *
*                                                                            *
******************************************************************************
******************************************************************************

---MD5 Keyfile Configuration

Would you like to create a new ntp.keys file? ([y]es, [n]o) n

---NTP Authentication Configuration

Do you want authentication enabled using some or all of the keys in
the ntp.keys file? ([y]es, [n]o) n

---NTP Broadcast/Multicast Configuration

Would you like to enable unauthenticated broadcast/multicast client
operation? ([y]es, [n]o) n

---Polled NTP Server Configuration

Would you like to configure NTP servers to be polled? ([y]es, [n]o) n


******************************************************************************
******************************************************************************
*                                                                            *
*      The FDC3300e Network Time Protocol configuration has been updated.    *
*                                                                            *
*              Please re-boot now for the changes to take effect.            *
*                                                                            *
******************************************************************************
******************************************************************************
******************************************************************************
```

Answering “y” to any of the questions above would have continued a sequence of questions and answers to configure a specific aspect of the NTP daemon operation. On completion, the resulting *ntp.conf* file is copied to */boot/etc* where it will be non-volatile across reboots of the Linux subsystem.

For basic setup to synchronize the FDC system clock for time stamping log files, select “yes” to the Polled NTP Server Configuration step and input the ip address of an NTP server(s) that is reachable from the FDC. Select “no” for all other steps unless authentication keys are used.

Knowledgeable NTP users may find it simpler to directly edit the *ntp.keys* and *ntp.conf* files. If you do so, then all that remains to be done is to copy both of them to */boot/etc* so that they will be non-volatile across reboots of the Linux subsystem.

Security

The Network Time Protocol (NTP) cannot be disabled. To restrict access see below.

Restrict Query Access - NTP

By factory default, remote control and query of the NTP daemon **ntpd** is disabled. Query-only operation is supported only from processes running on the FDC itself, i.e. from the *localhost*. This restricts access to **ntpd** from remote hosts using either of the two NTP companion utilities **ntpq** and **ntpdc**.

Control via these two utilities is disabled in the */etc/ntp.conf* file in two ways. First, MD5 authentication keys are not defined for control operation via a *requestkey* or *controlkey* declaration. Second, this default address restriction line is present in the file:

```
restrict default nomodify noquery nopeer
restrict 127.0.0.1 nomodify
restrict 0::1 nomodify
```

The first line eliminates control and query access from ALL hosts. The second and third lines disable the localhost from making any modifications to the **ntpd** daemon, but query access is not affected by this restriction. These lines must not be removed, as they are necessary for various monitoring processes running on the FDC to function properly.

Knowledgable NTP users who would like to customize the security aspects of the configuration of the NTP daemon in the FDC should edit the */etc/ntp.conf* file directly and then copy it to the */boot/etc* directory. Be sure to retain the ownership and permissions of the original file by using **cp -p** when performing the copy.

CAUTION

If you are planning to make changes to the ***/etc/ntp.conf*** file, you must NOT restrict query access from the local host to the NTP daemon. Various system monitoring processes running on the system require this access.

An example follows which shows how to allow query access from a specific remote host with IP address 192.168.1.10 while also allowing processes running on the FDC to have query access as well:

```
restrict default noquery nomodify nopeer
restrict 127.0.0.1 nomodify
restrict 0::1 nomodify
restrict 192.168.1.10 nomodify
```

This page intentionally left blank.

Chapter *Eight*

IPv6 Information

The FDC3300e (FDC) supports IPv6 out-of-the-box with a modern version 4.9.75 Linux kernel. During network configuration, you have the option to disable IPv6. The IPv6 addressing scheme may see expanding deployment in the future due to the fact that there are no longer any IPV4 addresses to be allocated in many regions of the world.

IPv6 Capabilities

The presence of an IPv6-capable kernel will automatically enable most of the IPv6 capabilities. By default, autoconfiguration of the Ethernet interface via IPv6 Router Advertisements is enabled. To disable acceptance of Router Advertisements, or to configure a static IPv6 address and default IPv6 gateway, and to configure IPv6 domain name servers, you must run the interactive **`netconfig`** script. This will allow you to configure your Ethernet interface for both IPv4 and IPv6 operation. You can also configure the hostname and domainname for the unit.

OpenSSH

By default, **`sshd`** is factory-configured to listen on both IPv4 and IPv6 addresses. It may be forced to listen on either IPv4 only, or IPv6 only by editing the */etc/ssh/sshd_config* file and modifying the **`AddressFamily`** directive, and then copying it to */boot/etc/ssh*. Refer to the *sshd_config* man page for detailed information (**`man sshd_config`**).

Hiawatha HTTPS

By default, **`hiawatha`** is factory-configured to listen on IPv4 only. It may be configured to listen on IPv6 only. Refer to ***Chapter 6 - HTTP/HTTPS Interface, Configure HTTPS for IPv6***.

Net-SNMP

By default, **`snmpd`** is factory-configured to listen on both IPv4 and IPv6 addresses. This may be changed by editing */etc/rc.d/rc.snmpd* and modifying the agent address argument passed to **`snmpd`** at start-up, and then copying it to */boot/etc/rc.d*.

NTP

By default, **`ntpd`** is factory-configured to listen on both IPv4 and IPv6 addresses. This may be changed by editing */etc/ntp.conf* and adding the desired **`interface`** directives to achieve the desired behavior, and then copying it to */boot/etc*. For example, adding this line:

```
interface ignore ipv6
```

will cause ntpd to not bind to any IPv6 addresses. Refer to the NTP documentation for details on the **interface** directive.

IPv4-Only Protocols

There are several protocols running on FDC which are not IPv6 capable: **telnet** (client and server), **ftp** and **dhcpcd**. Due to their intrinsic insecurity, **telnet** and **ftp** are rapidly being deprecated, and probably have little business running over an IPv6 network. The address autoconfiguration capabilities of IPv6 along with the Neighbor Discovery Protocol (NDP) make the DHCP protocol less important in IPv6 networks.

Chapter *Nine*

System Log Files

The FDC3300e (FDC) supports logging of Distribution Subsystem status and the Network Time Protocol (NTP) status. Details are below.

Distribution Subsystem Status

A history of Distribution Subsystem status information is kept in:

/logs/status.log

Information is logged every 30 seconds and 30 to 40 days of data is kept. The format of each data string is shown here:

YYYY MMM DD HH:MM:SS 111111 2222222222 3333 DD PP S IN 1234567890

Where:

YYYY MMM DDD is the UTC year, month and day-of-month.

hh:mm:ss	are the UTC hours, minutes and seconds.
111111	are Group 1 alarms (see **`alarmstat`** in ***Chapter 3***.)
2222222222	are Group 2 alarms (see **`alarmstat`** in ***Chapter 3***.)
3333	are Group 3 alarms (see **`alarmstat`** in ***Chapter 3***.)
DD	is the status of Disable A and Disable B (see **`disablestat`** in ***Chapter 3***.)
PP	is the power supply status (see **`pwrstat`** in ***Chapter 3***.)
S	is the selected input A or B
IN	is the signal input status (see **`siginstat`** in ***Chapter 3***.)
1234567890	is the signal output status (see **`sigoutstat`** in ***Chapter 3***.)

Here is an example:

```
2018 Sep 05 15:21:00 000001 0000000000 0000 00 10 A 11 1111111111
```

NTP Status

NTP is used to synchronize the Linux Subsystem clock for accurate time stamping of log files. To enable NTP see ***Chapter 7 - Network Time Protocol***. NTP status information is logged once per minute and a 30 to 40-day history is kept in:

/logs/ntpstat.log

The format of the logged data shows the status of the NTP daemon:

YYYY MMM DD HH:MM:SS IPADDR S +S.sssssssss +FF.ffffff LI

Where:

YYYY MMM DDD is the UTC year, month and day-of-month.

hh:mm:ss	are the UTC hours, minutes and seconds.
IPADDR	is the reference ID of the NTP server currently being used for synchronization.
S	is the stratum level of the NTP daemon (the reference server stratum + 1).
+S.sssssssss	is the offset in seconds between the NTP system clock and the reference server.
+FF.ffffff	is the frequency offset of the Linux Subsystem oscillator in PPM.
LI	are the leap second indicator bits as received from the reference server.

Here is an example:

```
2018 Sep 05 15:24:30 192.168.1.128  2 +0.000025649 +26.421101 00
```

Appendix *A*

LED Indicators

This appendix describes the distribution chassis LED indicators and what they mean.

Power LEDs

COLOR	MEANING
Green	Power supply is good.
Red	One of the power supplies has failed. This condition will only exist in a unit with redundant power supplies.
Off	The redundant power supply is not installed.

Input LEDs

The operation of these LEDs depends on the **`switchmode`** and **`disablemode`** settings (see ***Chapter 3 - Console Port Control and Status***). The switchmode command determines whether a particular Signal Input should be present or not. For example, if switchmode=a then Signal Input B need not be present.

COLOR	MEANING
Green	The signal input is selected as the current input.
Red	The signal input should be present but it is not. See **`switchmode`** to determine whether a signal input should be present or not.
Flashing Red	The signal input should be present but its corresponding disable input has been enabled (see **`disablemode`**) and is asserted.
Yellow	The signal input is present but is not selected as the current input.
Flashing Yellow	The signal input is present, but should not be (see **`switchmode`**) and its corresponding disable input has been enabled (see **`disablemode`**) and is asserted. This usually occurs only when the user has configured the system incorrectly. For example, a secondary input has been connected and its disable input has been enabled but **`switchmode`** is configured as **`switchmode=a`** or **`switchmode=b`**.
Off	The signal input is not present and should not be present per **`switchmode`**.

Output LEDs

COLOR	MEANING
Green	The output is present.
Red	The output is absent, shorted, or the output driver has failed.

Alarm LED

COLOR	MEANING
Green	No alarm condition exists.
Red	An alarm condition exists. See commands **`faultstat`** and **`alarmstat`** for more information.

Appendix *B*

Upgrading the Firmware

Periodically, EndRun Technologies will make bug fixes and enhancements to our products available for download from our website. All such downloads are freely available to our customers, without charge. After you have downloaded the appropriate binary image file from the EndRun Technologies website, you are ready to perform the upgrade to your distribution chassis.

NOTE

In order to upgrade via the console port (network or serial) you will need to first download the appropriate firmware image from our website. The FDC firmware consists of three different binary files. You may only need one or two of them. The revision history on our website will tell you which files need to be upgraded. The firmware image files are for the Linux RFS (root file system), the Linux Kernel and the Distribution Subsystem. Here is the website link:

https://www.endruntechnologies.com/support/software-upgrades/distribution

Performing the Linux RFS Upgrade

NOTE TO LINUX GEEKS

There are two disk partitions which hold the compressed Linux root file system images. These partitions are raw blocks, have no file system and may not be mounted. They are accessed through low-level device drivers. To protect the factory root file system from accidental erasure or over-writing, the upgrade utilities you will be using will only access the upgrade root file system partiton. When performing an upgrade, you will be erasing and then copying the new image to this device.

First you need to download the Linux RFS firmware from the EndRun website to a place on your network which is accessible to the FDC. The link to the FDC upgrade page is shown in the note above.

CAUTION

Some browsers will automatically unzip the file when downloading from the website. Please make sure that the downloaded file size matches what the website says it should be. Upgrading the partition with a too-large file size will cause problems.

Transfer File to FDC

You may transfer the file to your FDC using either **ftp** or **scp**. If you are using **ftp**, transfer the previously downloaded file using *binary* transfer mode from the remote host to this specific file on your FDC: */home/rootfs.gz*. The root file system image will be named with the software part number and version like: *6010-0083-000_3.00.gz*. When following the instructions below, substitute the name of the actual root file system image that you are installing for *6010-0083-000_3.00.gz*. Issue these commands from the console of your FDC:

```
ftp remote_host                          {perform ftp login on remote host}
bin                                      {set transfer mode to binary}
get 6010-0083-000_3.00.gz /home/rootfs.gz {transfer the file}
quit                                     {close the ftp session after transfer }
```

If you are using **scp**, you may open a command window on the remote computer and securely transfer the root file system image from the remote computer to your FDC. A command like this should be used:

```
scp –p 6010-0083-000_3.00.gz root@host.your.domain:/home/rootfs.gz
```

Now issue the following command to the FDC console to initiate the upload:

```
upgraderootfs
```

Next, update the default file system partition by issuing this command to your FDC console:

```
updaterootflag 1
```

You should see this line displayed:

```
Default Root File System now set to: UPGRADE
```

Finally, reboot the system by issuing this command at the shell prompt:

```
reboot
```

Wait about 90 seconds for the system to shutdown and reboot. Then log in to the FDC using **telnet** or **ssh**. If all has gone well, you should be able to log in the usual way. After you have entered your password, the system version message will be displayed. You should notice that it now indicates the software version and date of the upgrade that you previously downloaded. You can also check this at any time by issuing

```
sysversion
```

which will cause the system version message to be re-displayed.

You can also check to see which root file system image the system is currently booted under by issuing this command at the shell prompt:

```
sysrootfs
```

Which should cause this to be printed to the console:

```
BOOTED ROOT FILE SYSTEM IMAGE = 1 (Upgrade)
```

If so, and your unit seems to be operating normally, you have successfully completed the root file system upgrade. If your unit does not boot up successfully, and you are not able to **telnet** or **ssh** into the system after 90 seconds, then there has been some kind of problem with the root file system upgrade. It is possible that the file downloaded was corrupt or that you forgot to set your FTP download file mode to binary when downloading the file--either from the EndRun Technologies website or when transferring it to the FDC.

Recovering from a Failed RFS Upgrade

To restore your FDC to a bootable state using the factory root file system, you must use the serial I/O port and reboot the FDC by cycling the power. Refer to ***Chapter 2 – Basic Installation, Connect the Serial I/O Port and Test the Serial I/O Port*** for setup details. When you have connected your terminal to the serial I/O port, apply power to the FDC.

Pay close attention to the terminal window while the unit is rebooting. After the Linux bootloader displays the message

```
Current default Kernel/Root File System: FACTORY/UPGRADE

You can:

  Override the default kernel and/or root file system boot configuration.
  and/or
  Reset the root password to the factory password.

By typing these commands:

bootcfg=*#     (* = 0 or 1 to select FACTORY or UPGRADE kernel,
                # = 0 or 1 to select FACTORY or UPGRADE root file system)

pwrst=xxxxxxxx (xxxxxxxx is reset code obtained from EndRun Tech Support)

Begin typing within 5 seconds to extend the boot timeout.
```

you must begin typing "**bootcfg=00**" within five seconds to let the bootloader know that you are going to override the default root file system. Five seconds after entering the last character, the boot process will continue. Watch the rest of the boot process to make sure that you have successfully recovered. If the system boots normally, then you should resolve the problems with the previous root file system upgrade and re-perform it.

Performing the Linux Kernel Upgrade

First you need to download the Linux Kernel firmware from the EndRun website to a place on your network which is accessible to the FDC. The link to the FDC upgrade page is shown above.

Transfer File to FDC

You may transfer the file to your FDC using either **ftp** or **scp**. If you are using **ftp**, transfer the previously downloaded file using *binary* transfer mode from the remote host to this specific file on your FDC: */tmp/kernel.gz*. The kernel image will be named with a software part number like: *6010-0082-000_2.00.gz*. When following the instructions below, substitute the name of the actual kernel image that you are installing for *6010-0082-000_2.00.gz*. Issue these commands from the console of your FDC:

```
ftp remote_host                          {perform ftp login on remote host}
bin                                      {set transfer mode to binary}
get 6010-0082-000_2.00.gz /tmp/kernel.gz  {transfer the file}
quit                                     {close the ftp session after transfer }
```

If you are using **scp**, you may open a command window on the remote computer and securely transfer the kernel image from the remote computer to your FDC. A command like this should be used:

```
scp -p 6010-0082-000_2.00.gz root@host.your.domain:/tmp/kernel.gz
```

Now issue the following command to the FDC console to initiate the upload:

```
upgradekernel
```

Next, update the default file system partition by issuing this command to your FDC console:

```
updatekernelflag 1
```

You should see this line displayed:

```
Default Kernel now set to: UPGRADE
```

Finally, reboot the system by issuing this command at the shell prompt:

```
reboot
```

Wait about 90 seconds for the system to shutdown and reboot. Then log in to the FDC using **telnet** or **ssh**. If all has gone well, you should be able to log in the usual way. You can check the running kernel version at any time by issuing

```
kernelversion
```

which will cause the kernel version message to be displayed.

You can also check to see which kernel image the system is currently booted under by issuing this command at the shell prompt:

```
syskernel
```

Which should cause this to be printed to the console:

```
BOOTED KERNEL IMAGE = 1 (Upgrade)
```

If so, and your unit seems to be operating normally, you have successfully completed the kernel upgrade. If your unit does not boot up successfully, and you are not able to **telnet** or **ssh** into the system after 90 seconds, then there has been some kind of problem with the kernel upgrade. It is possible that the file downloaded was corrupt or that you forgot to set your **ftp** download file mode to binary when downloading the file--either from the EndRun Technologies website or when transferring it to the FDC.

Recovering from a Failed Kernel Upgrade

To restore your FDC to a bootable state using the factory kernel, you must use the serial I/O port and reboot the FDC by cycling the power. Refer to ***Chapter 2 – Basic Installation, Connect the Serial I/O Port and Test the Serial I/O Port*** for setup details. When you have connected your terminal to the serial I/O port, apply power to the FDC.

Pay close attention to the terminal window while the unit is rebooting. After the Linux bootloader displays the message:

```
Current default Kernel/Root File System: UPGRADE/UPGRADE

You can:

  Override the default kernel and/or root file system boot configuration,
  and/or
  Reset the root password to the factory password.

By typing these commands:

bootcfg=*#     (* = 0 or 1 to select FACTORY or UPGRADE kernel,
                # = 0 or 1 to select FACTORY or UPGRADE root file system)

pwrst=xxxxxxxx (xxxxxxxx is reset code obtained from EndRun Tech Support)

Begin typing within 5 seconds to extend the boot timeout.
```

you must begin typing "**bootcfg=01**" within five seconds to let the bootloader know that you are going to override the default kernel. Five seconds after entering the last character, the boot process will continue. Watch the rest of the boot process to make sure that you have successfully recovered. If the system boots normally, then you should resolve the problems with the previous kernel upgrade and re-perform it.

Performing the Distribution Subsystem Upgrade

This section has instructions for upgrading the Distribution Subsystem.

First you need to download the Distribution Subsystem firmware from the EndRun website to a place on your network which is accessible to the FDC. The link to the FDC upgrade page is shown above.

You may transfer the file to your FDC using either **ftp** or **scp**. If you are using **ftp** to perform the upgrade, transfer the previously downloaded file using *binary* transfer mode from the remote host to this specific file on your FDC: */tmp/subsys.bin*. The Distribution Subsystem image will be named with the software part number and version like: *6010-0077-000_3.01.bin*. When following the instructions below, substitute the name of the actual Distribution Subsystem image that you are installing for *6010-0077-000_3.01.bin*. You will be transferring the file to a temporary file, */tmp/subsys.bin* on your FDC.

```
ftp remote_host                {perform ftp login on remote host}
bin                            {set transfer mode to binary}
get 6010-0077-000_3.01.bin /tmp/subsys.bin       {transfer the file}
quit                           {close the ftp session after the transfer }
```

If you are using SSH to perform the Distribution Subsystem upgrade, you may open another command window on the remote computer and securely transfer the Distribution Subsystem image to */tmp/subsys.bin* using **scp** from the remote computer. A command like this could be used:

```
scp -p 6010-0077-000_3.01.bin root@host.your.domain:/tmp/subsys.bin
```

Now perform the following two commands to initiate the upload.

```
kill `pidof g_keeper`          {the back quote` is on the tilde ~ key}
upgradesubsys
```

The first command kills a system process that would interfere with the firmware upload to the Distribution Subsystem. The **upgradesubsys** command performs the actual file transfer to the Distribution Subsystem. You will see a file transfer progress message while it is performing the transfer. After it completes, wait about 10 seconds and issue these commands to restart the **g_keeper** system process and to check the Distribution Subsystem version:

```
g_keeper
dcversion
```

You should see a message like this:

```
F/W 6010-0077-000 Ver 3.01 - FPGA 6020-0006-000 Ver 04 - AUG 12 15:30:58 2018
```

The firmware version should match that of the binary file that you uploaded.

Problems with the Distribution Subsystem Upgrade

Should you have difficulties with the upgrade due to a corrupt file, power failure during upload, or other accident, do not be alarmed. Even though you may have lost the existing application program, the Distribution Subsystem bootloader program will remain intact. Correct any problem with the binary file and retry the upload procedure. If you are still unable to successfully perform the Distribution Subsystem upgrade, you should contact Customer Support at EndRun Technologies.

This page intentionally left blank.

Appendix C

Helpful Linux Information

You do not need knowledge of Linux commands in order to operate your FDC3300e (FDC). All commands necessary for proper operation are described in ***Chapter 3 - Console Port Control and Status****. However, the FDC does support a subset of the standard Linux commands and utilities and it uses the* **bash** *shell, which is the Linux standard, full-featured shell. Very brief descriptions of some of the most useful Linux information is described in this appendix.*

Linux Users

FDC is shipped from the factory with two users enabled. The first is the "root" user with password "endrun_1". The root user has access to everything on the system, including the ability to perform system setup procedures.

The other user is "sysuser" with password "Praecis". When logged in as sysuser you may check status information and view log files but you will not be able to modify any system settings or view secure files.

For security reasons, we recommend you change the default passwords using the Linux **passwd** command (see ***Change Password*** below).

Linux Commands

Detailed Information Is Available

A very brief description of the most helpful Linux commands and utilities is listed in this appendix. On Linux systems, the system commands are located in the directories with "bin" in their name, e.g. */usr/bin* or */sbin*. You can list the contents of those directories using the **ls** command to see what is installed on your FDC. Then you can find out about those commands using the **man** command, which stands for "manual". For example, to read details on the **ps** command type this:

```
man ps
```

A very detailed description, called a "man page", of the **ps** command will be shown. To navigate in the document, press `d' to scroll down, `b' to scroll up, and `q' to quit and return to the command prompt.

To search the database of man pages, use either **apropos** or **whatis**. **apropos** will do partial word searches, while **whatis** will only find matching whole words. For example to find all man pages dealing with ntp:

```
apropos ntp
```

The relevant available man pages are shown:

```
ntp []                (1)  - keygen - Create a NTP host key
ntpd []               (1)  - NTP daemon program
ntpdc []              (1)  - vendor-specific NTP query program
ntpq []               (1)  - standard NTP query program
ntpsnmpd []           (1)  - NTP SNMP MIB agent
sntp []               (1)  - standard SNTP program
```

Now you can issue issue **man** commands on each of these man pages to find what you are looking for.

Change Password

This command is used to change the password for the user that you are logged in as. It affects the serial port, SSH, Telnet and HTTPS.

```
passwd
```

List Active Processes

This command displays all active processes running in the system.

```
ps -e
```

NTP Monitoring and Troubleshooting

The following command displays which NTP clients are reaching the NTP daemon running on the FDC. It will not try to look up host names.

```
ntpq -n -c mrulist
```

A useful command for querying NTP status is the following.

```
ntpq -peers
```

To query a remote time server (if the remote timeserver will accept the query) type:

```
ntpq -peers <hostname>
```

A table of information will be displayed. For details on what each of the table columns means type:

```
man ntpq
```

To see what version of the NTP daemon, ntpd, is operating type:

```
ntpd -version
```

Text Editors

There are two text editors resident on the FDC file system: **edit** and **joe**. Each of these may be useful when needing to edit system configuration files or to view and search within system log files.

joe is the recommended editor for all purpose use in configuring and monitoring the FDC. It is a full-featured editor with syntax highlighting and is also based on the Wordstar commands. It is user friendly with easy to find help for its key commands, and complete man page documentation. It is started by simply issuing the command **joe [file-to-edit]**, optionally with a file name to edit. It is the modern replacement for **edit** (see below).

edit is a very simple editor with Wordstar key commands that was originally developed for extremely memory-limited environments, such as floppy boot disks and embedded Linux appliances. When EndRun Technologies' first generation Linux-based embedded network time servers were introduced, they fell into this category and the **edit** text editor was appropriate. Now it is included on the FDC file system for legacy reasons, since it has been the default editor for all first and second generation EndRun Technologies products. A man page for **edit** is resident on the system. When it is first started, and you did not give it a file name to edit on the command line, it shows a start-up screen with its command syntax, But once you have opened a file to edit, online help is not available. It is started by issuing the command **edit [file-to-edit]**, optionally with a file name to edit.

Change Log-In Banners

There are three different log-in banners in the FDC - the serial port banner, the Telnet banner, and the SSH banner. You must be logged in as the "root" user in order to edit the *rc.local* file and change the log-in banners. Perform the following:

```
edit /etc/rc.d/rc.local
```

Change the banners as appropriate. After saving the file, copy it to */boot/etc* like this:

```
cp -p /etc/rc.d/rc.local /boot/etc/rc.d
```

Then reboot for your changes to take effect.

Query and Change Ethernet Port

ethtool is a Linux utility that allows you to query or change the settings for Port 0 (**eth0**). For example, to view current settings for Port 0 issue the following command:

```
ethtool eth0
```

Here is an example of one way to set the speed on Port 0 to 100Base-T:

```
ethtool -s eth0 speed 100 duplex full autoneg off
```

The command above will immediately change the port speed to 100Base-T, but it will revert to its factory (10/100Base-T) at a system reset. If you want to retain the setting after a system reset, then you need to edit the *rc.M* configuration file. Follow this sequence:

1. Edit */etc/rc.d/rc.M* using one of the editors on the previous page.
   Insert the desired **ethtool** line (see example above) after the Gatekeeper Daemon is started. Exit and save the *rc.M* file.

2. Now you need to copy the *rc.M* file into a location that will ensure your changes persist through a system reset. Copy */etc/rc.d/rc.M* to */boot/etc/rc.d* as shown:

```
cp /etc/rc.d/rc.M /boot/etc/rc.d
```

For more details on **ethtool** and how to use it type:

```
man ethtool
```

Redirect Syslog Files to Remote Host

You can redirect syslog files to a remote host (syslog server) by adding the standard Linux redirect commands to the FDC's *syslog.conf* file. Follow this sequence:

1. Edit */etc/syslog.conf* using one of the editors on the previous page. Insert this line:

```
*.* @remote_host
```

   Substitute the actual name or IP address of your remote syslog server for "remote_host". The most common log file to be directed to the Syslog Server is the *messages.log* file which contains authenticated user login activity. If you would like to only redirect this log info to the remote host, insert this line instead of the one above:

```
messages.log @remote_host
```

   Exit and save the *syslog.conf* file.

2. Now you need to copy the *syslog.conf* file into a location that will ensure your changes persist through a system reset. Copy */etc/syslog.conf* to */boot/etc/syslog.conf* as shown:

```
cp /etc/syslog.conf /boot/etc/syslog.conf
```

Appendix *D*

Third-Party Software

The FDC3300e is running several different software products created and/or maintained by open source projects. Open source software comes with its own license. These are printed out for your information below.

The license for the GNU software project requires that we provide you with a copy of all source code covered under the GNU Public License (GPL) at your request. Please contact us with your request and we will mail it to you on a CD. We will charge you a fee for our incurred expenses as allowed for in the license.

GNU General Public License

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989,1991 Free Software Foundation, Inc.,
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in

reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

NTP Software License

Information about the NTP Project, led by Dr. David Mills, can be found at www.ntp.org. The distribution and usage of the NTP software is allowed, as long as the following copyright notice is included in our documentation:

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

Appendix *E*

Specifications

Reference Inputs (A or B):

Frequency Range: 10 kHz to 10 MHz.
Impedance: 50Ω, SWR < 1.1.
Amplitude: +13 dBm Full Performance, +3 dBm minimum, +19 dBm maximum.
A Input to B Input Isolation: < -90 dB, full frequency range.
Output to Input (Reverse) Isolation: < -110 dB, full frequency range.
Protection: Protected to 24V peak-to-peak.
Connectors: Rear-panel female BNCs labeled “Signal In”.

Distribution Outputs (1 through 10):

Impedance: 50Ω, SWR: < 1.3.
Unity Gain: 0 dB, +/-1 dB.
Harmonics: < -45 dBc
Spurious: < -90 dBc.
Adjacent Output to Output Isolation: > 70 dB.
Protection: Outputs may be shorted to ground with no damage.
Connectors: Rear-panel female BNCs numbered 1 through 10.

External Alarm Input/Disable Inputs (A or B):

Normal State: TTL low.
Alarm State: TTL high or high Z (internal 10kΩ pull-up).
Connectors: Rear-panel female BNCs labeled “Disable In”.

Alarm Output:

Open-collector, 40 VDC Max, 100 mA Max Saturation Current.
High Impedance when any fault condition exists.
Connector: Rear-panel female BNC labeled “Alarm Out”.

Front-Panel System Status Indicators:

Signal Input LEDs: Red/Green/Yellow LEDs indicate signal presence, selection status of each Signal Input and, if configured, Disable Input (external alarm input) status.
Signal Output LEDs: Red/Green/Yellow LEDs indicate signal presence status on each output.
Power LEDs: Red/Green LEDs indicate power supply status of each power input.
Alarm LED: Red/Green/Yellow LED indicates a serious fault condition.

Network I/O:

One rear-panel RJ-45 jack.
10/100 Base-T Ethernet.

Supported IPv4 Protocols:

SNTP, NTP v2, v3, v4, SHA/MD5 authentication, broadcast/multicast and autokey
SSH client and server with "secure copy" utility, SCP
SNMP v1, v2c, v3 with Enterprise MIB
TELNET client/server
FTP client
DHCP client
SYSLOG
HTTP/HTTPS via TLS

Supported IPv6 Protocols:

SNTP, NTP v2, v3, v4, SHA/MD5 authentication, broadcast/multicast and autokey
SSH client and server with "secure copy" utility, SCP
SNMP v1, v2c, v3 with Enterprise MIB
HTTP/HTTPS via TLS
Note: See ***Chapter 8 - IPv6 Information*** for more details.

Serial Port I/O:

Signal: I/O port at RS-232 levels for secure, local terminal access.
Parameters: 19200 baud, 8 data bits, no parity, 1 stop bit.
Connector: Rear-panel DB-9M connector labeled "RS-232".
To connect to a computer, a null-modem adapter must be used. The serial cable provided with the shipment is wired as a null-modem. Pinout for the RS-232 console port is shown below.
Note: For operational details see ***Chapter 3 - Console Port Control and Status***.

DB9M Pin	Signal Name
1	Not Connected
2	Receive Data (RX)
3	Transmit Data (TX)
4	Not Connected
5	Ground
6	Not Connected
7	Not Connected
8	Not Connected
9	Not Connected

AC Power:

90-264 VAC, 47-63 Hz, .5 A Max. @ 120 VAC, .25 A Max. @ 240 VAC.
110-370 VDC, 0.5A Max @ 120 VDC.
3-Pin IEC 320 on rear panel, 2 meter line cord is included.

DC Power (Option):

12 VDC (10-20 VDC), 5A maximum.
24 VDC (19-36 VDC), 2.5A maximum.
48 VDC (38-72 VDC), 1.5A maximum.
125 VDC (70-160 VDC), 0.75A maximum.
3-position terminal block on rear panel: +DC IN, SAFETY GROUND, -DC IN.
(Floating power input: Either "+" or "-" can be connected to earth ground.)

Size:

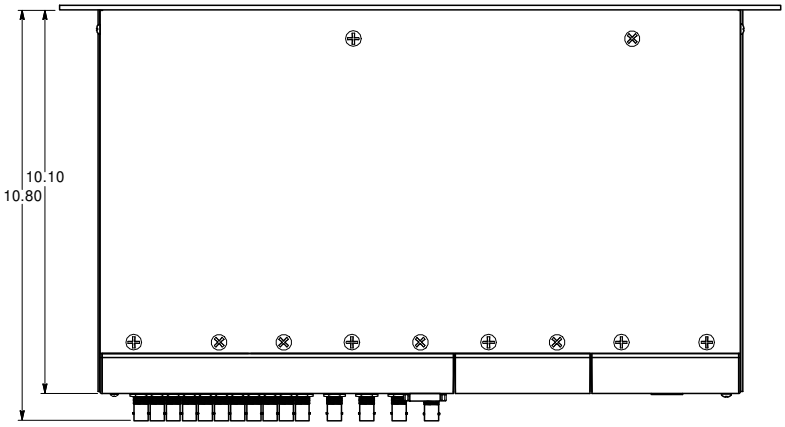
Chassis: 1.75"H x 17.0"W x 10.75"D.
Weight: < 5 lb. (2.70 kg.).

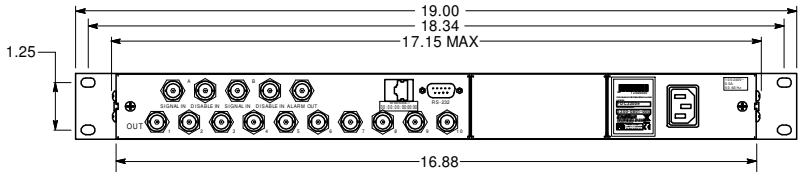
Environmental:

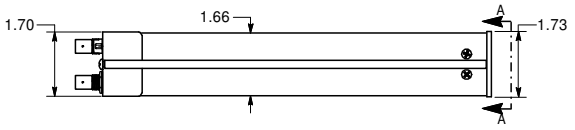
Operating Temperature:	0° to +50° C	
Storage Temperature:	-40° to +85° C	
Antenna Operating Temperature:	-40° to +85° C	
Operating Humidity:	5% to 90%, RH, non-condensing	
Storage Humidity:	5% to 95%, RH, non-condensing	
Maximum Operating Altitude:	AC:	13,125 ft. / 4000 meters
	12/24 VDC:	13,125 ft. / 4000 meters
	48 VDC (<61 VDC Max.):	13,125 ft. / 4000 meters
	48 VDC (>60 VDC Max):	6,562 ft. / 2000 meters
	125 VDC:	6,562 ft. / 2000 meters

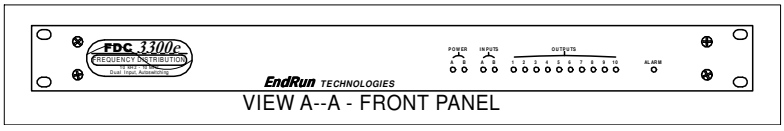
Compliance:

CE, FCC, RoHS, WEEE.









VIEW A--A - FRONT PANEL

FDC3300E DIMENSIONS - AC POWER

CE

EndRun TECHNOLOGIES

DECLARATION OF CONFORMITY

(According to ISO/IEC 17050-1 and ISO/IEC 17050-2)

Manufacturer's Name: **EndRun Technologies, LLC**

Manufacturer's Address: **2270 Northpoint Parkway**
Santa Rosa, California 95407, U.S.A.
+1-707-573-8633

DECLARES, THAT THE PRODUCT

Product Name: ***Pulse, Frequency, and Timecode Distribution Chassis***

Model Number: ***3300-XXXX-XXX, 3301-XXXX-XXX, 3302-XXXX-XXX, 3303-XXXX-XXX***
(FDC3300, FDC3300e, PDC3301, PDC3301e, FDC3302, FDC3302e, TDC3303, TDC3303e)
Where x represents any alphanumeric character, blank, slash or dash.

CONFORMS TO THE FOLLOWING EUROPEAN DIRECTIVES

Low Voltage Directive: 2014 /35 / EU
EMC Directive: 2014 /30 / EU
RoHS Directive: 2011 / 65 / EU
WEEE Directive: 2012 / 19 / EU

Supplementary Information:

Safety : ***EN 60950-1:2006/A11:2009/A1:2010/A12:2011/A2:2013***
EMC: ***EN 55032:2012 w/AC1***
EN 50024:2010 w/A1
VCCI-CISPR 32 2016 Class A
ICES-0003 Class A Issue 6
FCC Part 15 Subpart B Class A

I, the undersigned, hereby declare that the equipment specified above conforms to the above Directives and Standards.

Place: Santa Rosa CA USA Signature:

Date: 2/19/2019 Full Name: Bruce M. Penrod

Position: V.P. Product Development

This page intentionally left blank.

Special Modifications

Changes for Customer Requirements

From time to time EndRun Technologies will customize the standard FDC3300e Frequency Distribution Chassis for special customer requirements. If your unit has been modified then this section will describe what those changes are.

This section is blank.

This page intentionally left blank.

EndRun TECHNOLOGIES
"Smarter Timing Solutions"
2270 Northpoint Parkway
Santa Rosa, CA 95407
TEL 1-877-749-3878
FAX 707-573-8619
www.endruntechnologies.com