



Safety Boot Operational & Maintenance Manual



Document Revision C555B 10/03
Safety Boot Version 1.00

Copyright and Trademark

© 2003, Computer Support Systems. All rights reserved. No part of the contents of this manual may be transmitted or reproduced in any form or by any means without the written permission of Computer Support Systems.

Ethernet is a trademark of XEROX Corporation. UNIX is a registered trademark of The Open Group. Windows 95®, Windows 98®, Windows 2000, Windows NT®, and Windows XP are trademarks of Microsoft Corp. Netscape is a trademark of Netscape Communications Corporation. Java™ is a trademark or a registered trademark of Sun Microsystems, Inc. in the United States and other countries.



Computer Support Systems Pty Ltd.

Head Office: 373 Johnston Street
Abbotsford
VICTORIA 3067
Australia

Telephone: 61 3 9419 3955
Facsimile: 61 3 9419 3509
Web Address: www.csspl.com.au
sales@csspl.com.au
support@csspl.com.au



Disclaimer and Revisions

Operation of this equipment in a residential area may cause interference in which case the user, at his or her own expense, will be required to take whatever measures may be required to correct the interference.

Date	Revision	Comments
22/10/2003	CSSSB10/03	NK

Declaration of Conformity

Manufacturer's Name & Address:

Computer Support Systems Pty Ltd, 373 Johnston Street, Abbotsford VICTORIA
3067, Australia.

Product Name Model: Safety Boot Version 1.00



Warranty

Computer Support Systems warrants Safety Boot; if used in accordance with all applicable instructions, to be free from defects in material and workmanship for a period of one year from the date of initial purchase.

This warranty is voided if the customer uses the Safety Boot in an unauthorized or improper way, or in an environment for which it was not designed. Warranty does not apply to normal wear or to damage resulting from accident, misuse, abuse or neglect.

Safety Instructions

When using this product, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:

1. Read and understand all instructions.
2. Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
3. Do not use this product in an outdoor environment or near water, for example, near a bathtub, washbowl, kitchen sink, or laundry tub, in a wet basement, or near a swimming pool.
4. Do not place this product on an unstable cart, stand, or table. The product may fall, causing serious damage to the product.
5. This product should never be placed near or over a radiator or heat register. This product should not be placed in a built-in installation unless proper ventilation is provided.
6. Do not allow anything to rest on the power cord. Do not locate this product where the cord will be abused by persons walking on it.
7. Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.
8. Never push objects of any kind into this product through slots as they may touch dangerous voltage points or short out parts that could result in a risk of fire or electrical shock. Never spill liquid of any kind on the product.
9. To reduce the risk of electrical shock, do not disassemble this product. Opening or removing covers will expose you to dangerous voltages or other risks. Incorrect re-assembly can cause electric shock when the appliance is subsequently used.
10. Unplug this product from the wall outlet and return to CSS for repairs under the following conditions:
 - a) When the power supply cord or plug is damaged.
 - b) If liquid has been spilled into the product.
 - c) If the product has been exposed to rain or water.
 - d) If the product does not operate normally by following the operating instructions. Adjust only those controls that are covered by the operating instructions because improper adjustment of other controls may result in damage and will often require extensive work by a qualified technician to restore the product to normal operation.
 - e) If the product has been dropped or has been damaged.
 - f) If the product exhibits a distinct change in performance.
11. Do not exceed the maximum output rating of the auxiliary power receptacle.

Contents

COPYRIGHT AND TRADEMARK	I
DISCLAIMER AND REVISIONS	II
DECLARATION OF CONFORMITY	III
WARRANTY	IV
1 INTRODUCTION TO SAFETY BOOT	1
2 GETTING STARTED	2
2.1 REQUIREMENTS	2
2.2 HARDWARE INSTALLATIONS	2
2.2.1 <i>Ethernet Connection</i>	2
2.2.2 <i>Power Connection</i>	3
2.2.3 <i>Connect External 240V Device</i>	3
2.2.4 <i>Power Connection Indicator</i>	3
2.3 SAFETY BOOT CONFIGURATION	4
2.3.1 <i>Assigning of an IP Address</i>	4
2.3.1.1 IP address allocation using DHCP	4
2.3.1.2 IP address allocation using ARP and Telnet	5
2.3.1.3 IP address allocation using a Web Browser	5
3 SAFETY BOOT WEB INTERFACE	6
3.1 SAFETY BOOT CONTROL INTERFACE	6
3.2 SAFETY BOOT CONFIGURATION INTERFACE	7
3.3 SECURITY FEATURES ON SAFETY BOOT	8
3.3.1 <i>Password</i>	8
3.3.1.1 <i>Forgetting the Password</i>	9
3.3.2 <i>Single User Control</i>	9
3.3.3 <i>Inactivity Timed Logouts</i>	9
4 HARDWARE SPECIFICATIONS	10
5 TROUBLESHOOTING	11
5.1 TECHNICAL SUPPORT	12

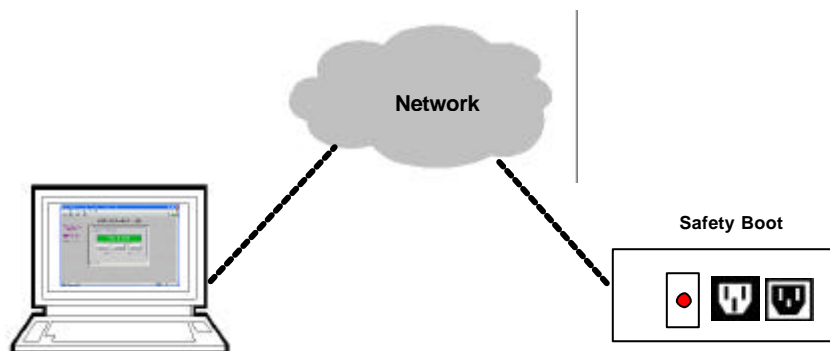


1 Introduction to Safety Boot

Safety Boot is a web enabled 240 volt A/C power switch. It is controlled over the network by simply using a Java enabled web browser. Safety Boot is password protected and hence secure.

Typical applications of Safety Boot:

- ✍ Remotely reboot any device that uses 240V power. The device connected need not to be a network device.
- ✍ Power down equipment when not required, power up when required
- ✍ Cycle power to reboot devices that do not respond. (E.g.: computer equipment)



Safety Boot ZSP 2019 Back View

2 Getting Started

2.1 Requirements

The minimum requirements to run Safety Boot effectively are as follows:

- ✍ Access to the network
- ✍ Java enabled web browser. (Netscape 4.0 or higher & IE 5.5 or higher recommended)
- ✍ Java™ 2 Runtime Environment, Standard Edition, Version 1.4.2
(You may install this from <http://java.sun.com/j2se/1.4.2/download.html>)

Note: Read *install_notes.txt* & *readme.txt* for details on minimum system requirements to install Java™ Runtime Environment Version 1.4.2

Note: On Windows XP The "Internet Connection Firewall" must be disabled, or else UDP Ports 30718 & 30704 must be available. Otherwise, you will not be able to detect or communicate with any of the Safety Boots on the network. To configure, go to the Control Panel, go to Network Settings, select the corresponding network adapter, choose Properties, and go to the Advanced tab.

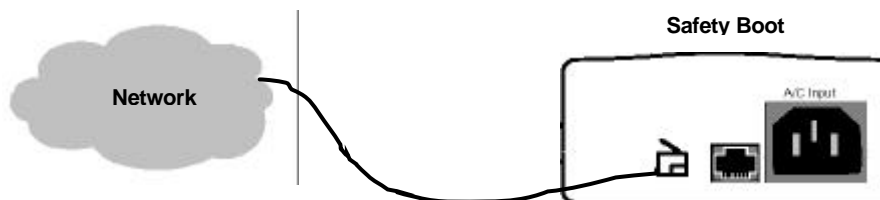
2.2 Hardware Installations

Follow the steps given below:

- ✍ Step 1: Connect the Ethernet connection to the unit
- ✍ Step 2: Connect A/C power cord to the unit with no A/C power
- ✍ Step 3: Turn A/C power on and make sure the red LED is lit.

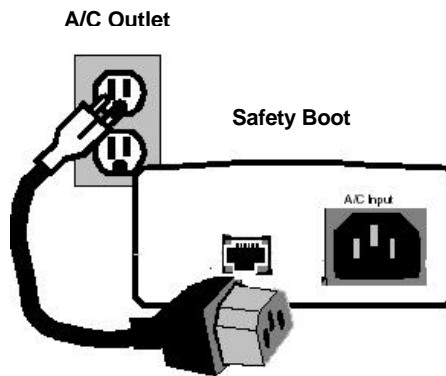
Diagrams below explain each connection.

2.2.1 Ethernet Connection



Connect the RJ45 Ethernet connection to the network.

2.2.2 Power Connection

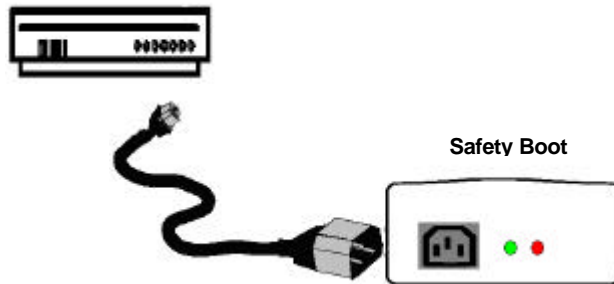


Connect A/C power source

2.2.3 Connect External 240V Device

(It is highly recommended that you connect this device once you have your device setup correctly)

Any 240V external device



2.2.4 Power Connection Indicator

The red LED Indicator next to the output power connection shows that Safety Boot is active.

The green LED is lit when the output power is enabled. The green LED is off when output power is off.

2.3 Safety Boot Configuration

The most important configuration aspect is to assign an appropriate IP address, subnet mask and the gateway to the unit.

2.3.1 Assigning of an IP Address

The Safety Boot default IP address is 0.0.0.0, which enables DHCP. When you initially connect the device to the network and connect power, it will automatically allocate an IP address if your server is DHCP enabled.

There are several methods to assign an IP address to the unit. (Consult your network administrator in determining the appropriate IP address.)

An IP address can be applied to the unit by:

1. DHCP server automatic IP allocation.
2. ARP (Address Resolution Protocol) and Telnet (Recommended)
3. Web browser via the Safety Boot configuration page. (Also recommended)

Note: *In typical installations, a fixed IP address is recommended. Your network administrator generally provides the IP address. Make sure that your IP address is not a duplicate of an already existing IP address. Obtain the following information before starting to set up your unit:*

Serial No: _____ (Label on the back of device)

IP Address: _____

Subnet Mask: _____

Gateway: _____

The best method to allocate an IP address is to isolate the unit from the external network, and use a direct cross over RJ 45 network connection with a PC. Then use ARP and telnet to allocate and IP address as described below in section 2.3.1.2.

2.3.1.1 IP address allocation using DHCP

With Safety Boots' default IP address of 0.0.0.0, DHCP has been enabled. If your server is DHCP enabled, the unit will be allocated with an automatic IP address, gateway address and a subnet mask when powered on.

The units' serial number is the MAC address of the unit. By using a DHCP client on an administrative right enabled machine you will be able to determine the IP address allocated by the DHCP server. Please consult your network administrator for further details on finding the DHCP allocated IP address.

(Ensure that you connect the network connection before power for DHCP allocated IP address)

Note: *When DHCP is enabled, Safety Boot web configuration web interface will not indicate the IP address allocated automatically as the DHCP server dynamically allocates it. We recommend that you use an appropriate static IP address given by your network administrator.*

Once you find out the IP address allocated by the DHCP server by using a DHCP client, use your web browser and point to the IP address to load web interface pages from the unit.

Section 3.2 of this document describes the Safety Boot configuration web interface in order to change any of the parameters.

2.3.1.2 IP address allocation using ARP and Telnet

You can use Address Resolution Protocol (ARP) method from UNIX and Windows® - based systems to assign a temporary IP address on to Safety Boot. The steps to configure the unit through the network are as follows.

1. Open command prompt and create an entry in the host's ARP table using the intended IP address and the hardware MAC address, which is found on the devices' serial number label.

```
Eg: arp -s 192.168.1.220 00-20-4a-xx-xx-xx  
    |---- new IP ---- || --- MAC Address --- |
```

Note: For the ARP command to work on Windows® 95, the ARP table on the PC must have at least one IP address defined other than its own. You can verify your ARP table by typing ARP -A at the DOS command prompt.

2. Open a Telnet connection to port 1. The connection will fail quickly, but Safety Boot will temporarily change its IP address to the one designated in this step.

```
Eg: telnet 192.168.1.220 1
```

3. Finally, open a Telnet connection to port 9999, and press Enter within three seconds to go into setup mode. If you wait longer than three seconds, the unit will reboot. If this happens go back to step 2 and start again.

```
Eg: telnet 192.168.1.220 9999
```

4. Set all required parameters by following the instructions given by the menu. Most importantly set a static IP address. Once this is completed you may use the web browser configuration to make further changes. Save settings before exiting.

Note: The IP address you just set is temporary and will revert to the default value when Safety Boots' power is reset unless you log into Safety Boot Configuration web interface and store the changes permanently. Refer to Configuration Interface on section 3.2 for instructions on permanently configuring the IP address.

2.3.1.3 IP address allocation using a Web Browser

In order to run the Java applets you need to have a Java Runtime Environment version 1.4.2 installed on your system. Read install_notes.txt for further details on how to install the Java Runtime Environment.

Open your default web browser and direct to the IP address of Safety Boot. Click on the link on the page to get into Safety Boot configuration.

Note: You will need to find the DHCP allocated IP address by contacting your network administrator. If you used ARP and Telnet (Further details on section 2.3.1.2) you would know the IP address already.

Enter the password to login to configuration and click OK. The factory default password is "password".

Section 3.2 describes the configuration interface of Safety Boot. Make appropriate changes to the unit settings and make sure you click Apply at each section.

3 Safety Boot Web Interface

Safety Boot web interface is controlled by Java applets. You will need the Java™ Runtime Environment version 1.4.2 by installed on your computer to load the applets. See section 2.1 requirements for further details.

If your system is not up-to-date with the runtime environment your browser will prompt you to download the latest Java™ 2 Runtime Environment from Sun Microsystems.

Safety Boot has two web interfaces:

- ☞ Safety Boot Controls
- ☞ Safety Boot Configuration

Safety Boot web interface gives hyperlinks for easy navigation between the two web interfaces.

Safety Boot is password protected and case sensitive. Factory default password for both web interfaces is set to be "password". These passwords can be changed at Safety Boot configuration

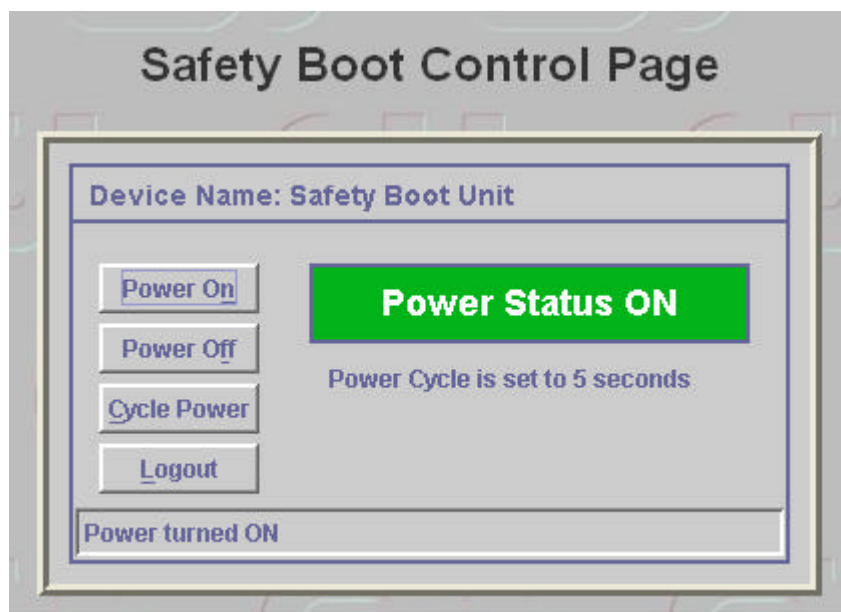
3.1 Safety Boot Control Interface

You can enter the Safety Boot control interface by typing the IP address in the address bar of your browser. Eg: 192.168.1.220

Alternatively you may configure your WINS (Windows Internet Name Service) to provide a name resolution for the adapter from NetBIOS names to IP addresses for Windows PCs.

You will need to enter the appropriate password to gain access to Safety Boot Controls.

Safety Boot Controls web interface will allow you to turn power on, off or cycle power on a predetermined cycle period.



Available Controls

Power On: Turn power on

Power Off: Turn power off

Cycle Power: Cycle power for the given period

Logout: Logout from Safety Boot

You can control Safety Boot by clicking on the appropriate button.

During a power cycle other buttons are disabled except for the “Abort” button. If you abort the power cycle, the last known power status will remain. You can change the power cycle period on Safety Boot Configuration.

If you close the browser you will be automatically logged out from Safety Boot. If you stay inactive for over 5 minutes you will be automatically logged out from Safety Boot.

Click on logout once you have completed your task.

3.2 Safety Boot Configuration Interface

You can enter the Safety Boot configuration interface by typing the IP address followed by /config.html in the address bar of your browser or by clicking on the hyperlink provided on any of the pages.

Eg: 192.168.1.220/config.html

Safety Boot Configuration interface will allow you to configure the parameters of Safety Boot

The screenshot displays the Safety Boot Configuration interface, which is organized into three main sections: Device Settings, IP Settings, and Password Settings. At the bottom, there is a 'Logout' button and a 'Connected.' status indicator.

- Device Settings:** Includes a 'Device Name' field with the value 'Safety Boot Unit' (with a '(Max 32 chars)' note), a 'Cycle Time' field with the value '5' (with a note 'Seconds.(Max=255, Min=1)'), and 'Apply' and 'Reset' buttons.
- IP Settings:** Includes 'IP Address' (192.168.1.222, with 'Eg: 192.168.1.10'), 'Subnet Mask' (255.255.255.0), and 'Gateway' (0.0.0.0) fields, along with 'Apply' and 'Reset' buttons. A note below reads: 'PS: Clicking 'Apply' will cause SafetyBoot to reboot...'
- Password Settings:** Divided into two sub-sections:
 - Control Password:** Has fields for 'Current Password', 'Enter New Password', and 'Confirm New Password', with an 'Apply' button.
 - Setup Configuration Password:** Has fields for 'Current Password', 'Enter New Password', and 'Confirm New Password', with an 'Apply' button.

Device Settings

Device Name: Allows you to enter a 32-character name for your Safety Boot. This name will be displayed on the Safety Boot Controls web interface to easily identify multiple Safety Boot units.

Cycle Time: Defines the power cycle period in seconds. Maximum of 255 seconds is accepted as a value.

IP Settings

IP Address: Enter new IP address of 0.0.0.0 to enable DHCP.

Subnet Mask: Indicates the number of subnets in the network. Contact your network administrator for further details. DHCP will automatically allocate the subnet mask.

Gateway Address: Contact your network administrator for further details. DHCP will automatically allocate the gateway address.

Password Settings

Control Password: Allows you to change the control password.

Configuration Password: Allows you to change the configuration password.

By clicking on “Reset” at each section, values you entered are rolled back to its original readings.

By clicking on “Apply” the new settings are applied to Safety Boot. Safety Boot will reboot when you click “Apply”.

Note: *You need to click on “Apply” for each subsection (i.e. Device Settings, IP Settings or Password Settings). Each time you click on “Apply” Safety Boot will reboot, thereby logging you out from Safety Boot. Allow about 10 seconds for Safety Boot to be active again. After a reboot safety Boot will always have its output status loaded with its last known status.*

If you do not need to change any settings, you can logout by clicking the logout button.


If you close the browser you will be automatically logged out from Safety Boot. If you stay inactive for over 5 minutes you will be automatically logged out from Safety Boot.

Please note that your external device should be turned off at a Safety Boot configuration change. If you fail to do this, your external device may momentarily be switched off at a configuration change.

3.3 Security Features on Safety Boot

3.3.1 Password

Safety Boot is secured by passwords at two levels:

-  Safety Boot Control Level
-  Safety Boot Configuration Level

The factory default password is set to be “password”. We recommend that you change it to a desired password with at least four characters.

Note: *Safety Boot passwords are case sensitive. The password is limited to a maximum number of eight characters.*

3.3.1.1 Forgetting the Password

If you have forgotten any of your passwords there is a method to restore the factory default passwords on Safety Boot. This method will reset both passwords back to "password".

However in order to minimise the risk of any user taking advantage of this, you will need to have physical access as well as network access to Safety Boot.

Method:

1. Go to <http://192.168.1.222/resetsb.html> (replace IP address with your IP address)
2. Click on "Reset" and your count down will begin.
3. If you want your passwords to be set back to factory defaults you will need to unplug Safety Boot before this count down is completed. The count down period is set to be one minute.
4. If you do not unplug Safety Boot before the count down is completed your passwords will remain unchanged.
5. If you are unable to load the default passwords please contact Computer Support Systems technical support.



3.3.2 Single User Control

Safety Boot is implemented as a single user control system due to security. This feature will avoid incidents where two users are simultaneously attempting to control the same device at any given time. It is important that you log out from Safety Boot once you have completed your task.

If a second user attempt to log into a Safety Boot device on use, it will indicate that the device is busy by redirecting you to a different web page.

3.3.3 Inactivity Timed Logouts

If you log into Safety Boot and be inactive for more than 5 minutes you will be automatically logged out from the web interface. This feature will protect users from forgetting to logout from Safety Boot.

4 Hardware Specifications

Device Model: Safety Boot Version 1.00

Physical Dimensions

- ✂ Dimensions: 192 mm L X 100 mm W X 40 mm H
- ✂ Weight: 380g

Network Interface

- ✂ RJ45 Ethernet 10Base-T or 100Base-TX (Auto-sensing)
- ✂ LED indication: 10Base-T & 100Base-TX Activity, Full/half duplex.
- ✂ Network Compatibility: Ethernet: Version 2.0/IEEE 802.3

Operating Temperature

- ✂ Operating range: -40°C to +85°C (-40°F to 185°F)

Power Requirements

- ✂ Current Usage: 300 mA
- ✂ Operating Voltage: 240V AC 50~60Hz
- ✂ Maximum capacity of power delivery: 8 Amps

5 Troubleshooting

This section of this manual will give you tips to troubleshoot Safety Boot without having to contact technical support staff from Computer Support Systems. Please make sure that your external device/output power is disconnected as rebooting Safety Boot can cause changes momentary changes on its output state.

When troubleshooting the following problems, make sure that Safety Boot is powered up. Confirm that you are using a good network connection. The LED's at the Ethernet connection and the table below (Table 1) will give you your connection type.

Table 1

Left LED	Right LED	Meaning
Off	Off	No Link
Off	Solid Amber	100BASE-T Half Duplex Link
Off	Blinking Amber	100BASE-T Half Duplex; Activity
Off	Solid Green	100BASE-T Full Duplex
Off	Blinking Green	100BASE-T Full Duplex; Activity
Solid Amber	Off	10BASE-T Half Duplex Link
Blinking Amber	Off	10BASE-T Half Duplex; Activity
Solid Green	Off	10BASE-T Full Duplex Link
Blinking Green	Off	10BASE-T Full Duplex; Activity

Note: Some unexplained errors might be caused by duplicate IP addresses on the network. Make sure that your unit's IP address is unique.

Table 2

Problem/Message	Reason	Solution
When you load the IP address on your browser, you are directed to a Safety Boot busy web page	Another user has already logged in.	Make sure that no one else is using the Safety Boot web interface. Safety Boot web interface is a single user system.
	Your computer is not able to connect to ports 30718 (77FEh) & 30704 (77F0h) on the server.	Make sure that ports 30718 (77FEh) & 30704 (77F0h) are not blocked with any router that you are using on the network.
Your password is not accepted any more or you have forgotten the correct password	Caps lock may be on.	Safety Boot passwords are case sensitive. Make sure you are entering the correct password.
	Password memory location may have been corrupted.	Use the Safety Boot Reset applet to load default passwords. See section 3.3.1.1 of this manual for details.
There is no respond when you type the IP address on the browser address bar.	Safety Boot may not have rebooted properly.	Disconnect power to Safety boot, wait for 20 seconds and then apply power again.

<p>You are able to ping Safety Boot, but not Telnet on port 9999.</p>	<p>There may be an IP address conflict on your network</p> <p>You are not Telneting to port 9999.</p>	<p>Turn Safety Boot off and then issue the following commands at the DOS prompt of your computer: ARP -D X.X.X.X (X.X.X.X is the IP of Safety Boot)</p> <p>PING X.X.X.X (X.X.X.X is the IP of Safety Boot).</p> <p>If you get a response, then there is a duplicate IP address on the network</p>
<p>When you issue the ARP -S command in Windows, "The ARP entry addition failed: 5" message displays.</p>	<p>Current logged in user does not have the correct rights to use this command on this PC.</p>	<p>A user with sufficient rights needs to complete the task for user rights have to be adjusted.</p>
<p>When you attempted to assign an IP address to Safety Boot via the ARP method, the "Press Enter to go into Setup Mode" error displayed. Now when you Telnet to Safety Boot, the connection fails.</p>	<p>When you Telnet into port 9999 and do not press Enter quickly, the server will reboot, causing it to lose the IP address.</p>	<p>Telnet back into Port 1. Wait for it to fail, then Telnet to port 9999 again. Make sure you press Enter quickly.</p>
<p>When you click on Power ON or OFF you get one of the following error messages on the status bar</p> <p>Power status OFF; - Internal Circuitry Error 0001</p> <p>Power status ON; - Internal Circuitry Error 0002</p> <p>Power status ON; - Internal Circuitry Error 0003</p> <p>Power status OFF; - Internal Circuitry Error 0011</p> <p>Power status OFF; - Internal Circuitry Error 0012</p> <p>Power status ON; - Internal Circuitry Error 0013</p>	<p>Internal circuitry may have been damaged.</p>	<p>Contact CSS technical staff for assistance.</p>

5.1 Technical Support

If you are unable to troubleshoot Safety Boot by using the above table (Table 2) or if you cannot fix your error, you may contact CSS technical support at
 Email: support@csspl.com.au

Telephone: 03-9419 3955

Please have the following details when you contact CSS technical staff

- ~~///~~ Model of product
- ~~///~~ Serial number
- ~~///~~ Date of purchase
- ~~///~~ Clear definition of problem
- ~~///~~ Steps taken so far to fix problem
- ~~///~~ Steps taken so far to fix problem