



CyberForce[®] System v2.0

USER GUIDE

CyberForce® System User Guide v2.0

CyberGlove Systems LLC

2355 Paragon Drive, Suite D

San Jose, CA 95131

Tel: (408) 451-9463

Fax: (408) 689-4362

www.cyberglovesystems.com

Table of Contents

OVERVIEW	5
System Components	5
System Component Diagrams	8
Technical Specifications	9
NETWORK SETUP	11
Configure the FCU for Your Network	11
HARDWARE SETUP	14
Install the Protective Shields	14
Attach the Tripod Base to the Armature	15
Make Connections Between Components	17
Turn Off Power Switches	18
Orient the FCU	20
Connect the CyberGlove to the FCU	21
Connect the CyberGrasp Actuator Unit to the FCU	21
Connect the CyberForce Armature to the FCU	22
Connect the CyberForce Armature to the Power Supply Unit	22
Connect the Power Supply Unit to the Force Control Unit	23
Connect the Safety System User Footswitch	
to the CyberForce Armature	23
Connect the FCU to the Network	23
Connect Power Cords to the FCU and Power Supply Unit	23
Connect a Monitor to the FCU (Optional)	23
Attach the CyberGrasp Exoskeleton to	
CyberForce Structure	24
SYSTEM SETUP	25
Home the Systems	25
FCU Boot-up Sequence	27
Wearing the CyberGrasp Exoskeleton	28
Establish the Device Configuration	31
Calibrate the CyberGrasp System	32
Become Familiar with the CyberForce Safety System	32
APPENDIX A	34
Controlling the FCU Over the Network	34
APPENDIX B	34
FCU Software Installation	34
Initializing the FCU for Software Installation	35
Installing/Updating the FCU Software Over the Network	35
APPENDIX C	36
Maintenance and Troubleshooting	36

Overview

Congratulations on purchasing your new CyberForce® haptic-feedback interface. With its intuitive “reach in and grab it” paradigm, this novel device provides a natural way to interface with complex 3D computer-generated worlds and to control end-effectors in telerobotic applications requiring a high level of dexterity. Possible applications include CAD, training and simulation, virtual reality, rapid prototyping, telerobotics, medical training, data visualization, education, and underwater exploration and salvage operations.

This manual describes how to set up and get your CyberForce unit operational. Refer to the CyberGlove® system user's manual for information on using the CyberGlove system and to the VirtualHand® SDK User's Guide and Programmer's Guide for additional software information. We strongly recommend that you read this entire manual before attempting to configure or operate your CyberForce system.



WARNING: *If equipment is used in a manner not specified in this manual or by CyberGlove Systems, the protection provided by the equipment may be impaired.*

System Components

The CyberForce system, as shipped, should consist of the following parts, packaged in five boxes:

- CyberForce Armature with appropriate mounting accessories
- FCU : Force Controller Unit (IV-FFCU-SA900)
- PSU : Power Supply Unit (IV-FPSU-SA900-120 or -230)
- CyberForce Data Cable (HAR908-LF)
- CyberForce Control Cable (HAR904-LF)
- CyberForce Motor Power Cable (HAR903-LF)

- CyberGrasp Exoskeleton with actuator box
- CyberGrasp Data Cable (HAR708-LF)

- CyberGlove System with 22 sensors
- User Guides: CyberForce, CyberGrasp, CyberGlove Systems
- Footpedal (CPED-D-STD)
- AC Power Cables, 2, region specific

The main system components are shown in Figure 1-1. A 22-sensor CyberGlove system is the core of the interface, and is used to measure the joint angles of the fingers. This information is used by the host to display a graphical hand on the screen or control a telerobotic manipulator. The CyberGrasp system is responsible for providing force feedback to the fingers. The CyberGrasp exoskeleton attaches to the back of the hand and guides force-applying tendons to the fingertips. The CyberForce system measures the position and orientation (6 degrees of freedom) of the hand and generates translational (3 degrees of freedom) force feedback. The Force Control Unit (FCU) is the interface between the devices worn by the user and the host computers, which communicate via Ethernet. The host computers need only communicate with the FCU, which in turn communicates with all other peripherals (CyberGlove, CyberGrasp, and CyberForce).

System Component Diagrams

Figure 1-1
Main System
Components

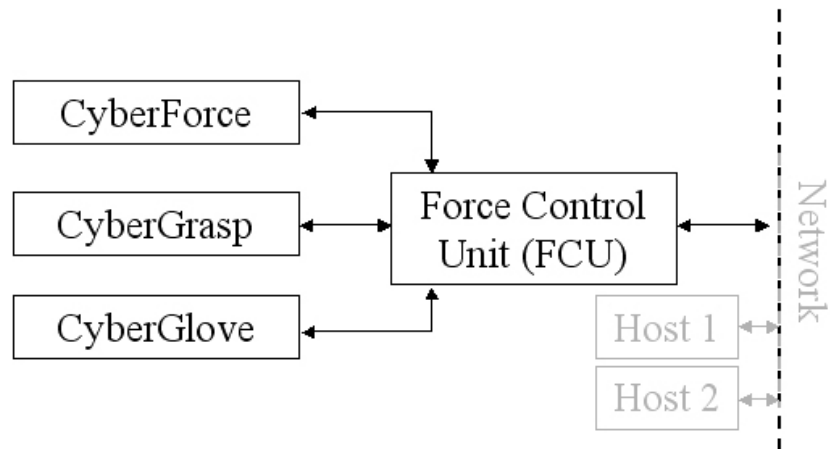


Figure 1-2
FCU Circuit
Diagram

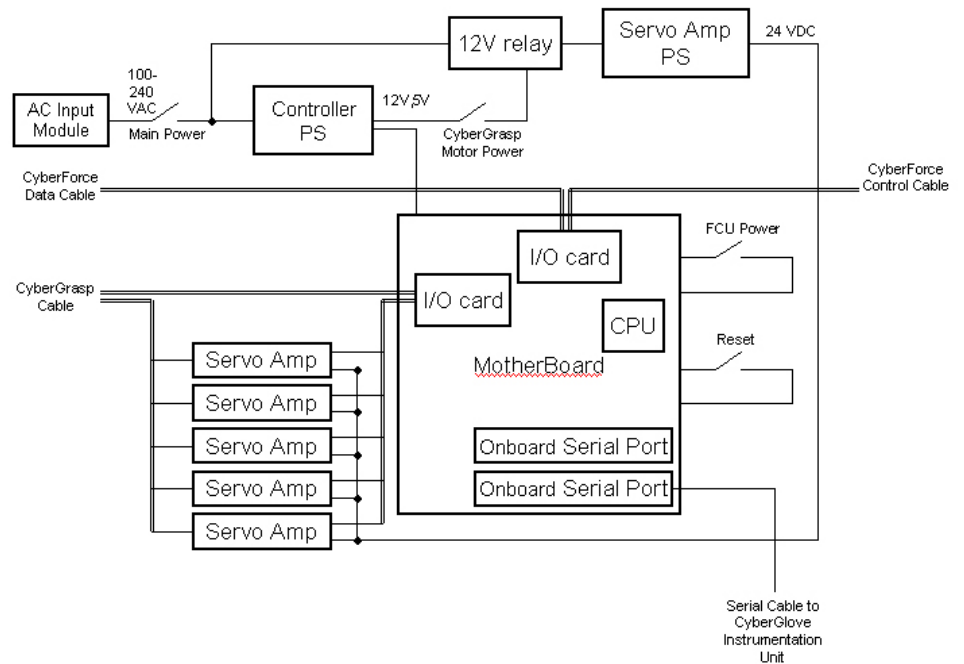


Figure 1-3
PSU Circuit
Diagram

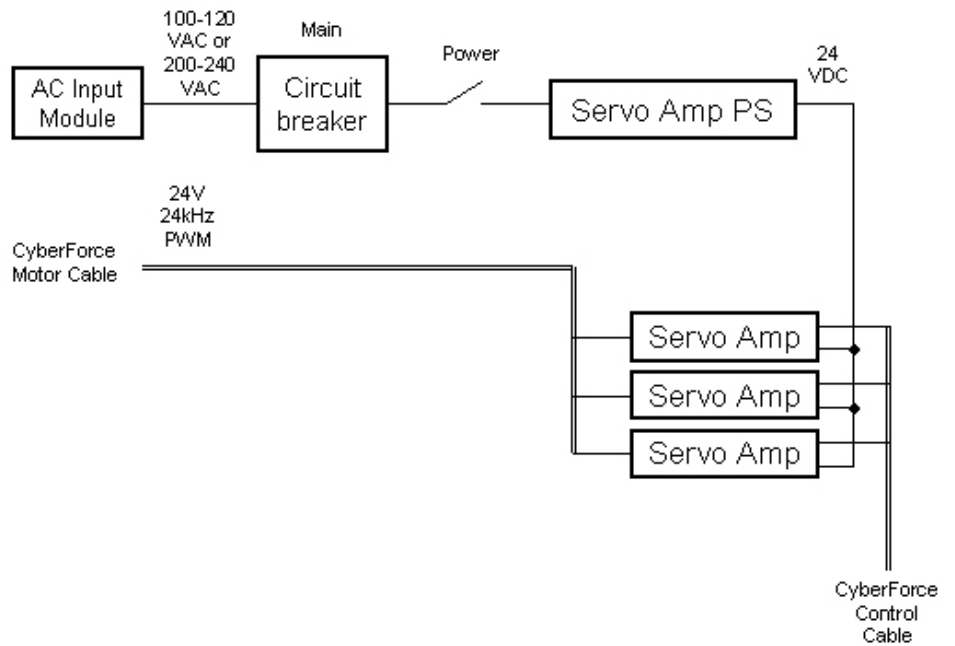
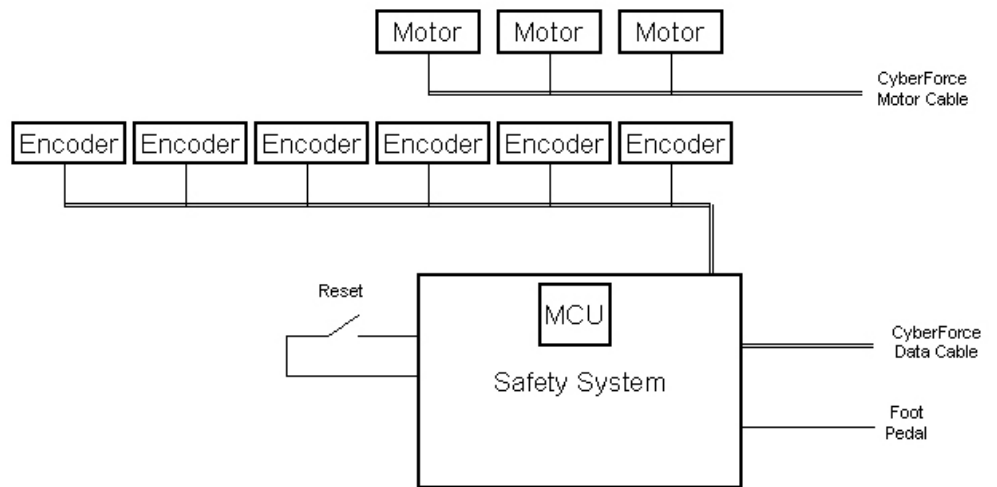


Figure 1-4
Armature
Circuit
Diagram



Technical Specifications

Performance^{1,2}	
Specification	Description
Force Limits at Hand Center	8.8 N at 14" radius from base 7.2 N at 26" radius from base
Positional Sensing Resolution	0.0024" at 14" radius from base 0.0029" at 26" radius from base
Orientation Resolution	0.09 degrees (in roll, pitch, yaw)

¹Based on a 12" x 12" workspace swept through 133° at a radius of 20.0".

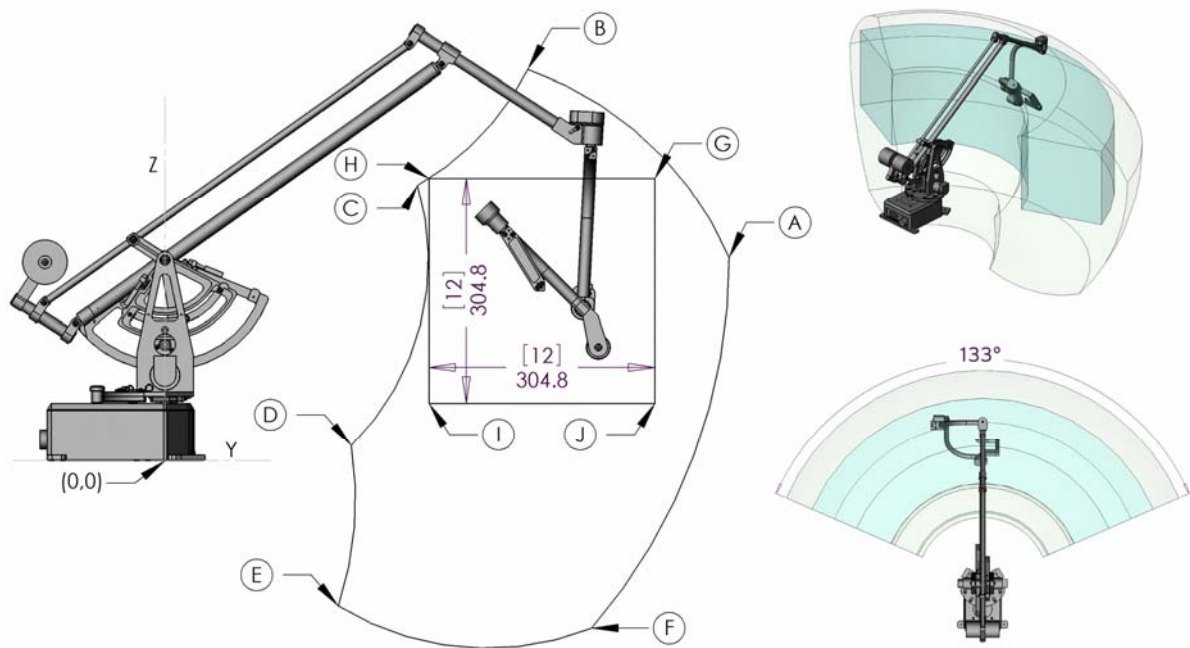
²Calculated based on the hardware specifications. Actual force and resolution will be less due to mechanical flexing of the system, friction, and transmission efficiencies.

Environment	
For indoor use only. Intended to be used in laboratory/office environment.	
Specification	Description
Temperature	+5 to +40 degrees C
Altitude	Up to 2000 m above sea level
Humidity	Max humidity 80% up to 31 degrees C, decreasing to 50% at 40 degrees C.

Electrical	
Specification	Description
Mains	FCU 100-240 VAC, 47-63 Hz PSU 100 to 240 VAC, 47-63 Hz. Mains supply voltage fluctuation not to exceed plus/minus 10%.
Overvoltage Category	II
Protective Earthing	Equipment is Class I Earthed equipment and must be connected to a properly grounded main.
Interface	Ethernet (standard STP Category 5 Ethernet cable required)

Mechanicals	
Specification	Description
Workspace ³	12" x 12" vertically oriented rectangle centered at 20" from vertical rotation axis of armature and swept through 133 degrees.
Weight	19 lbs (Armature) 44 lbs (FCU) 20 lbs (PSU)

Workspace Extents, mm [inches]



Points A through J refer to the Cartesian position in the YZ plane of the wrist gimbal rotational center. The origin of the YZ plane is defined as the intersection

³ Workspace as defined here is used for force, orientation, and position limit specifications. The CyberForce system is capable of operating in the larger workspace depicted in figure XX, however force and position specifications may be reduced when operating outside of the specification workspace.

of the base rotation axis and the plane formed by the base plate of the CyberForce armature.

Point	Y coordinate mm [inches]	Z coordinate mm [inches]
A	760 [29.9]	275 [10.8]
B	489 [19.3]	529 [20.8]
C	340 [13.4]	373 [14.7]
D	251 [9.9]	20 [0.8]
E	234 [9.2]	-196 [-7.7]
F	575 [22.6]	-226 [-8.9]
G	660 [25.9]	387 [15.24]
H	356 [14.0]	387 [15.25]
I	356 [14.0]	98 [3.86]
J	660 [25.9]	98 [3.86]

Total workspace volume for the CyberForce system: 0.3280 m³ [20015.5 in³]

Network Setup

Configure the FCU for your Network

Communication with the FCU is achieved via Ethernet over a network. The FCU must therefore be added to your network just like any other new computer. The system comes with a default IP address of 192.168.4.254. If this IP address is suitable for your network, the device can be powered up without modification. If this IP address is not suitable for your network, you must follow the procedure in this section. These configuration steps are only needed: 1) when first installing your FCU; 2) when changing your network configuration; or 3) when re-installing or updating the FCU internal software. If some of the network terminology used in the following sections is not familiar to you, please contact your system administrator.



WARNING: A Microsoft Windows (XP) PC with a 1.44 MB floppy drive is required for editing the FCU configuration floppy disk.

Four steps are required to configure the network settings for the FCU. First, you must physically connect the FCU to the network and power. Second, you must create an FCU initialization floppy disk. Third, you must write your network setting information onto the disk using the netcfg.exe utility. Fourth, you must initialize the FCU using the floppy disk.

1) Make physical connections for initializing the FCU.

To perform the initialization of the FCU, make minimal hardware connections to the Ethernet network and to FCU power, as described below. After completing the initialization, proceed with hardware setup before the final rebooting. Always be sure all devices are powered off before making or changing cable connections.

a) Connect the FCU to the Network

Using a standard STP Category 5 Ethernet cable, connect the FCU to your network hub. The Ethernet connector is located on the back panel of the FCU (see Figure 1-11). The FCU can also be connected directly to the host computer if a cross-over cable is used.

b) Connect Power Cords to the FCU and Power Supply Unit

Make sure the main power switch located on the back of the FCU is in the OFF position. Connect the AC power cord to the back of the FCU (Figure 1-11) and then to the mains. Turn the main power switch to ON position.

c) Power up the FCU

Depress the FCU Power switch on the front of the controller. Wait for it to boot up. When it is ready, it will emit three beeps. This will take approximately 20 to 30 seconds.

2) Create the FCU initialization floppy.

This process consists of transferring a disk image onto a floppy disk. The disk image is located in the FCU Installation/CyberForce/RevE directory of the VirtualHand SDK distribution directory.

- Load VirtualHand SDK onto a compatible Microsoft Windows computer
- Put a blank formatted floppy into the floppy drive
- Open a DOS shell, and change your directory to FCUInstallation/CyberForce/RevE inside the VirtualHand install directory. To open a DOS shell, click the Windows **Start** button on the bottom left corner of your screen. Go to the **Run** pull-out and Type Run to get an **MS-DOS Prompt**.

- Finally, type the line below and follow the instructions:

```
rawrite -f disc.raw -d a
```

The floppy drive will be active for approximately 30 - 45 seconds as it writes the disk.



WARNING: ONCE THE DISK IMAGE HAS BEEN COPIED TO THE FLOPPY DISK, REMOVE IT FROM YOUR DRIVE AND LABEL IT CAREFULLY. BOOTING YOUR COMPUTER WITH THAT FLOPPY DISK MAY RESULT IN UNRECOVERABLE DATA LOSS AS THE CYBERFORCE SOFTWARE REPLACES THE CONTENTS ON YOUR MAIN DISK!

3) Record your network configuration settings on the FCU initialization disk.

The network settings for the FCU are stored on the FCU Initialization Disk by running the netcfg.exe utility provided on the disk. The netcfg.exe utility runs in a Microsoft Windows XP environment.

Before running the utility, you will need to obtain the following information from your system administrator:

- **fcu name:** a name by which the FCU will be known within your network
- **network domain:** the name of your network domain (if any)
- **IP address:** an IP address that is assigned to the FCU within your network
- **network gateway:** an IP address that refers to the network gateway for the network segment in which the FCU will be connected
- **domain name server:** an IP address for the computer that serves the domain names for your network
- **netmask:** an IP mask that is used by the segment in which the FCU will be connected

On a computer running Microsoft Windows, open a DOS shell (**Start > Run**), then type **cmd** and insert the FCU initialization floppy into drive A. At the DOS shell prompt, type the following:

```
cd a:  
netcfg
```

The utility will prompt you with the configuration questions, and present a default answer (in brackets) for each question. You can either enter a new value, or press enter to accept the default answer. The FCU comes with its software pre-installed, so at the final question select "network configuration only." If you need to perform a full FCU software installation, refer to Chapter 2, "FCU Software Installation".

! **WARNING:** *ONCE THE FLOPPY DISK HAS BEEN WRITTEN, REMOVE IT FROM DRIVE AND LABEL IT CAREFULLY. BOOTING YOUR COMPUTER WITH THAT FLOPPY DISK MAY RESULT IN UNRECOVERABLE DATA LOSS AS THE CYBERFORCE SOFTWARE REPLACES THE CONTENTS ON YOUR MAIN DISK!*

4) Initialize the FCU.

Once you have provided all the network configuration information, the FCU must be initialized with the floppy. To do so, put the initialization floppy into the FCU floppy drive and then power it on or re-boot it if it is already on. The FCU initialization will start automatically. When the initialization is complete, the FCU will beep three times. Take the floppy disk out of the floppy drive.

Power the FCU down and complete the hardware setup as described in "Hardware Setup" below. Be sure all the devices are off while making the connections.

Hardware Setup

Install the Protective Shields

The CyberForce armature comes packaged with a two part protective enclosure for the cable drive cam mechanisms. The protective enclosure serves to protect the user from pinch points in the mechanism as well as protective the moving parts of the device from falling objects.

Assemble the two enclosure halves onto the armature using the four screws provided as shown in Figures 1-5 and 1-6.

**Figure
1-5**
Protective
shield
installation

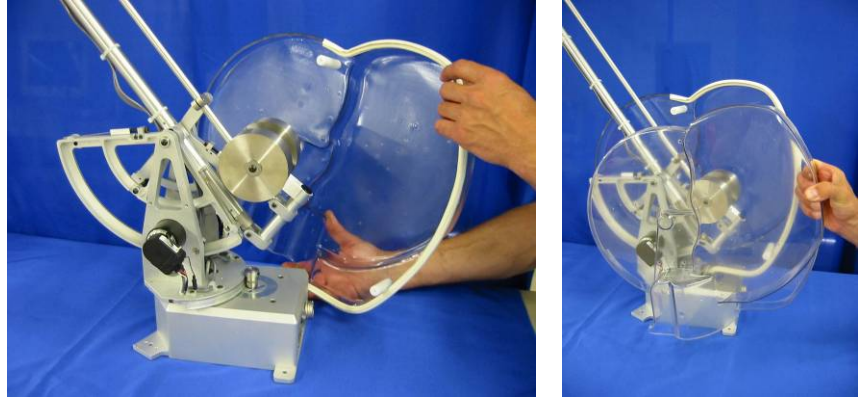
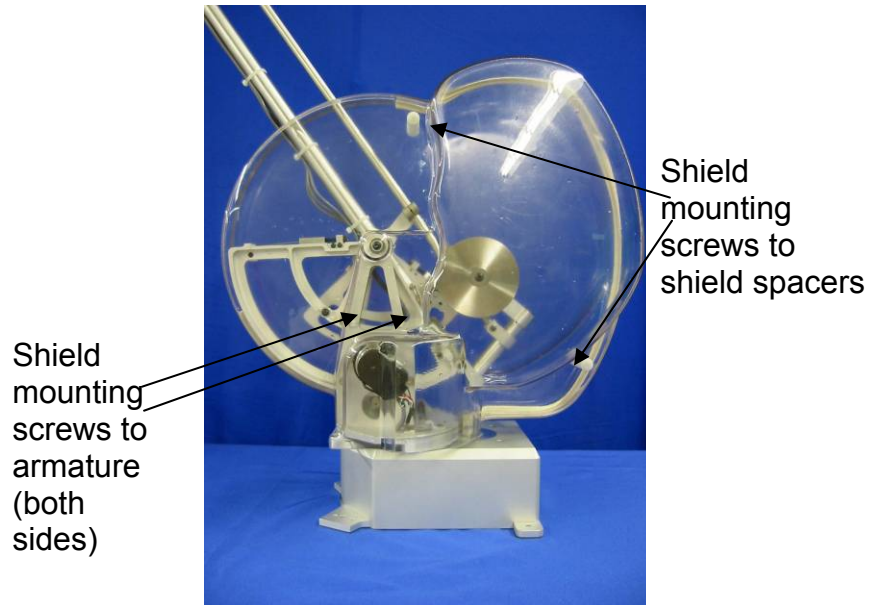


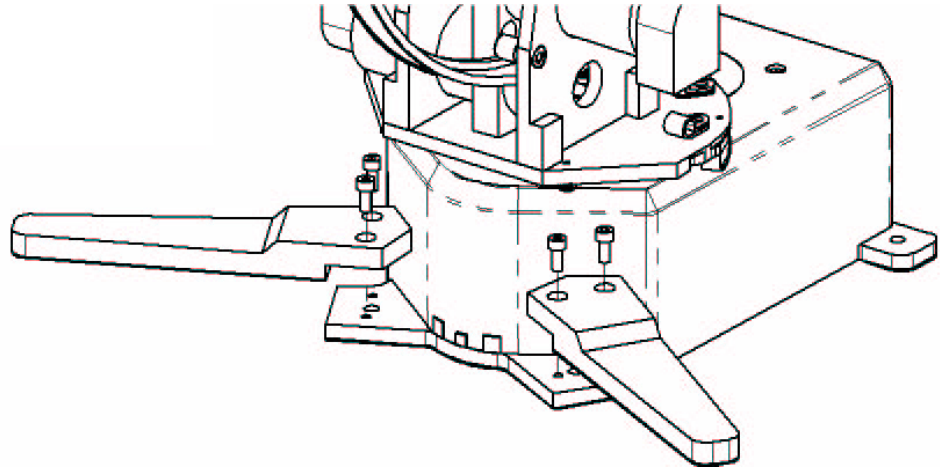
Figure 1-6
Protective
shield



Attach the Tripod Base to the Armature

The CyberForce armature comes packaged with a two piece base and mounting hardware (4 socket head screws) to secure them to the base of the armature. Attach the base feet to the armature prior to using the CyberForce system. The assembly is illustrated in Figure 1-7.

Figure 1-7
Attaching
tripod
base to
armature



The base is rubber lined on one side to ensure a high friction contact with the desktop or lab bench. For better performance, it is recommended that the armature be mounted without base feet to the desktop or lab bench using the provided C-clamps or bolted directly to the desktop or lab bench using four #12 screws. The mounting configuration is shown in Figure 1-8.

Figure 1-8a
Mounting
Hole
Pattern

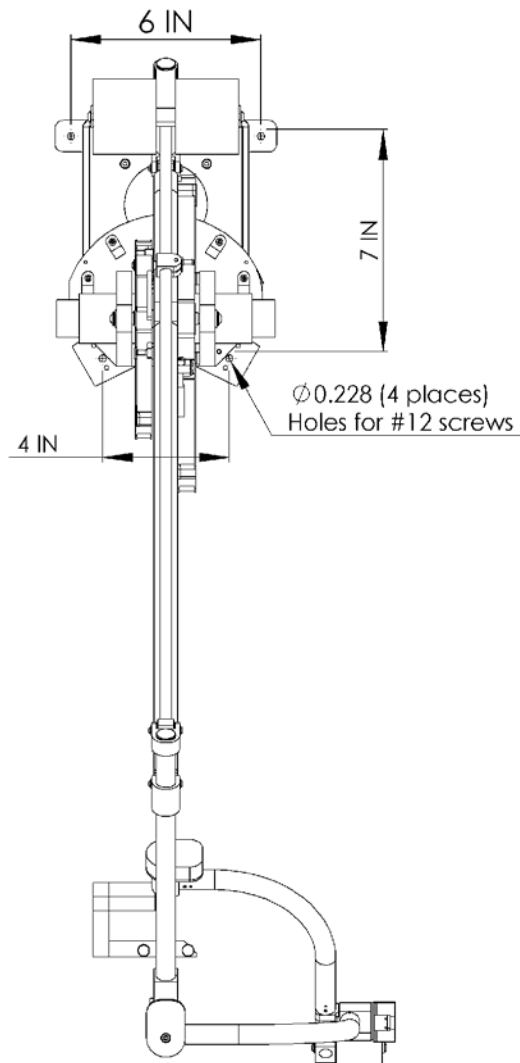
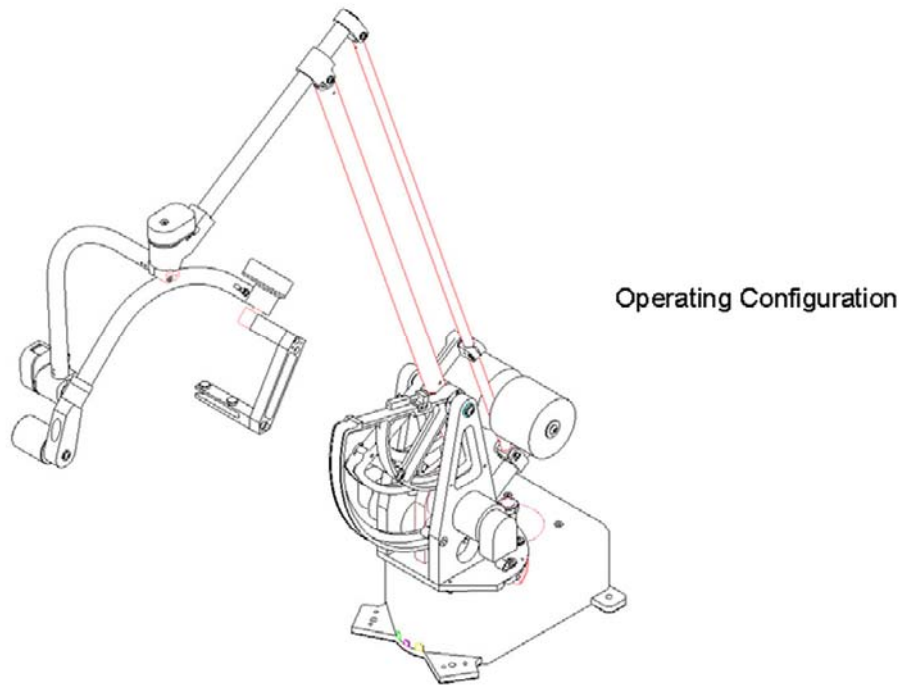


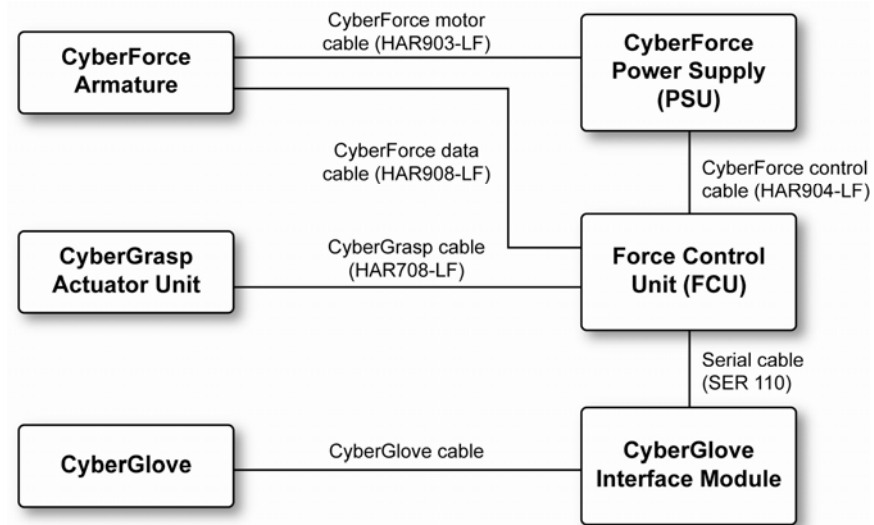
Figure 1-8b
Operating Configuration



Make Connections Between Components

! **WARNING:** Make sure the Force Control Unit (FCU) is powered-off to avoid damage when connecting the various components.

Figure 1-9
System
Connection
Details



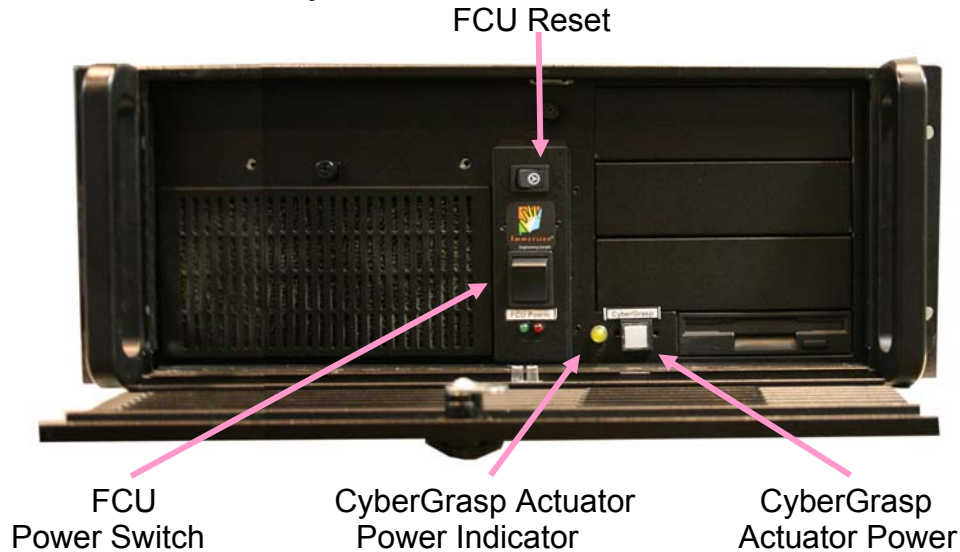
The interconnection details of the sub-systems are shown in Figure 1-9. All harnesses and cables are labeled. The FCU communicates with the CyberGlove system via a serial RS232 link. The CyberGrasp and CyberForce systems are controlled using I/O cards on the system bus. The power-amplifiers for the CyberForce system are located in a separate enclosure called the *Power Supply Unit* or PSU. The following steps are required to connect all the devices. Please refer to Figure 1-10 and Figure 1-11 for the PSU and FCU panel layouts for cable connections.

Turn Off Power Switches

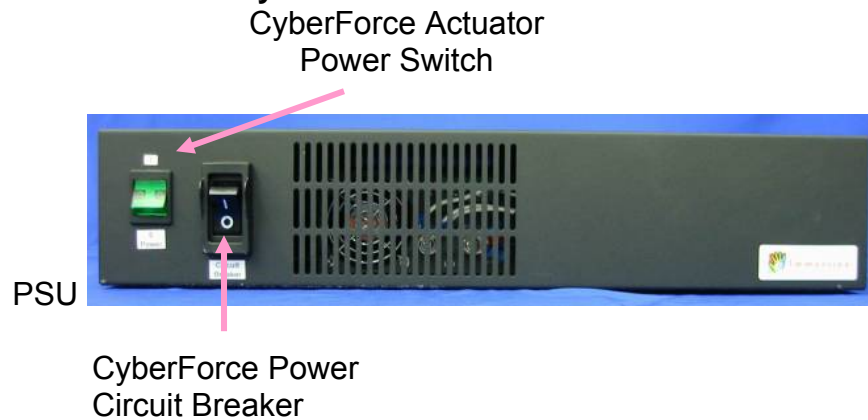
Before connecting any of the equipment, it is good practice to turn off all power switches. The switches and their functions are described below. The **CyberGrasp Actuator Power** switch (on the front panel of the FCU) controls the power to the CyberGrasp motors alone, without affecting the FCU processor or the CyberForce actuators. The indicator is lit when power is on. To reset the FCU (reboot), toggle the processor **Reset** switch. The **FCU Power** switch controls power to the FCU's central processing unit. The **Main Power** switch located on the back of the FCU case (see Figure 1-11) controls power to the whole FCU and, when turned off, overrides front panel switches.

Figure 1-10: FCU and PSU Front Panel Layouts

FCU Front Panel Layout



PSU Front Panel Layout



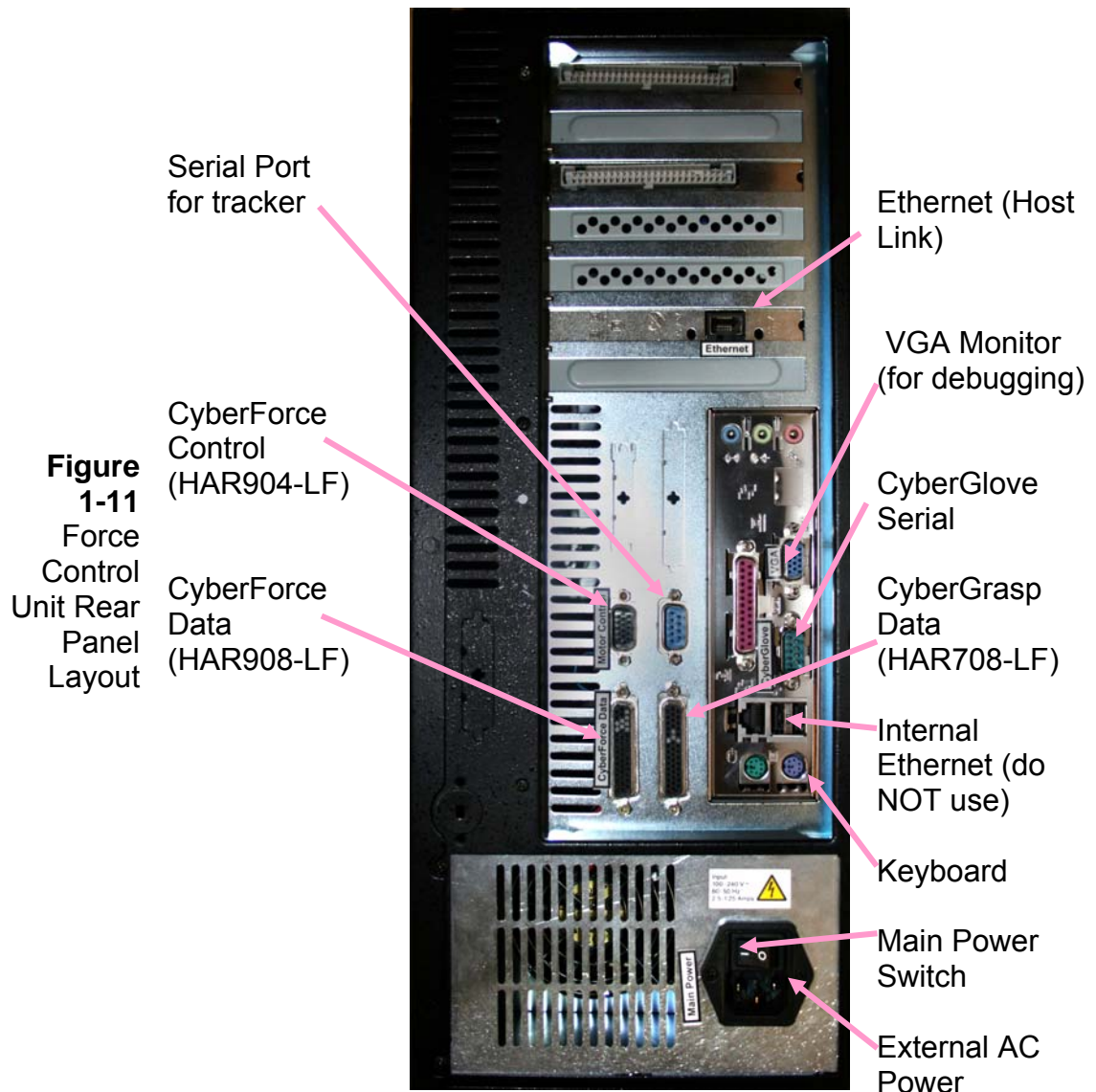
NOTE: The **CyberGrasp Actuator Power Indicator** light will flash intermittently upon shut-off as the amplifiers for the motors power down.

The PSU enclosure has a green switch, labeled CyberForce Actuator Power Switch in Figure 1-10 above, that controls the power for the CyberForce motors. The PSU also has a circuit breaker that shuts down CyberForce system power if an over-current condition occurs. The circuit breaker must be in the ON position to apply power to the CyberForce system.

The two actuator power switches (one on the FCU and one on the PSU) allow the user to independently activate or deactivate the CyberGrasp or CyberForce systems.

Orient the FCU

If the FCU is operated in the horizontal configuration ensure that nothing is to be placed on top of the chassis as this could adversely affect the performance of the device.



NOTE: At the rear panel of the FCU, as shown in Figure 1-11, there are a number of unused motherboard ports including USB, mouse, parallel, sound, and auxiliary Ethernet. These additional ports are not to be used during normal

operation of the CyberForce system. In some *circumstances*, CyberGlove Systems technical support may ask that the keyboard and monitor ports be used to access internal diagnostic information. Only attach devices to the appropriately labeled ports as documented in this manual.

Connect the CyberGlove to the FCU

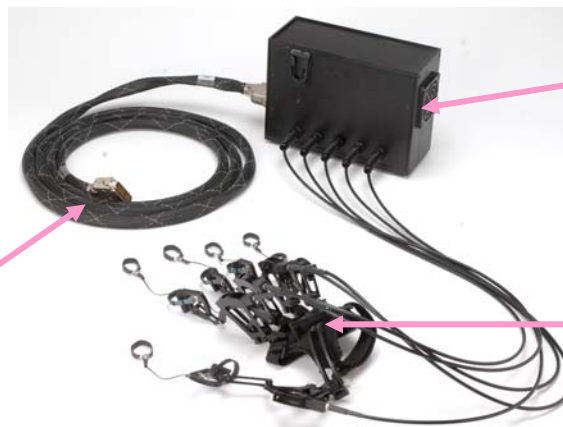
Refer to the CyberGlove manual for more information on using your CyberGlove system. The CyberGlove system includes a separate unit called the CyberGlove Interface Unit (CGIU) that processes data and communicates to the Force Control Unit (FCU). The serial cable coming from the CGIU should connect to the CyberGlove Serial Port on the FCU (see Figure 1-11).

Connect the CyberGrasp Actuator Unit to the FCU

Connect the CyberGrasp cable (part no. HAR708-LF) to the CyberGrasp actuator unit (see Figure 1-12) and to the back of the FCU (see Figure 1-11). The actuator unit is the box that contains the motors that drive the tendons on the CyberGrasp exoskeleton.

Figure 1-12
CyberGrasp
Actuator Unit
and
Exoskeleton

CyberGrasp
Data Cable
(HAR708-LF)



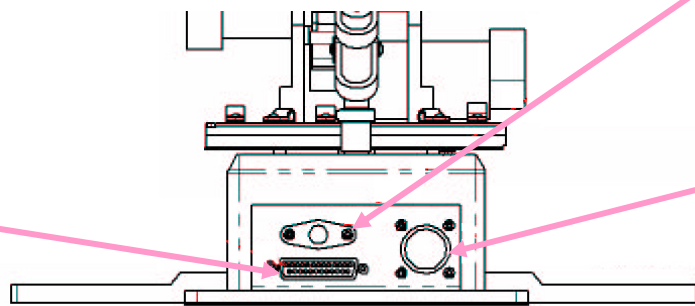
CyberGrasp
Actuator Unit

Exoskeleton

Figure 1-13

CyberForce Armature Connections

CyberForce Data Cable Connector (HAR908-LF to FCU)



Safety System User Footswitch Jack

CyberForce Motor Cable Connector (HAR903-LF to PSU)

Connect the CyberForce Armature to the FCU

Connect the CyberForce data cable (part no. HAR908-LF) to the CyberForce armature (see Figure 1-13) and to the FCU rear panel (see Figure 1-11).

Figure 1-14
CyberForce Power Supply Unit (PSU) Rear Panel

CyberForce Control Cable (HAR904-LF to FCU)



CyberForce Motor Cable (HAR903-LF to CyberForce Armature)

AC Power

Connect the CyberForce Armature to the Power Supply Unit

Connect the CyberForce motor power cable (part no. HAR903-LF) to the CyberForce armature (see Figure 1-13) and to the CyberForce power supply unit (see Figure 1-14). This harness has a round connector. The connector port is on the back of the PSU.

Connect the Power Supply Unit to the Force Control Unit

Connect the CyberForce control cable (part no. HAR904-LF) to the PSU (see Figure 1-14) and to the rear panel of the FCU (see Figure 1-11).

Connect the Safety System User Footswitch to the CyberForce Armature

Connect the Safety System User Footswitch to the CyberForce Armature footswitch socket on the rear of the armature electronics enclosure in the base of the armature. See Figure 1-13.

Connect the FCU to the Network

Using a standard STP Category 5 Ethernet cable, connect the FCU to your network hub. The Ethernet connector is located on the back panel of the FCU (see Figure 1-11). The FCU can also be connected directly to the host computer if a cross-over cable is used.

Connect Power Cords to the FCU and Power Supply Unit

Make sure the main power switch located on the back of the FCU is in the OFF position. Note that the FCU accepts power inputs from 100 to 240 VAC at 63 – 47 Hz. Connect the AC power cord to the back of the FCU (Figure 1-11) and then to the mains.

Make sure the main power switch of the Power Supply Unit is in the OFF position. Note that the PSU accepts power inputs from 100 to 240 VAC at 63 - 47 Hz. Connect the AC power cord to the back of the PSU (see Figure 1-14) then to the mains.

Connect a Monitor to the FCU (Optional)

For debugging purposes, a VGA (or SVGA) monitor can be connected to the FCU to view error messages, but it is not required (see Figure 1-11). A monitor is not included in the system.

! WARNING: Refer to the CyberGlove manual to obtain more information on how to configure it properly. Do not attempt to run your CyberGrasp unit before familiarizing yourself with the CyberGlove devices!

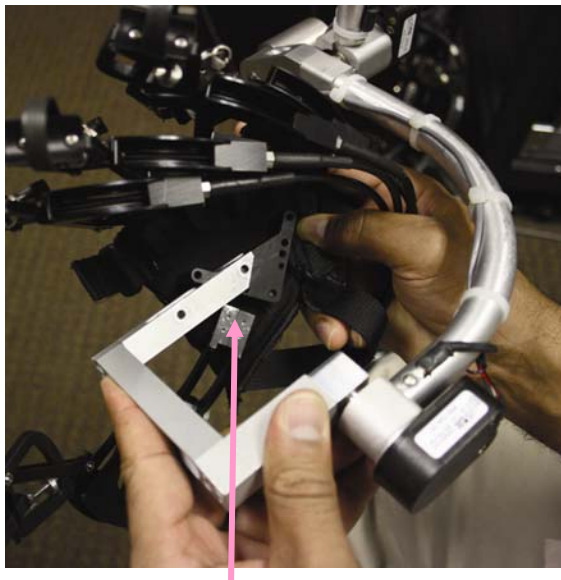
NOTE: FCU Unused Ports

At the rear panel of the FCU, as shown in Figure 1-11, there are a number of unused motherboard ports including USB, mouse, parallel, sound, and auxiliary Ethernet. These additional ports are not to be used during normal operation of the CyberForce system. In some circumstances, CyberGlove Systems technical support may ask that the keyboard and monitor ports be used to access internal diagnostic information. The second serial port may be used for a tracker. Only attach devices to the appropriately labeled ports as documented in this manual.

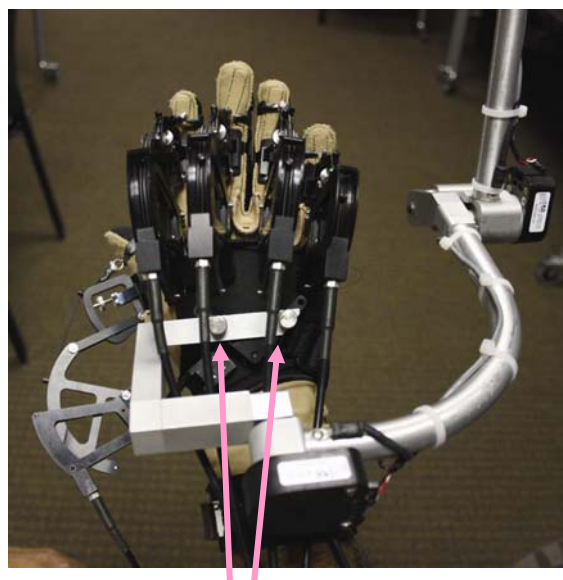
Attach the CyberGrasp Exoskeleton to CyberForce Structure

The CyberForce system end-attachment fits into the CyberGrasp mounting bracket as shown in Figure 1-15. Use the two screws that are shipped with the system to secure the mating.

Figure 1-15
CyberGrasp Exoskeleton Attachment to Right-hand CyberForce



CyberForce part slides into the mounting bracket



Mounting thumb screws

System Setup

Home the Systems

In order for CyberForce to measure the correct hand position, it is necessary to first orient the device by moving it into the home position and maintaining the position during the FCU booting process (about 20 seconds). When the FCU has finished booting, it will beep three times, indicating that the home position has been recorded and the system is ready for use.

Home position (see Figure 1-16) is achieved when:

- The base horizontal swivel joint is positioned so it is at the middle of its motion range.
- The first linkage is positioned so it reaches its up motion limit stop (up configuration).
- The second linkage is positioned so it reaches its down motion limit stop (down configuration).
- The remaining linkages are positioned horizontally with the grasp (finger) mount facing down.

Figure 1-16a
Homing Position

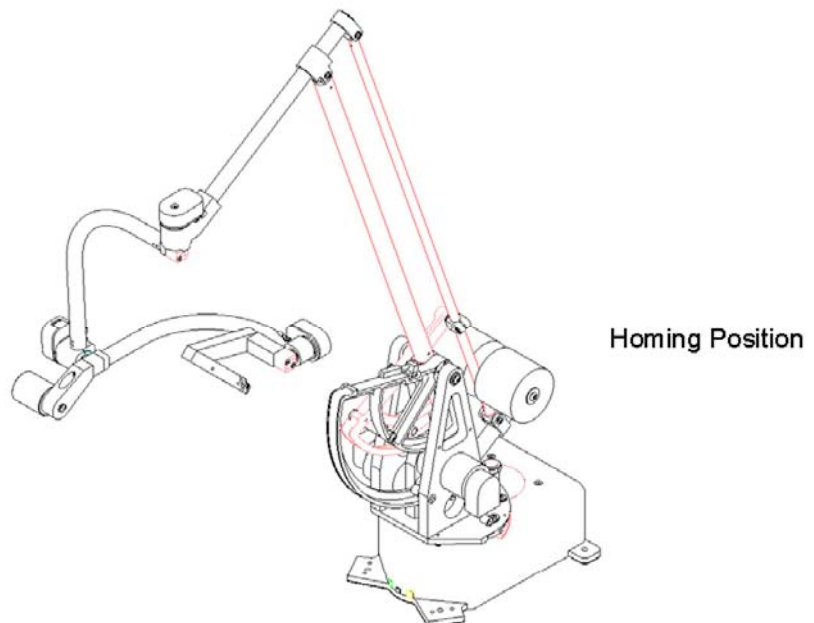
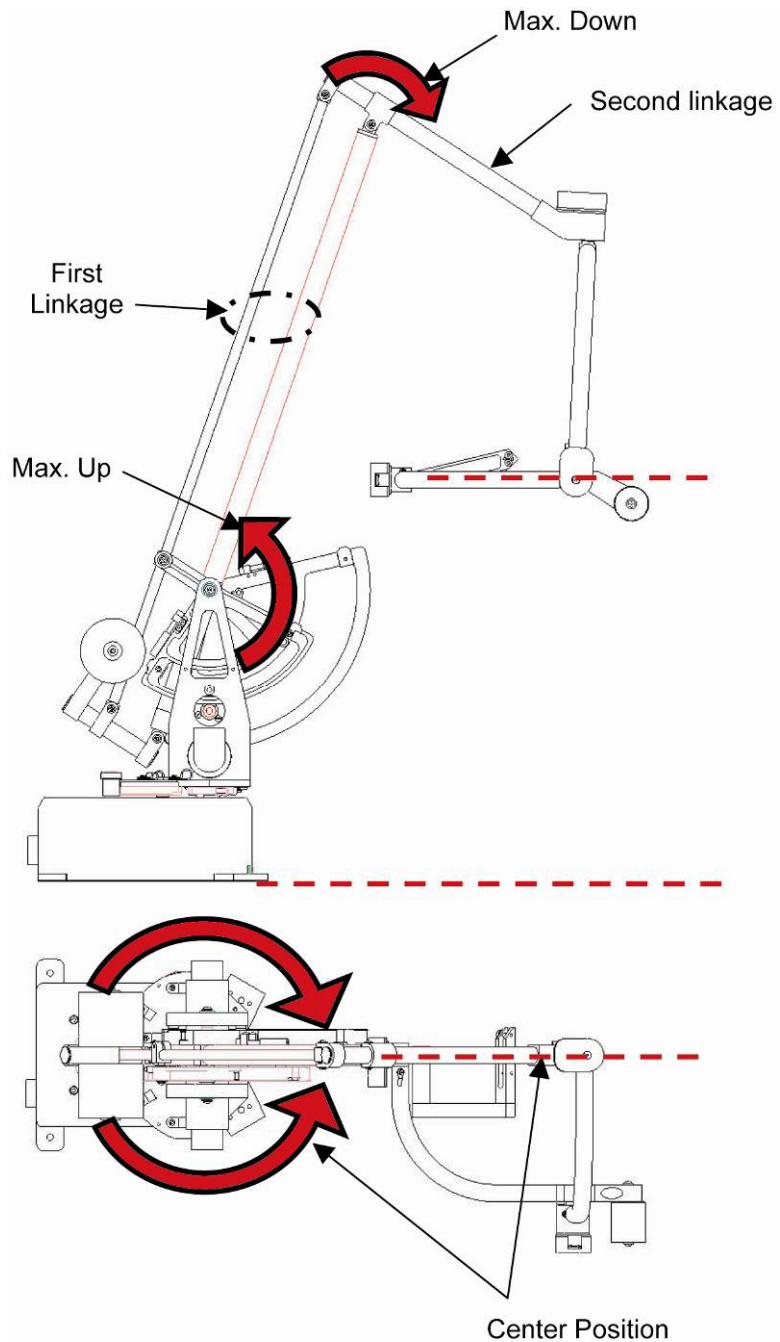
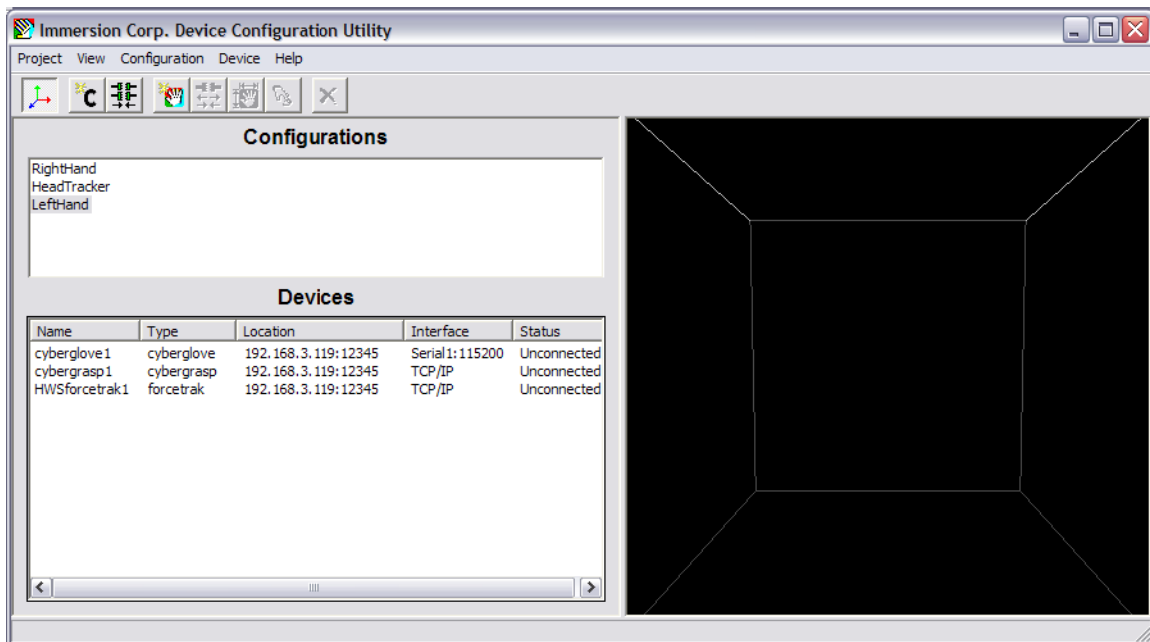


Figure 1-16b
Home Position



NOTE: The two-handed version of this particular configuration of the CyberForce system is also known as the Haptic Workstation. Users of the VirtualHand SDK will need to set the **useHapticWorkstation** flag in the `vhtKinematics` class to assure correct kinematics for the arm. VirtualHand for V5 users will need to name their forcetrack devices with the **HWS** prefix in the Device Configuration Utility (DCU) to assure compatibility with this revision of hardware.





FCU Boot-up Sequence

1. Make sure there is no disk in the floppy drive and that the **FCU Power** button is in the OFF (0) position. The **FCU Power** button is located on the front panel of the system controller (see Figure 1-10).
2. Make sure that the CyberGrasp Actuator Power Switch is OFF (out), that the CyberForce PSU power switch is OFF (0), and that the CyberForce PSU circuit breaker is ON (1) (see Figure 1-10).
3. Put the FCU **Main Power** switch in the ON (I) position. The switch is located in the back of the FCU (see Figure 1-11).
4. Put the CyberForce armature into the home position configuration as described under "Home the Systems" above, and hold it there. The *home position* needs to be set every time the system is booted for normal operation. If the system is booted only for network configuration using the configuration floppy (see "Configuring the FCU for your Network"), this step is not required.
5. Depress the **FCU Power** switch for few seconds. The switch is located in the front of the controller (see Figure 1-10).
6. Wait for the FCU to boot up. When it is ready, it will emit three consecutive beeps. This will take approximately 20 - 30 seconds. When this step is complete, you can move the CyberForce armature away from its home position.

7. If you are planning to use both CyberGrasp and CyberForce together and the CyberGrasp exoskeleton is not already mounted to the CyberForce system, mount it now (see the “Attaching CyberGrasp Exoskeleton to CyberForce Structure” section).
8. After your software is ready to control the actuators, push the CyberGrasp Actuator Power Switch on the FCU so that it is ON (in) and switch the CyberForce Actuator Power Switch on the PSU to ON (1). See Figure 1-10. Both switches should be illuminated when on.

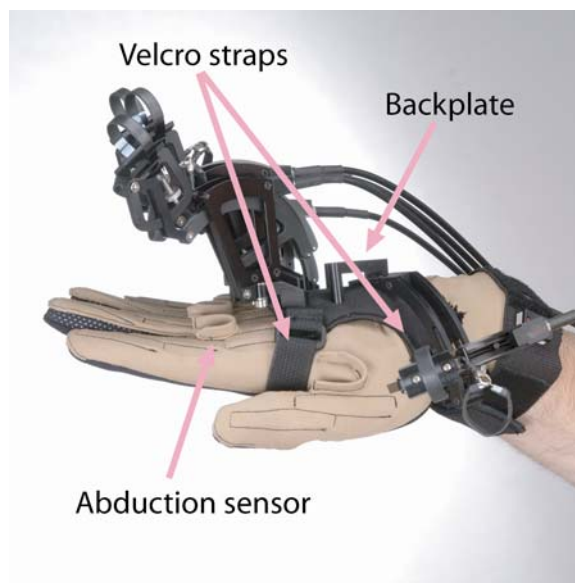
Depress and hold down the user footswitch to enable the CyberForce actuators.

Wearing the CyberGrasp Exoskeleton

The user should first put on the CyberGlove (fabric glove) and then follow steps 1 through 8 to properly position the CyberGrasp exoskeleton on the hand:

1. Make sure the tendon cables and the CyberGlove cable are not tangled before beginning. They should all fall to the right of the arm for a right-handed system, and to the left of the arm for a left-handed system.
2. Make sure the thumb tendon cable goes over the arm and not under.

**Figure
1-17**



3. Position the CyberGrasp backplate in the middle of the back of the hand such that the plate is just behind the abduction sensors (the U-shaped elements rising from the back of the CyberGlove). The plate should rest comfortably on the back of the hand. All cables should go over the hand towards the little finger.

! WARNING: Do not place the backplate on top or against, the abduction sensors! This may result in damage to the sensors and is not covered under warranty.

Figure 1-18



4. Tighten both Velcro straps as tightly as possible without being uncomfortable. At this point, the backplate should be firmly and squarely positioned on the back of the hand.

Figure 1-19



5. Slide all the finger loops onto the corresponding fingers. If they are too tight, loosen them using the thumbscrew. The force applicator rings should then be slid onto the fingertips, i.e. the distal phalanges.

**Figure
1-20**



6. The finger loops can be tightened using the thumbscrews. Position the cam in the center of the middle phalanx before tightening. Flexing the finger makes it easy to locate the middle phalanx. The device comes with multiple finger rings. If the current ring is too small or too large to reliably stay on the fingertip, use the ring clip to replace it with another one.

**Figure
1-21**



7. The next step is to ensure that the thumb assembly is properly aligned with the thumb as indicated in the Figure 1-21. This is achieved with the adjustment screw shown in Figure 1-22.

**Figure
1-22**



8. When the adjustment screw is loosened, it is possible to slide the thumb assembly back and forth in the slots. The slots are designed so the orientation of the assembly does not change as it slides through the slots. When moving the assembly, hold on to the adjustment screw, not the assembly itself, as it may bind. Very little torque is required to sufficiently tighten the screw. Excessive torque may cause damage.

! WARNING: *Do not place the backplate on top or against, the abduction sensors! This may result in damage to the sensors and is not covered under warranty!*

Establish the Device Configuration

After all devices have been physically connected, their relationship to each other needs to be established within the Device Configuration Utility (DCU). The configuration also includes the unique calibration settings for each user of the Cyber systems. See the VirtualHand SDK User Guide for complete instructions, but in summary, establishing device relationships requires that you:

- Start the Device Manager and the DCU on your host PC.
- Create a new configuration using the DCU's Configuration menu.
- Add the devices that make up the configuration by using the DCU's Device menu.
- Connect to each device by selecting it in the DCU's Devices window, then pulling down Device > Connect.

Calibrate the CyberGrasp System

Refer to the VirtualHand SDK user guide for complete instructions, but in summary, calibrating the devices relative to the CyberForce system requires that you:

- Select the device you want to calibrate from the device list within the DCU, then pull down Device > Calibrate.
- Follow the onscreen instructions, which require you to move your hand and fingers in specific ways.
- Save the calibration.

Become Familiar with the CyberForce Safety System

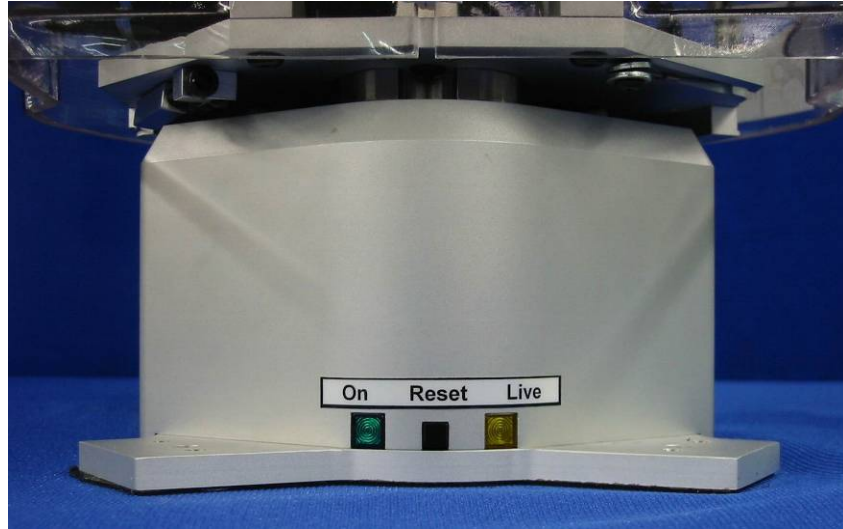
The CyberForce safety system monitors the performance of CyberForce and disables its actuators if any of the following conditions occur:

1. The user footswitch is released.
2. Overspeed of an encoder is sensed.
3. FCU ok signals are not asserted by the FCU software.

A green LED on the front panel of the electronics enclosure in the base of the CyberForce armature lights to indicate that the safety system started successfully. A yellow LED on the same panel lights whenever the CyberForce power amplifiers are enabled.

After start-up or a safety system reset, depress the user footswitch connected to the jack on the back of the CyberForce armature (see Figure 1-13) to enable the CyberForce actuators. The yellow LED on the front panel of CyberForce will light, which alerts the user that the actuators are powered. If at any time one or more of the disable conditions listed above occurs, the CyberForce actuators will power down and the yellow LED will turn off alerting the user that the actuators were powered down due to a safety violation (see Figure 1-23).

Figure 1-23
Front Panel
Armature



To reactivate the CyberForce actuators after the safety system shuts down, the safety system must be reset by pressing the reset button on the front of the base of the CyberForce armature. Depressing the user footswitch will then re-enable the amplifiers as described above

Appendix A

Controlling the FCU Over the Network

The FCU can be controlled and monitored over the network for maximum flexibility. The FCUInstallation/CyberForce/RevE directory of the distribution CD contains a shell-based utility called nc that will let you perform remote management. To use it, you must go to the appropriate directory, and type:

```
nc numeric_ip_address_of_force 24
```

The following menu will appear on the screen:

```
=====
a. restart the device manager

b. restart the device manager and watch its output

c. reboot the grasp controller

d. shutdown the grasp controller

q. quit
=====
```

Type your choice and hit <enter>. You can choose any above menu items by type its leading character and hit the enter key.

Appendix B

FCU Software Installation

The Force Control Unit (FCU) comes with a Device Manager and all associated software pre-installed at the factory. In normal situations, it must only be given a network name and address so that it can operate over a TCP/IP network. This procedure is explained in *Network Setup*, page 11.

If for any reason the FCU software should become damaged, the VirtualHand SDK distribution CD contains all necessary files for initializing and configuring the FCU. Re-installing the software is done in two steps. First, you must initialize the FCU as described in the “Configuring the FCU for your Network” section with the modifications below. Then you must download the FCU software over the network.

! WARNING: *Reinstalling the FCU software is not required on new units! Only refer to this chapter if upgrading the FCU software or reinstalling it to replace lost/damaged files.*

Initializing the FCU for Software Installation

Follow the instructions in the “Creating the FCU Initialization Floppy” section to create the disk. Then follow the instructions in the “Recording Your Network Configuration Settings on the FCU Initialization Disk” section to write your network configuration settings onto the disk, but instead of selecting “network configuration only,” select “full FCU software installation” in response to the last question.

! WARNING: *ONCE THE DISK IMAGE HAS BEEN COPIED TO THE FLOPPY DISK, REMOVE IT FROM YOUR DISK DRIVE AND LABEL IT CAREFULLY. BOOTING YOUR COMPUTER WITH THAT FLOPPY DISK MAY RESULT IN UNCOVERABLE DATA LOSS AT THE CYBERFORCE SOFTWARE REPLACES THE CONTENTS ON YOUR MAIN DISK!*

Then follow the instructions in the “Initializing the FCU” section to initialize the FCU. Once the initial installation has succeeded, instead of beeping three times (as happens if you are only configuring the network settings), the FCU will beep once every 10 seconds to indicate that it is awaiting the rest of the Device Manager software to be installed over the network.

Installing/Updating the FCU Software Over the Network

Note: These instructions apply to the hardware revision E of the CyberForce system. If you purchased your CyberForce system before January 2007, please contact fyazadi@cyberglovesystems.com for modified instructions.

This process consists of transferring the software packages from your workstation to the FCU using the network link. The software packages are contained in three archives, located in the FCUInstallation/CyberForce/RevE directory of the VirtualHand SDK installation directory.

From a DOS command prompt , go to the appropriate directory, and type:

```
update_FCU.bat numeric_ip_address_of_force main.tgz
update_FCU.bat numeric_ip_address_of_force stg_update.tgz
update_FCU.bat numeric_ip_address_of_force RevE_Right.tgz
```

(substitute RevE_Left.tgz above if you have a left-handed CyberForce)

The numeric_ip_address_of_force is the number you provided at the configuration stage of the initialization floppy disk.

Depending on your network capacity and traffic, the data transfer will take from one to ten seconds. The FCU will beep three times after the software packages have successfully been installed.

You will then re-boot your FCU. Upon re-boot, a Device Manager is started automatically and is ready to handle client requests. You can use either the Device Configuration Utility or the demo applications supplied in the distribution CD to ensure that the system is working properly. Please refer to the VirtualHand SDK User's Guide for instructions on how to do so.

Appendix C

Maintenance & Troubleshooting

Maintenance

CyberForce is factory serviceable only, containing no user serviceable parts. Surfaces of armature, PSU and FCU may be cleaned with mild detergent using a slightly damp cloth.

Troubleshooting

If you are experiencing problems with your CyberForce or CyberGrasp unit, please read the following list of problems carefully. If you are still unable to solve your problem, you can contact CyberGlove Systems LLC support staff at fyazadi@cyberglovesystems.com

PROBLEM: Cannot hear the three beeps after the floppy drive light goes off.

SOLUTION: This is most likely caused by a defective boot floppy. Try to make another boot floppy, preferably using a new diskette, and boot the FCU with it. If it still fails, try to make the floppy on another machine. ***DO NOT USE THE FCU INITIALIZATION FLOPPY TO BOOT YOUR PC. BOOTING YOUR COMPUTER WITH THIS DISK MAY RESULT IN UNRECOVERABLE DATA LOSS AS THE CYBERFORCE SOFTWARE REPLACES THE CONTENTS ON YOUR MAIN DISK!***

PROBLEM: The update_FCU.bat on XP prompts "Failed to connect to the CyberGrasp."

SOLUTION: The message indicates that the installation program cannot establish a stable connection to the FCU. The following should be checked:

- Make sure the network setting for the FCU is configured properly, and has access to your LAN. Any typographic error in the information you provided when running netcfg.exe will likely cause the FCU network interface to be configured incorrectly. Examine the settings by running netcfg.exe on the boot floppy again. Contact your network administrator if you are not sure about the settings.
- Make sure the host computer can access the FCU over the network. This can be verified by using the ping command and "pinging" the FCU from the host machine as:

```
ping grasp_ip.
```

- Only one update session is allowed to run at any time. Attempts to start the update process will be denied if there is another update session running. If you aborted an update; please wait for at least 10 seconds before another attempt.

PROBLEM: Could not hear the three beeps after the installation program finished on the host computer.

SOLUTION: Your network may be experiencing heavy traffic at the moment you run the update program. Therefore it may time-out before it finishes the update. Try to run the update program a few more times. Also, the beeps may be too weak to hear if you are at a distance from the FCU. Verify whether the Device Manager is running with the Device Control Utility. You can also use the nc program to restart the Device Manager or reboot the FCU manually.

PROBLEM: The FCU beeps continuously after it is booted with the Installation floppy.

SOLUTION: The beeps are normally an indication of a serious hardware

problem. Please contact CyberGlove Systems technical support for further assistance.

PROBLEM: The software installation finished successfully, but I could not access the FCU with the nc utility.

SOLUTION: Reboot the FCU.

PROBLEM: I can control the FCU with nc, but my application fails to access devices on it.

SOLUTION: Make sure you can access the FCU with the Device Configuration Utility (See the VirtualHand User's Guide for more information).

- Make sure the right IP address is being used by your application. If a canonical address (e.g. grasp.domain.com) doesn't work, try the corresponding numerical IP address (e.g. 192.1.34.15) instead.
- Make sure the configuration of the device matches what is specified in your application. Check if it is connected to the right serial port, running at appropriate baud rate etc. You may choose to restart the Device Manager and watch its output in the nc program. This will give you more clues as you debug the setup.

CYBERFORCE LIMITED HARDWARE WARRANTY

PLEASE READ THIS DOCUMENT CAREFULLY! IT CONTAINS VERY IMPORTANT INFORMATION ABOUT CUSTOMER RIGHTS AND OBLIGATIONS, AS WELL AS LIMITATIONS AND EXCLUSIONS THAT MAY APPLY TO THIS LIMITED WARRANTY.

TERM: The term of this warranty ("Warranty Period") is one (1) year from the date of delivery of the CyberForce Product ("Product") only to the initial end user purchaser ("Customer") located anywhere in the world, except a member state of the European Union. For end user purchasers located in a member state of the European Union only, the term of this warranty ("Warranty Period") is two (2) years from the date of delivery of the Product only to the initial end user purchaser ("Customer").

LIMITED WARRANTY REPAIRS: During the Warranty Period, CyberGlove Systems agrees to repair or replace the Customer's Product if such Product does not perform substantially in accordance with CyberGlove Systems' then-current, published functional specifications for the Product at the date of the Product's manufacture.

To request warranty service, Customer must contact CyberGlove Systems' Customer Technical Support within the applicable Warranty Period. Customer agrees to provide CyberGlove Systems the following information: (i) Product model; (ii) Product serial number; (iii) description of problem or reason for coverage; and (iv) such other information as CyberGlove Systems may request. If CyberGlove Systems determines service is required and covered by this warranty, CyberGlove Systems will issue a Return Material Authorization ("RMA") Number and return instructions. Once Customer has received an RMA number, Customer must ship the Product to CyberGlove Systems (or another location specified by CyberGlove Systems) in its original or equivalent packaging and in accordance with CyberGlove Systems' return instructions, include the RMA number, prepay shipping charges, and insure the shipment or accept the risk of loss or damage during shipment.

CyberGlove Systems will ship the repaired or replacement Product to Customer freight prepaid (Incoterms 2000 - Delivery Duty Unpaid), if the repair or replacement is covered by this warranty. CyberGlove Systems assumes no responsibility for freight and all other taxes and charges for non-warranty repairs or replacement (Incoterms 2000 - ExWorks).

CyberGlove Systems owns all parts removed from repaired Products. CyberGlove Systems uses new and reconditioned parts made by CyberGlove Systems and/or various manufacturers in performing limited warranty repairs and building replacement Products. If CyberGlove Systems repairs or replaces a Product, the Warranty Period is not extended.

EXCLUSIONS: This warranty does not apply to Products which CyberGlove Systems determines, upon inspection, have become defective, damaged or nonconforming due to external causes, including accident, abuse, mishandling, misuse, alteration, negligence, normal wear and tear, improper installation by a party other than CyberGlove Systems, problems with electrical power, use which is not in accordance with the information and precautions described in the applicable end user manual and/or documentation, service by a party other than CyberGlove Systems, failure to perform required preventive maintenance, problems caused by use of parts or components not supplied by CyberGlove Systems, operation or storage of the Product in a temperature or environment outside of those specified, damage during shipment, or other causes beyond CyberGlove Systems' control. This warranty does not apply to (i) any third party products, software or components not manufactured by CyberGlove Systems or (ii) any third party products sold by CyberGlove Systems for use with the Product.

THIS WARRANTY IS PROVIDED IN LIEU OF ALL OTHER RIGHTS, CONDITIONS AND WARRANTIES. CYBERGLOVE SYSTEMS MAKES NO OTHER EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE SOFTWARE, HARDWARE, PRODUCTS, DOCUMENTATION OR CYBERGLOVE SYSTEMS SUPPORT, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, THOSE ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE AND NON-INFRINGEMENT.

CYBERGLOVE SYSTEMS DOES NOT WARRANT THAT ANY PRODUCTS WILL BE ERROR-FREE, OR THAT ANY DEFECTS THAT MAY EXIST IN ITS PRODUCTS CAN BE CORRECTED. IN NO EVENT SHALL CYBERGLOVE SYSTEMS BE LIABLE FOR COST OF PROCUREMENT OF SUBSTITUTE GOODS, LOST PROFITS OR ANY OTHER SPECIAL, INDIRECT, CONSEQUENTIAL OR INCIDENTAL DAMAGES (INCLUDING BUT NOT LIMITED TO LOST DATA), HOWEVER CAUSED WHETHER OR NOT CYBERGLOVE SYSTEMS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

NO RESELLER IS AUTHORIZED TO MAKE ANY MODIFICATIONS, EXTENSIONS, OR ADDITION TO THIS WARRANTY.

THE WARRANTIES EXPRESSLY SET FORTH IN THIS LIMITED WARRANTY STATEMENT ARE LIMITED IN DURATION TO THE LIMITED WARRANTY PERIOD SET FORTH ABOVE AND NO WARRANTIES, WHETHER EXPRESS OR IMPLIED, WILL APPLY AFTER SUCH PERIOD.

Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply. Additionally, some jurisdictions do not allow the exclusion of certain implied

warranties or conditions or limitations as to the term of warranty or condition. Therefore the foregoing disclaimers may not apply in the jurisdiction of Customer's purchase.

The CyberGrasp system was partially developed with funding from the Office of Naval Research's STTR program (contract #N00014-97-C-0112).

The CyberForce system was partially developed with funding from the Office of Naval Research's STTR program (contract #N00014-98-C-0060).

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 instructions, 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 personal expense.



CyberGlove Systems LLC

2355 Paragon Drive, Suite D

San Jose, CA 95131

Tel: (408) 451-9463

Fax: (408) 689-4362

fyazadi@cyberglovesystems.com

This document does not create any express or implied warranty about CyberGlove Systems or about its products or services. CyberGlove Systems has made reasonable efforts to verify that the information contained herein is accurate, but CyberGlove Systems assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact CyberGlove Systems for current information regarding its products or services. CyberGlove Systems' products and services are subject to CyberGlove Systems' standard terms and conditions.

©2009 CyberGlove Systems LLC. All rights reserved. CyberGlove Systems, the CyberGlove Systems logo, CyberForce, CyberGlove, CyberGrasp, and VirtualHand are trademarks of CyberGlove Systems LLC in the U.S. and other countries. All other trademarks are the property of their respective owners. CyberForce is produced under license from SensAble Technologies, Inc.

Doc P/N M01006, rev A, 09/07