

Sync Defender

Network Time Server

User Manual

Version 1.2

Model versions:

Sync Defender 50

Sync Defender 100

Sync Defender 200

SAFETY PRECAUTIONS

To reduce the risk of fire, or electric shock, **DO NOT** allow the Sync Defender to be exposed to rain or moisture.

To avoid the risk of electric shock, **DO NOT** open the enclosure.

This unit is designed to be installed into an equipment rack or on a suitable flat surface. **DO NOT** install this product on an uneven surface.

To prevent damage to the unit, clean **ONLY** with a dry cloth.

Use this product **ONLY** with the supplied power cord. If the power cord becomes damaged, consult a qualified electrician for advice.

The plug on the supplied power cord is intended to serve as a disconnect device. The socket-outlet should be installed near the equipment and should be easily accessible.

This product may contain a coin / button cell battery. **DO NOT INGEST BATTERY, CHEMICAL BURN HAZARD!** If the coin / button cell battery is swallowed, it can cause severe internal burns in just two hours and can lead to death. Keep new and used batteries away from children. If you think batteries might have been swallowed, or placed inside any part of the body, seek immediate medical attention.

CERTIFICATION



In accordance with European Directives 2006/95/EC (*The Low Voltage Directive*) and 2004/108/EC (*The Electromagnetic Compatibility Directive*), the Sync Defender is in conformity with the applicable requirements of BS EN 60950-1:2006 (*Information Technology Equipment - Safety*), BS EN 55022:2006 (*Information Technology Equipment - Radio disturbance characteristics - class B*) and BS EN 55024:2003 (*Information Technology Equipment - Immunity characteristics*).

A copy of the EC Declaration of Conformity is included at the rear of this user manual. Copies of the original document may be downloaded from our web site at:

www.worldtimesolutions.com

RoHS COMPLIANCE

World Time Solutions Limited works with its suppliers to ensure all products comply with the Restriction of Hazardous Substances (RoHS) directive.

DISPOSAL



Please dispose of this unit properly. To minimize pollution and help protect the environment, this unit should be recycled.

COPYRIGHT

© 2023 - 2025 World Time Solutions Limited. All Rights Reserved.

All information contained within this document is the property of World Time Solutions Limited and cannot be used or reproduced by any person or company without written consent from World Time Solutions Limited.

World Time Solutions Limited reserves the right to make periodic amendments to the information in this document without notice.

TRADEMARKS

Microsoft, Windows, Windows 10 and Windows 11 are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

All other registered trademarks and trademarks are property of their respective owners.

SOFTWARE LICENCE

This product contains proprietary World Time Solutions Limited software. This proprietary World Time Solutions Limited software is supplied under the *World Time Solutions Limited Software Licence Agreement*.

To obtain further information and/or a copy of the software licence please visit:

www.worldtimesolutions.com

LIMITED WARRANTY

The Sync Defender network time server is guaranteed against failure due to faulty parts or workmanship for a period of five (5) years from date of purchase.

In the event of product failure due to faulty parts or workmanship within the warranty period, World Time Solutions Limited, at its own discretion, will either (a) repair the product, (b) supply a replacement product, (c) supply a functionally equivalent replacement product, or (d) refund the purchase price of the product.

The limited warranty will not apply if (a) the product has not been installed or operated as per our instructions, (b) the product has been modified in anyway.

In the event of failure, the Sync Defender should be returned to the manufacturer for inspection and repair. Please visit our support pages for further details:

www.worldtimesolutions.com/support.html

TECHNICAL SUPPORT

To obtain help with the installation or operation of the Sync Defender, please visit our web site at:

www.worldtimesolutions.com/support.html

Contents

1 - Introduction	1
1.1 - Introducing Sync Defender	1
1.2 - How Sync Defender enhances the security of your network	1
1.3 - Simplified theory of operation	1
1.4 - Modular design	1
1.5 - Front panel layout.....	2
1.6 - Rear panel connections.....	2
1.7 - Package contents	2
1.8 - Optional upgrades	3
1.8.1 - Timing reference options.....	3
1.8.2 - Antenna upgrades.....	3
1.8.3 - Oscillator upgrades	3
1.8.4 - Additional timing LANs	4
1.8.5 - Industrial outputs.....	4
1.8.6 - Power supply options.....	4
2 - Installation	5
2.1 - Installing the GNSS patch antenna	5
2.2 - Installing the optional anti-jam GNSS timing antenna	5
2.3 - Installing the optional lightning arrester	6
2.4 - Installing your Sync Defender in a 19" rack.....	6
2.5 - Connecting the antenna to your Sync Defender.....	6
2.6 - Dual redundant time reference	6
2.7 - Connecting to a GPS6000 system	7
2.8 - Connecting power.....	7
2.9 - Connecting the timing LAN	7
2.10 - Connecting the USB interface	7
2.11 - Optional outputs.....	7
3 - Setup and configuration	8
3.1 - Minimum setup configuration steps	8
3.2 - Guided security setup.....	8
3.3 - Setting up the time reference	8
3.3.1 - Time reference trust level.....	8
3.3.2 - Anti-jamming mode	9
3.3.3 - Time discontinuity allowance	9

3.3.4 - Oscillator steering allowance	10
3.3.5 - Antenna cable delay compensation	10
3.3.6 - GNSS constellation	10
3.3.7 - Active antenna monitoring	11
3.3.8 - Time reference sync prefer	11
3.3.9 - Feature availability	11
3.4 - Setting up the timing LAN	11
3.4.1 - Enabling DHCP on the timing LAN	11
3.4.2 - Programming static IP settings	11
3.4.3 - Enabling NTP broadcast support	11
3.5 - Setting the local time zone	12
3.6 - Holdover configuration	12
3.7 - Front panel trust level	13
3.8 - USB interface trust level	13
3.9 - Passwords & recovery pin	13
3.10 - Setting the time and date manually	13
3.11 - Seasonal summertime/wintertime changes	13
3.12 - Leap seconds	13
3.13 - Low power mode	14
3.14 - Disabling audible indications	14
3.15 - Setting the LCD contrast	14
3.16 - Restoring factory settings	14
3.17 - Optional outputs	14
3.18 - Realtime clock option	14
4 - Status and operation.....	15
4.1 - Checking the status of your Sync Defender	15
4.2 - Error and status info on the LCD	15
4.3 - System power status	15
4.4 - Time reference status	15
4.5 - System status & holdover	16
4.6 - Timing LAN status and bandwidth utilisation	16
4.7 - Expansion card status	16
4.8 - GNSS operation	16
4.9 - Holdover operation	17
4.10 - What is NTP?	17
4.11 - NTP client accuracy	17
4.12 - NTP broadcast mode	17
4.13 - Viewing system information	17
4.14 - Viewing system firmware version	18
4.15 - Viewing uptime	18

4.16 - System statistics	18
5 - System security	19
5.1 - Guided security setup	19
5.2 - Front panel trust level	19
5.3 - USB interface trust level	20
5.4 - System passwords	20
5.5 - Using the password recovery pin	21
5.6 - Time reference trust level	21
5.7 - Timing LAN security	22
6 - Remote access	23
6.1 - Remote access via the timing LAN	23
6.2 - Remote serial port access	23
6.3 - Accessing the Sync Defender via USB	23
7 - Optional outputs	24
7.1 - Ethernet timing LAN card	24
7.2 - RS-232 output	24
7.2.1 - Connecting to the RS-232 output	24
7.2.2 - RS-232 data message format	24
7.2.3 - RS-232 transmission parameters	24
7.2.4 - RS-232 time zone	25
7.2.5 - RS-232 serial port PPS output	25
7.2.6 - Checking the status of the RS-232 card	26
7.3 - RS-485 output	26
7.3.1 - Connecting to the RS-485 output	26
7.3.2 - RS-485 data message format	26
7.3.3 - RS-485 transmission parameters	27
7.3.4 - RS-485 time zone	27
7.3.5 - Checking the status of the RS-485 card	27
7.4 - PPS output	28
7.4.1 - Connecting to the PPS output	28
7.4.2 - Configuring the PPS output	28
7.4.3 - Checking the status of the PPS output card	28
7.5 - IRIG-B output	28
7.5.1 - Connecting to the IRIG-B output	28
7.5.2 - Checking the status of the IRIG-B output card	28

A - Specifications	29
A.1 - Model variations and option codes.....	29
A.2 - Performance specifications	30
A.3 - Mechanical specifications and approvals.....	31
B - Menu structure	32
C - Serial formats	33
D - Time zones	34
E - Firmware updates	36
F - Troubleshooting	37
G - Revision history	38
Index	39

1 - Introduction

1.1 - Introducing Sync Defender

Sync Defender is the ideal solution for secure synchronised timing on computer networks. Available with one to five timing LAN ports, Sync Defender enables secure synchronised dependable timing on up to five separate physical networks.

1.2 - How Sync Defender enhances the security of your network

Sync Defender enhances the security of your network providing a trusted stable stratum 1 NTP time source behind your firewall. Sync Defender helps safeguard the integrity of your systems with its security hardened design. It incorporates a proprietary network stack built from the ground up to provide secure stable timing. As a result of this intentional design methodology, the timing LAN ports only implement the essential protocols needed for timing.

Sync Defender further strengthens the resilience of your network by offering a choice of reference inputs, antenna upgrades and enhanced holdover performance oscillators.

1.3 - Simplified theory of operation

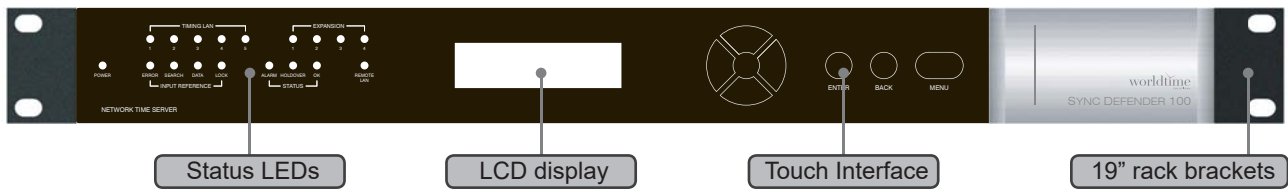
Sync Defender acquires stable and secure time data from Global Navigation Satellite Systems (GNSS). Once data has passing strict error checking, a dedicated security-hardened timing LAN then serves this time data to devices on your network.

1.4 - Modular design

Sync Defender allows you to future-proof your system architecture with its scalable modular design. You can easily add additional LAN cards as your network grows, allowing you to securely synchronise up to five separate physical networks.

A range of optional expansion cards are also available, enabling secure synchronisation of your network with industrial systems and other equipment.

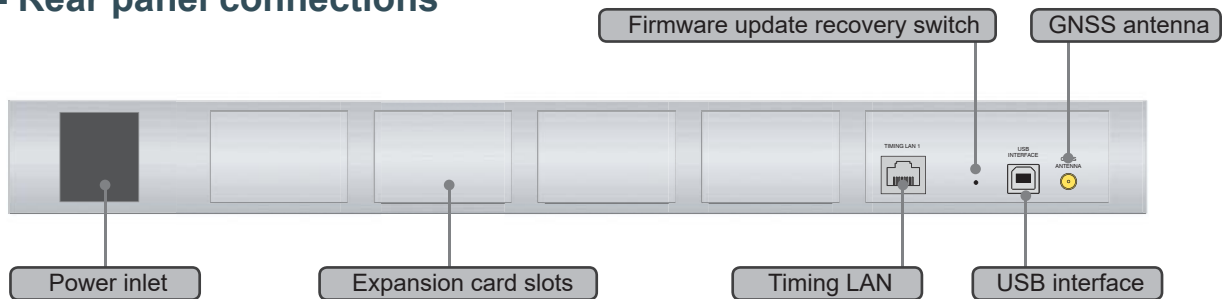
1.5 - Front panel layout



LED marking	Function
POWER	Indicates system power status
TIMING LAN	Timing LAN link and data status
EXPANSION	Expansion card output status
ERROR	Input reference error detected
SEARCH	Input reference unsynchronised
DATA	Input reference data received
LOCK	Input reference locked
ALARM	System alarm
HOLDOVER	System running in holdover mode
OK	System OK

Table 1.1 - Status LEDs

1.6 - Rear panel connections



1.7 - Package contents

Your Sync Defender is supplied with the following accessories:

- Power cord
- 19" rack mount brackets and fixing screws
- Ethernet patch cable
- USB cable
- GNSS patch antenna
- Quick start guide

1.8 - Optional upgrades

1.8.1 - Timing reference options

Sync Defender is available with a flexible choice of time reference options. The SD-101-GNSS decoder cards provides multi-constellation GNSS support. With 32 satellite parallel tracking and class-leading high-performance design, the SD-101-GNSS synchronises Sync Defender to within 30 nsec of UTC. The SD-101-GNSS card incorporates anti-jamming technology and offers selectable support for GPS, GLONASS and Galileo. The card provides real time diagnostics, active antenna monitoring and user programmable cable delay compensation. A SD-101-GNSS decoder card is fitted to all standard configuration Sync Defender models.

Sync Defender enables you to strengthen the resilience of your network by adding a second SD-101-GNSS card as a dual redundant live backup. Depending on your specific needs, the second card can be configured as an identical live backup, or you can choose to configure each card to use a different GNSS constellation.

The SD-102-EXT external time reference interface card adds support for a GPS6000 system. By moving the RF decoding from within the Sync Defender to a remote GPS6000 system, the majority of the antenna cable link can be made using existing structured cabling, rather than dedicated RF coaxial cables. In large buildings, this can reduce installation costs and simplify the installation process significantly.

1.8.2 - Antenna upgrades

The SD-105-ANT high gain anti-jam timing antenna can be installed in place of the standard GNSS patch antenna. This antenna upgrade provides improved operation in the most demanding weak signal and hostile RF environments. You can purchase the anti-jam timing antenna with a choice of coaxial cable lengths to suit your installation needs. The SD-105-ANT high gain anti-jam timing antenna also enables the integration of a lightning arrester into your Sync Defender system. The lightning arrester protects your Sync Defender and connected networking equipment against damage from a lightning strike or surge event.

1.8.3 - Oscillator upgrades

Sync Defender is available with a choice of three oscillator upgrade options to provide improved holdover performance during periods of synchronisation loss. The SD-301-TCXO offers economical holdover performance providing stable timing during short periods of synchronisation loss. The SD-301-TCXO is fitted as standard on the Sync Defender 100 and Sync Defender 200 models. The SD-302-OCXO provides a good balance between cost and performance, offering improved holdover performance at a competitive price. The

SD-303-OCXO-HS delivers superb holdover performance, allowing Sync Defender to continue performing seamlessly during extended periods of synchronisation loss.

1.8.4 - Additional timing LANs

The SD-401-ETH timing LAN card adds an additional Ethernet port and delivers the capability to securely synchronise an additional physical network from your Sync Defender. The SD-401-ETH timing LAN card incorporates its own processor running its own security-hardened network stack. This ensures isolation between your networks and guarantees bandwidth availability on all ports. All models of Sync Defender have one timing LAN integrated onto the motherboard. The Sync Defender 200 model has one SD-401-ETH timing LAN card fitted as standard, providing two timing LANs in total. Optionally, a further three SD-401-ETH cards may be fitted, enabling Sync Defender 200 to provide secure synchronised timing on up to five separate physical networks.

1.8.5 - Industrial outputs

Sync Defender is available with a range of optional expansion cards providing high accuracy time synchronisation for industrial systems and other equipment.

- The SD-420-232 expansion card adds a serial time and date output and PPS output at RS-232 signal levels. The data can be transmitted in one of 27 different data formats.
- The SD-421-485 expansion card provides a serial time and date output as RS-485 signal levels. The serial data can be transmitted in one of 27 different data formats.
- The SD-425-PPS expansion card offers a high accuracy pulse per second (PPS) output.
- The SD-426-IRIG expansion card provides a 1KHz amplitude modulated IRIG-B timecode output.

Further expansion cards are available to special order.

1.8.6 - Power supply options

Sync Defender can be supplied with a range of power supply options, including DC power and dual redundant mains power.

2 - Installation

2.1 - Installing the GNSS patch antenna

To ensure reliable operation, the GNSS antenna needs to have at least a partial view of the sky. Increasing the amount of sky visible will improve system performance. The antenna should be mounted either externally (in a protected position) or in an internal position with a view of the sky (for example, on a window ledge).

If you choose to mount your antenna internally, best operation will be achieved by choosing a window facing towards the equator. Please ensure the window is not coated with a metallised film as this may disrupt the GNSS signals.

Having chosen a suitable installation location, secure the GNSS antenna in position using the adhesive tape supplied.

2.2 - Installing the optional anti-jam GNSS timing antenna

The optional anti-jam GNSS timing antenna should be installed externally, with the maximum possible sky visibility. For most installations, the ideal location will be the roof of your building. The antenna has been designed to withstand extreme temperatures, rain, snow and sunlight.

Ideally, the antenna should have a clear uninterrupted 360 deg view of the horizon. For installations where an unobstructed view of the sky is not practical, the antenna should be installed with as large a view as possible of the sky towards the equator. Installing the antenna with a substantially reduced view of the sky will degrade system performance and may increase synchronisation time.

The antenna should be mounted with the top of the dome facing directly upwards and secured using the antenna bracket. Care should be taken to ensure the fixings used (not supplied) as suitable for the application.

The antenna should be connected to the lightning arrester using the appropriate length TNC/TNC coaxial cable (available separately). For installations where a lightning arrester is not used, the antenna should be connected directly to the Sync Defender using the appropriate length TNC/SMA coaxial cable (available separately).

WARNING: WHEN INSTALLING THE ANTENNA WITHOUT A LIGHTNING ARRESTER, THE ANTENNA MUST NOT BE INSTALLED IN A POSITION WHERE IT MAY BE SUBJECTED TO A DIRECT LIGHTNING STRIKE.

To prevent moisture penetrating the RF connection, the coaxial cable connection to the antenna should be sealed using the supplied self-amalgamating tape. The tape should fully cover the coax heat shrink and the TNC connector, and should finish on the antenna mounting thread. The tape should be supplied in successive half-lapped layers working up towards the antenna. To ensure good sealing of the RF connection, the tape should be gently stretched as applied.

2.3 - Installing the optional lightning arrester

The optional lightning arrester provides surge protection for your Sync Defender. It should be connected inline between the external antenna and the Sync Defender. The lightning arrester should be installed internally as the point where the antenna cable enters the building.

PLEASE NOTE: THE LIGHTNING ARRESTER MUST NOT BE INSTALLED EXTERNALLY.

It is important that the lightning arrester is grounded to a low impedance ground system for proper operation.

The lightning arrester is supplied with a separate instruction sheet with full installation instructions. Please consult this separate instruction sheet when installing your lightning arrester.

2.4 - Installing your Sync Defender in a 19" rack

Sync Defender is supplied with side fixing brackets to enable installation into a 1 U high 19" rack slot. To mount your Sync Defender into a 19" rack, fix the brackets to the side of the enclosure using the supplied M5 screws. The Sync Defender can then be installed into the rack using appropriate fixings.

2.5 - Connecting the antenna to your Sync Defender

Connect the antenna cable to the SMA type RF connector on the rear of your Sync Defender. The input is labelled 'GNSS ANTENNA'.

2.6 - Dual redundant time reference

If your Sync Defender has the dual redundant time reference option, both antennas should be separately installed as per the instructions above. There will be two GNSS antenna inputs on the rear of your Sync Defender. Connect an antenna to each GNSS antenna input.

2.7 - Connecting to a GPS6000 system

The SD-102-EXT external time reference interface card adds the capability to connect a remote GPS6000 system (see section 1.8.1). Please refer to the GPS6000 user manual for installation instructions.

2.8 - Connecting power

Your Sync Defender has been supplied with a power cord suitable for connection to the mains power supply in your location. Before connecting to a mains power supply, please check compatibility between your local mains power supply and the power supply rating as stated on your Sync Defender.

CAUTION! DOUBLE POLE/NEUTRAL FUSING! THE IEC MAINS POWER INLET ON THE REAR OF YOUR SYNC DEFENDER IS DOUBLE FUSED. FUSES SHOULD ONLY BE REPLACED WITH THOSE OF THE SAME TYPE/RATING AND BY QUALIFIED PERSONNEL.

If your Sync Defender has been supplied with a non-standard power option, please refer to the separate instructions provided.

2.9 - Connecting the timing LAN

The timing LAN port on your Sync Defender should be connected to an Ethernet switch on your TCP/IP network. The connection should be made using the supplied patch cable (or similar).

Please note that your Sync Defender may have multiple timing LAN ports.

2.10 - Connecting the USB interface

The USB interface enables remote configuration of your Sync Defender using the supplied Windows application. The USB interface also provides secure firmware upgrade capability.

The USB interface should be connected to a Windows PC using the supplied USB type A to type B cable.

2.11 - Optional outputs

Sync Defender is available with arrange of additional optional outputs. Please refer to chapter 7 for installation information specific to your optional output.

3 - Setup and configuration

3.1 - Minimum setup configuration steps

Once your Sync Defender has been installed, as a minimum, you should complete the following configuration steps.

- Complete the Guided Security Setup
- Setup the timing LAN
- Set the local time zone

The above steps are explained in more details in the following sections.

3.2 - Guided security setup

When you first boot your Sync Defender, the Guided Security Setup procedure will automatically run. This guides you through setting up some mandatory security settings. You will be required to select a Front Panel Trust Level, a USB Interface Trust Level and, if required, passwords and a recovery pin. You can also optionally adjust the Time Reference Trust Level. *Please refer to section 5.1 for more details.*

3.3 - Setting up the time reference

The time reference on your Sync Defender comes preconfigured with settings suitable for a typical installation. If required, these settings can be adjusted as detailed below.

3.3.1 - Time reference trust level

The Time Reference Trust Level is a simple method to configure how much you want your Sync Defender to trust its time reference. It is set as part of the Guided Security Setup procedure or alternatively can be modified in the ADVANCED SETUP > SECURITY SETTINGS menu.

When you change the Time Reference Trust Level, you are actually configuring three different Time Reference settings; the GNSS Anti-jamming Mode, the GNSS Time Discontinuity Allowance and the GNSS Oscillator Steering Allowance. Please refer to the sections below and chapter 5 for more details.

3.3.2 - Anti-jamming mode

The first time your Sync Defender is booted, it automatically performs a self-survey to calculate its location as accurately as possible. Once this survey is complete, your Sync Defender stores this location data and then switches to a fixed location mode. In fixed location mode, Sync Defender uses data from one satellite vehicle only. This provides the most stable and accurate time data, but leaves the system vulnerable to GNSS spoofing.

With anti-jamming mode enabled, Sync Defender compares data from two satellite vehicles. This greatly reduces the vulnerability to GNSS spoofing, whilst still enabling highly accurate timing. Your Sync Defender is supplied with GNSS anti-jamming mode enabled. This setting can be disabled in the ADVANCED SETUP > TIME REFERENCE menu. However, for most installations, we would advise this setting should not be changed.

Note that the GNSS anti-jamming mode is also configured automatically as part of the time reference trust level (*see above and section 5.6*).

3.3.3 - Time discontinuity allowance

The Time Discontinuity Allowance is a function to limit the maximum time jump your Sync Defender will accept from a time reference source after initial synchronisation is complete. Three settings are available. In ANY mode, Sync Defender will accept any time jump and resync to the new time. In SMALL CHANGE ONLY mode, time jumps are limited to less than one second. In NO CHANGE mode, the time cannot jump.

Time discontinuity allowance	Maximum time jump
ANY	No limit to allowed time jumps
SMALL CHANGE	Time jumps limited to less than one second
NO CHANGE	Time jumps not permitted

Table 3.1 - Time discontinuity allowance

If the time reference jump is outside the allowed range, Sync Defender will switch to holdover mode and flag an alarm. The Time Discontinuity Allowance can be modified in the ADVANCED SETUP > TIME REFERENCE menu. Note that the Time Discontinuity Allowance is also configured automatically as part of the time reference trust level (*see above and section 5.6*).

Please note that the availability of this feature is partially dependent on the specific oscillator option fitted to your Sync Defender and may not be configurable on your unit.

3.3.4 - Oscillator steering allowance

All versions of Sync Defender have adjustable oscillators that enable the system to make small changes to its own clock frequency and maintain synchronisation with its time reference. This trimming prevents small time discontinuity issues and ensures timestamps are contiguous. The Oscillator Steering Allowance is a function to limit the maximum adjustment the Sync Defender can make to its oscillator frequency. Two options are available. As standard, the Oscillator Steering Allowance is set to FULL STEERING. In TIGHT LIMIT STEERING mode, the adjustment range of the oscillator is highly restricted. If the time reference attempts to steer the oscillator outside the allowed range, Sync Defender will switch to holdover mode and flag an alarm.

The Oscillator Steering Allowance can be modified in the advanced setup > time ref menu. Note that the Oscillator Steering Allowance is also configured automatically as part of the time reference trust level (*see above and section 5.6*).

Please note that this feature relies heavily on the stability of the oscillator in your Sync Defender. Tight limit steering can only be enabled on models fitted with an OCXO oscillator. In addition, we would advise that this feature only be adjusted as part of the time reference trust level.

3.3.5 - Antenna cable delay compensation

Your Sync Defender is capable of providing time data accurate to within 30 nsec of UTC. At this level of accuracy, talking account of cable lengths becomes critical. Every metre of cable between the GNSS antenna and your Sync Defender causes an additional error of approximately 5 nsec. For longer cable lengths, this accumulated error can become very significant.

If you are using your Sync Defender for a high accuracy application, for example with the optional PPS (pulse per second) output card, you may wish to add a correction for errors due to cable propagation delays.

Once the total antenna cable length has been entered, your Sync Defender applies a time offset to correct for cable propagation delays. The antenna cable delay compensation may be set in the ADVANCED SETUP > TIME REFERENCE menu.

3.3.6 - GNSS constellation

Sync Defender supports multiple GNSS constellations; GPS, GLONASS and Galileo. As standard, your Sync Defender is programmed to operate from the GPS constellation only. If required, this can be adjusted in the ADVANCED SETUP > TIME REFERENCE menu.

3.3.7 - Active antenna monitoring

The GNSS RF input on your Sync Defender incorporates open/short monitoring and active short circuit protection. If required, the monitoring feature can be disabled in the ADVANCED SETUP > TIME REFERENCE menu. Please note that disabling active antenna monitoring only disables the notifications. The active short circuit protection cannot be disabled.

3.3.8 - Time reference sync prefer

If your Sync Defender has dual time references fitted, the Time Reference Sync Prefer feature allows you to select which sync source is the default. This setting can be adjusted in the ADVANCED SETUP > TIME REFERENCE menu.

3.3.9 - Feature availability

Some of the above features may not be present on your Sync Defender if you have an alternative time reference option fitted. If your Sync Defender has dual time references, some of the above features will be duplicated.

3.4 - Setting up the timing LAN

If your Sync Defender has multiple timing LANs, the following settings will be repeated for each timing LAN. An additional separate submenu is provided for each additional timing LAN.

3.4.1 - Enabling DHCP on the timing LAN

DHCP enables your Sync Defender to obtain network address settings automatically from a DHCP sever on your network. To enable DHCP support, access the SYSTEM SETUP > TIMING LAN 1 menu and set DHCP to ENABLED.

With DHCP enabled, the IP ADDRESS, SUBNET MASK and GATEWAY screens will show the IP settings obtained from the DHCP sever.

3.4.2 - Programming static IP settings

Access the SYSTEM SETUP > TIMING LAN 1 menu and ensure DHCP is set to disabled. The IP address, subnet and gateway settings can then be adjusted using the multi-function switches.

3.4.3 - Enabling NTP broadcast support

In a typical computer network, NTP operates in Unicast mode; an NTP client requests the time and the Sync Defender responds directly to this request. However, in certain applications, it may be desirable to configure the Sync Defender to operate in NTP broadcast mode.

When operating in NTP broadcast mode, as well as responding

directly to Unicast requests, Sync Defender additionally broadcasts NTP messages to all devices on the local subnet. Broadcast messages are transmitted every 64 seconds. NTP broadcast mode can be enabled via the SYSTEM SETUP > TIMING LAN 1 menu.

3.5 - Setting the local time zone

Sync Defender maintains a time count for both UTC/GMT and local time. The UTC count is used as a reference for network timing. The local time is shown on the LCD display and can be used as a reference for the serial output option and other option cards.

Sync Defender converts between UTC and your local time automatically. Find your time zone from the preprogrammed list in appendix D then select this time zone in the SYSTEM SETUP > TIME ZONE menu. Once your Sync Defender has synchronised to GNSS satellites, your local time will be shown on the front panel display. Any seasonal summertime/wintertime changes will occur automatically.

3.6 - Holdover configuration

If the time reference in your Sync Defender loses synchronisation, Sync Defender automatically switches to HOLDOVER mode where the time count is maintained by the internal oscillator. If your Sync Defender has been in HOLDOVER mode continually for an extended period of time, the system will switch to ALARM mode. In ALARM mode, Sync Defender tells connected equipment that it is unsynchronised.

Sync Defender is available with a range of oscillator upgrade options to improve stability whilst in holdover mode. The length of time your Sync Defender will remain in holdover mode is configurable. Note that the available range is dependent on the oscillator option fitted.

The chart below shows the holdover alarm delay range for the standard Sync Defender models and oscillator options.

Model version/ oscillator option	Default holdover alarm delay	Programmable range
Sync Defender 50	5 mins	1 min - 4 hours
Sync Defender 100	2 hours	1 min - 12 hours
Sync Defender 200	2 hours	1 min - 12 hours
SD-302-OCXO	6 hours	1 min - 48 hours
SD-303-OCXO-HS	12 hours	1 min - 96 hours

Table 3.2 - Holdover alarm delay range

The holdover alarm delay can be adjusted in the ADVANCED SETUP > OSCILLATOR menu.

3.7 - Front panel trust level

The 'Front Panel Trust Level' dictates the lock-down level of the front panel touch interface. The front panel trust level is set as part of the Guided Security Setup when you first boot your Sync Defender. Alternatively, the front panel trust level can be modified in the ADVANCED SETUP > SECURITY SETTINGS menu. *Please refer to chapter 5 for more details.*

3.8 - USB interface trust level

The 'USB Interface Trust Level' dictates the lock-down level of the USB interface. The USB interface trust level is set as part of the Guided Security Setup when you first boot your Sync Defender. Alternatively, the USB interface trust level can be modified in the ADVANCED SETUP > SECURITY SETTINGS menu. *Please refer to chapter 5 for more details.*

3.9 - Passwords & recovery pin

The front panel touch interface and USB interface on your Sync Defender can be password protected to prevent unauthorised access. *Please refer to chapter 5 for more details.*

3.10 - Setting the time and date manually

If your Sync Defender has no active time reference, you can set the time and date manually via the SYSTEM SETUP > ADVANCED > UTILITIES menu. Note that the time zone must be programmed prior to adjusting the time and date (*see "Setting the local time zone" in section 3.5 above*).

3.11 - Seasonal summertime/wintertime changes

Sync Defender performs automatic seasonal summertime/wintertime changes (*see "Setting the local time zone" in section 3.5 above*).

3.12 - Leap seconds

The average rotational speed of the earth is very slowly decreasing and therefore the average length of a solar day is very slowly increasing. Leap seconds are occasionally added to the UTC time count to ensure alignment with solar day observations.

Your GNSS synchronised Sync Defender performs leap seconds automatically. However, if your Sync Defender has no active GNSS time reference, you can manually program a leap second via the

SYSTEM SETUP > ADVANCED > UTILITIES menu. The leap second can be positive (where a second is added) or negative (where a second is removed). If programmed, the leap second event will occur once only at the end of the following June or December (whichever occurs first) and then be erased.

3.13 - Low power mode

When low power mode is enabled, Sync Defender switches off the LCD display backlight after a short period of touch switch inactivity. Low power mode can be enabled in the SYSTEM SETUP > ADVANCED > UTILITIES menu.

3.14 - Disabling audible indications

Your Sync Defender produces audible switch press confirmation sounds to improve usability. If preferred, these audible switch press confirmation sounds can be disabled in the SYSTEM SETUP > ADVANCED > UTILITIES menu.

Sync Defender produces audible alarm notifications. These can also be adjusted in the SYSTEM SETUP > ADVANCED > UTILITIES menu.

3.15 - Setting the LCD contrast

The LCD contrast may be adjusted to help improve display visibility at different viewing angles. The LCD contrast can be adjusted in the SYSTEM SETUP > ADVANCED > UTILITIES menu.

3.16 - Restoring factory settings

Your Sync Defender can be reset to factory default settings via the Factory Reset function in the SYSTEM SETUP > ADVANCED > UTILITIES menu.

3.17 - Optional outputs

Sync Defender is available with arrange of optional output cards. *Please refer to chapter 7 for setup details.*

3.18 - Realtime clock option

The Realtime clock option allows your Sync Defender to maintain a time count during periods of power failure. Power-on behaviour can be adjusted via the REALTIME CLOCK menu.

4 - Status and operation

4.1 - Checking the status of your Sync Defender

The front panel status LEDs provide quick and easy visual indication of the status of your Sync Defender. More detailed status information is available via the front panel LCD.

4.2 - Error and status info on the LCD

If your Sync Defender is operating normally, the front panel LCD will display the time and date. If an error mode is detected, the LCD will show the relevant error message. More detailed information can be accessed via the LIVE STATUS submenu.

4.3 - System power status

The system power status of your Sync Defender can be visually checked via the front panel POWER LED. Sync Defender is continually monitoring its internal power systems. If operation is normal, the POWER LED will be solid white. If Sync Defender detects a problem with any of the power systems, the POWER LED will flash and an error message will appear on the front panel LCD.

More detailed power status information can be accessed via the LIVE STATUS submenu.

4.4 - Time reference status

The status of the time reference in your Sync Defender can be visually checked via the front panel INPUT REFERENCE LEDs. In normal operation, the LOCK LED will be solid white and the DATA LED will flash once per second. If the time reference is not synchronised, but otherwise the system is working normally, the SEARCH and ERROR LEDs will flash and an error message will be displayed on the front panel LCD. If the system is not working normally (for example an antenna problem is detected), the ERROR LED will fast flash and an error message will be displayed on the front panel LCD.

More detailed information regarding the time reference status can be accessed via the LIVE STATUS submenu.

4.5 - System status & holdover

The operational status of your Sync Defender can be visually checked via the front panel STATUS LEDs. If the system is synchronised and operating normally, the OK LED will be solid white. If the system has lost synchronisation recently, the HOLDOVER LED will be solid white and an error message will be displayed on the front panel LCD. If the time is not set or the system has lost synchronisation for an extended period, the ALARM LED will flash and an error message will be displayed on the front panel LCD.

More detailed information regarding system status can be accessed via the LIVE STATUS submenu.

4.6 - Timing LAN status and bandwidth utilisation

The status of the timing LANs on your Sync Defender can be visually checked via the front panel TIMING LAN LEDs. If the timing LAN is connected to your network and a link detected, the relevant TIMING LAN LED will be illuminated. The TIMING LAN LED flashes as data is detected.

Any relevant error status messages regarding the timing LAN will be displayed on the front panel LCD. More detailed information regarding the timing LAN status can be accessed via the LIVE STATUS submenu. Additionally, live timing LAN bandwidth utilisation data can be displayed also accessed via the LIVE STATUS submenu.

4.7 - Expansion card status

The status of any expansion cards can be visually checked via the front panel EXPANSION LEDs. *Please refer to the relevant section of chapter 7 for details relating to your specific card.*

4.8 - GNSS operation

Sync Defender uses multiple GNSS satellite constellations to obtain accurate time and date information. GNSS systems operate at very high frequencies (in the GHz range) and rely on a line-of-sight between the satellites and the antenna. The reliable operation of the GNSS decoding in your Sync Defender is heavily dependent on sensible antenna installation. Please follow the installation instructions in chapter 2 carefully to ensure trouble-free operation.

4.9 - Holdover operation

When operating normally, Sync Defender uses GNSS satellites as a time reference. If your Sync Defender loses synchronisation with the GNSS satellites, the system automatically switches to holdover mode where the time count is maintained by the internal oscillator. The stability of your Sync Defender whilst in holdover mode is entirely dependent on the oscillator fitted to your specific unit. The length of time Sync Defender will remain in holdover mode is configurable by the user. *For more information, please refer to section 3.6.*

4.10 - What is NTP?

NTP (Network Time Protocol) is a networking protocol that enables the synchronisation of computer clocks across data networks. Sync Defender uses NTP to synchronise client devices on a local area network.

4.11 - NTP client accuracy

Sync Defender provides NTP timestamps that are typically accurate to within 30 microseconds of UTC/GMT. However, the synchronisation accuracy of your NTP clients is dependent on many additional factors. These include network architecture, utilisation, delays and jitter. On a typical network, NTP clients using a Sync Defender as an NTP reference would be expected to be synchronised to within 200 microseconds to 2 msec of UTC on a local area network.

4.12 - NTP broadcast mode

Network Time Protocol normally operates in Unicast mode. In Unicast mode, an NTP client requests the time and the Sync Defender responds directly to this request. When operating in NTP broadcast mode, as well as responding directly to Unicast requests, Sync Defender additionally broadcasts NTP messages to all devices on the local subnet. *Please refer to section 3.4 for more details.*

4.13 - Viewing system information

Detailed information regarding your Sync Defender system can be viewed in the SYSTEM SETUP > ADVANCED SETUP > SYSTEM INFO menu.

4.14 - Viewing system firmware version

The firmware version of your Sync Defender system can be viewed in the SYSTEM SETUP > ADVANCED SETUP > SYSTEM INFO menu.

4.15 - Viewing uptime

The uptime of your Sync Defender can be viewed in the STATISTICS menu.

4.16 - System statistics

Detailed statistics data can be viewed in the STATISTICS menu.

5 - System security

Your Sync Defender incorporates a range of security features, most of which are preconfigured and running transparently in the background without any input from the user. However, there are some additional security features which are programmable by the user. Some of these features must be actively selected by the user. Others come preconfigured, but may be adjusted if required. This chapter details these user programmable security features.

5.1 - Guided security setup

Sync Defender incorporates some programmable security features that must be set by the user. When you first boot your Sync Defender, the guided security setup procedure will prompt you to actively select these mandatory settings. You will be guided through setting a Front Panel Trust Level, a USB Interface Trust Level and, if required, passwords and a recovery pin. You can also optionally adjust the Time Reference Trust Level.

Your Sync Defender will not operate until the guided security setup procedure has been completed.

5.2 - Front panel trust level

Sync Defender has a front panel touch interface to enable easy system setup. Depending on the physical security of your server room, it may be desirable that this interface has a level of password protection or is even fully disabled. The 'Front Panel Trust Level' dictates the lock-down level of the front panel touch interface. One of five trust levels must be actively selected by the user. The chart below details the available trust levels.

Front panel trust level	Function
5	No security
4	Password required for advanced setup
3	Password required for all setup
2	Password required for live status & stats
1	Touch interface disabled

Table 5.1 - Front panel trust levels

If your server room is locked down and secure, trust level 5 would be a good choice to allow engineers quick and easy access to your Sync Defender. For less secure environments, a lower trust level would normally be advisable.

The front panel trust level is set as part of the Guided Security Setup when you first boot your Sync Defender. Alternatively, the front panel trust level can be modified in the ADVANCED SETUP > SECURITY SETTINGS menu.

5.3 - USB interface trust level

Sync Defender has USB connection to enable configuration and firmware updates. Depending on the physical security of your server room, it may be desirable that the USB interface is password protected. The 'USB Interface Trust Level' dictates the lock-down level of the USB interface. One of five trust levels must be actively selected by the user. The chart below details the available trust levels.

USB interface trust level	Function
5	No security
4	Password required for advanced setup
3	Password required for all setup
2	Password required for live status & stats
1	USB interface disabled

Table 5.2 - USB interface trust levels

If your Sync Defender is located in a secure environment, trust level 5 would be a good choice to allow engineers easy access to your Sync Defender. For less secure environments, a lower trust level may be more suitable.

The USB Interface Trust Level is set as part of the Guided Security Setup when you first boot your Sync Defender. Alternatively, the USB Interface Trust Level can be modified in the ADVANCED SETUP > SECURITY SETTINGS menu.

5.4 - System passwords

Sync Defender can only be configured via two methods; 1) the front panel touch switches and 2) the USB interface. If required, access to both of these interfaces can be password protected or even fully disabled.

When you first boot your Sync Defender, the guided security setup procedure will prompt you to select a Front Panel Trust Level and a USB Interface Trust Level. If either of these settings are set to any level other than the highest setting (trust level 5), you will be prompted to enter a password. The front panel password and USB interface password are both unique, but can be the same password if you wish.

Both the front panel password and USB interface password can

be modified or the relevant trust levels adjusted in the ADVANCED SETUP > SECURITY SETTINGS menu.

When setting a password, you will also need to enter a recovery pin. The recovery pin enables either password to be reset if required.

5.5 - Using the password recovery pin

If a password has been mislaid, the password can be reset and access to your Sync Defender restored via the password recovery pin. The recovery pin is entered using the front panel touch interface via the ADVANCED SETUP > SECURITY SETTINGS menu. Alternatively, if your Sync Defender is set to a low trust level and access to the advanced setup menu is restricted, follow the on-screen prompts to recover the password and enter the recovery pin.

5.6 - Time reference trust level

Sync Defender incorporates many features to ensure secure synchronised timing on your network. However, any time server is always reliant on the operation of its time reference to be able to provide stable timing. The Time Reference Trust Level is a simple method to configure how much you want your Sync Defender to trust its time reference.

When you change the Time Reference Trust Level, you are actually configuring three different Time Reference settings; the GNSS Anti-jamming Mode, the GNSS Time Discontinuity Allowance and the GNSS Oscillator Steering Allowance. These three settings all have a direct effect on the security of the Sync Defender system timing. For most installations, selecting one of the five Time Reference Trust Levels would be the most optimal way to configure your Sync Defender. However, the three settings can be manually adjusted if required. *Please refer to chapter 3 for more details.*

The chart below details the five Time Reference Trust Levels.

Time reference trust level	Anti-jamming mode	Time discontinuity allowance	Oscillator steering allowance
5	DISABLED	ANY	FULL
4	ENABLED	ANY	FULL
3 (TCXO / OCXO)	ENABLED	SMALL CHANGE	FULL
2 (TCXO / OCXO)	ENABLED	NO CHANGE	FULL
1 (OCXO only)	ENABLED	NO CHANGE	TIGHT ONLY

Table 5.3 - Time reference trust levels (model dependent)

Sync Defender comes preset with the Time Reference Trust Level set to level 4. This is a good choice for most installations. It includes GNSS anti-jamming and spoofing support, but otherwise fully trusts the time reference.

However, there are situations in which it may be advisable to select a lower trust level. For example, for more mission critical applications, trust level 1 would give you much tighter control over the time on your network. In normal operation, the oscillator in your Sync Defender would be steered by the time reference, but only within very tight limits. If the time reference jumps in time, or tries to steer the oscillator frequency too far, your Sync Defender will switch to holdover mode and flag an alarm.

The Time Reference Trust Level also provides flexibility on dual sync input systems, where each sync input has its own trust level setting. For the main time reference, you may wish to trust a certain GNSS constellation completely but with anti-spoofing capability (trust level 4). The second time reference could be configured to use a different backup constellation with a lower trust level (trust level 1, where time jumps aren't allowed and steering is within tight fixed limits). This provides a good balance between time reference redundancy and security of your timing. If your preferred GNSS system fails, you still get backup timing, but are not trusting this without question.

Please note that the lower settings rely on the stability of the oscillator and as such are not available on all Sync Defender models. The strictest setting (Time Reference Trust Level 1) is only available on models with an OCXO oscillator.

The Time Reference Trust Level can be adjusted as part of the Guided Security Setup when you first boot your Sync Defender. Alternatively, the Time Reference Trust Level can be modified in the ADVANCED SETUP > SECURITY SETTINGS menu.

5.7 - Timing LAN security

The timing LAN on your Sync Defender is powered by a proprietary network stack built from the ground up to provide secure stable timing. The security hardened design of the timing LAN ensures that only the essential protocols needed for timing are supported. It is not possible to access or configure Sync Defender via the timing LAN. Security features implemented by the timing LAN cannot be disabled or adjusted by the user.

6 - Remote access

Sync Defender is purposely designed to provide a secure time solution for your network. Remote access to Sync Defender is intentionally highly locked down.

6.1 - Remote access via the timing LAN

It is not possible to remotely access or configure any settings via the timing LAN.

6.2 - Remote serial port access

The optional RS-232 and RS-485 serial ports on your Sync Defender transmit time and date data in one of 27 different serial formats. It is not possible to access Sync Defender or configure any settings remotely via the serial port.

6.3 - Accessing the Sync Defender via USB

Sync Defender has a dedicated USB connection to enable configuration and firmware updates. If required, this connection can be password protected (*see chapter 5 for more details*).

7 - Optional outputs

7.1 - Ethernet timing LAN card

The optional SD-401-ETH Timing LAN card provides an additional timing LAN for your Sync Defender. Up to four timing LAN cards may be fitted in one Sync Defender unit (model dependent). If your Sync Defender has optional SD-401-ETH timing LAN cards fitted, additional Timing LAN submenus will appear in the SYSTEM SETUP menu. The setup and operation of the SD-401-ETH timing LAN is identical to the onboard timing LAN fitted to all models of Sync Defender. Please refer to earlier chapters for installation and configuration details.

7.2 - RS-232 output

The optional SD-420-232 RS-232 expansion card provides a serial data output and PPS (pulse per second) output at RS-232 signal levels. If your Sync Defender has the optional RS-232 output card fitted, additional submenus will appear in the SYSTEM SETUP menu.

7.2.1 - Connecting to the RS-232 output

The RS-232 serial output option has a female DB-9 (DE-9) D-Sub (DTE) connector. Table 7.1 shows the pin connections.

Pin	Signal	Source	Description
1	PPS	Output	Pulse Per Second
2	TXD	Output	Transmitted data
3	RXD	Input	Received data
5	GND	Input	Signal ground
4, 6 - 9	unused	-	-

Table 7.1 - SD-420-232 option card RS-232 serial port pin connections

7.2.2 - RS-232 data message format

RS-232 serial data is transmitted in one of 27 different formats. The message format can be adjusted in the SYSTEM SETUP > SERIAL PORT menu. Available message formats are listed in appendix C.

7.2.3 - RS-232 transmission parameters

RS-232 messages can be transmitted at various different baud rates and with different numbers of data bits, stop bits and parity settings. All of these parameters can be adjusted by the user in the SYSTEM SETUP > SERIAL PORT menu. Table 7.2 lists the available

transmission parameters.

RS-232 data messages are transmitted aligned with the second edge. The serial port can be user-programmed to output an RS-232 data string every second, or periodically.

When set to the 'on demand' repetition rate, the serial port will only output serial data on receipt of a valid transmission request character. Valid characters are 's' (0x73), 'S' (0x53), 't' (0x74), 'T' (0x54) and '?' (0x3f). The data transmission starts on the second edge after a valid request character has been received.

Serial Output Menu Option	Description Of Function	Available options
Message format	Format of RS-232 data messages.	Please refer to appendix C
Baud rate	Data transmission speed (bits per second)	1200, 2400, 4800, 9600, 19200
Data bits	Number of data bits	7, 8
Parity	Error checking	none, odd, even
Stop bits	Number of stop bits	1, 2
Repetition rate	Time period between message transmissions	1 sec, 1 min, 5 mins, 1 hr, 24 hours (at 00:00), 24 hours (at 03.30), on demand
Serial port time zone	Time & date to which the RS-232 output is referenced	local, utc

Table 7.2 - SD-420-232 option card RS-232 output options

7.2.4 - RS-232 time zone

As standard, the serial port transmits RS-232 time and date information referenced to the local time zone (*please refer to section 3.5 for further details*). If required, RS-232 data can be referenced to UTC by adjusting the 'Serial port time zone' in the SERIAL PORT setup menu.

7.2.5 - RS-232 serial port PPS output

The RS-232 level PPS output is configured via the SYSTEM SETUP > PPS OUTPUT menu.

PPS Output Menu Option	Description Of Function	Available options
PPS output polarity	The polarity of the RS-232 PPS output pulse	standard, inverted, disabled
PPS pulse width	Length of each PPS pulse	20 msec, 100 msec, 200 msec

Table 7.3 - SD-420-232 option card RS-232 PPS output menu options

PPS (pulse per second) data is available on pin 1 of the RS-232 output port. When enabled, the PPS pin provides a short pulse every second, aligned with the second edge. PPS data is transmitted at RS-232 signal levels.

When set to standard output polarity, the pin is normally at a negative voltage level (RS-232 logic state 1). At the start of the second edge, the pin switches to a positive voltage level (RS-232 logic state 0). After the PPS pulse has ended, the pin switches back to a negative voltage level.

When set to inverted operation, pin polarity is the opposite of standard operation (normally held at logic state 0, switching to logic state 1 at the second edge).

The width of the PPS pulse may be adjusted from 20 msec to 200 msec.

7.2.6 - Checking the status of the RS-232 card

The status of the RS-232 output card can be visually checked via the relevant front panel EXPANSION LED. If the card is detected, the LED will be illuminated. As the card is outputting data, the LED will flash.

7.3 - RS-485 output

The optional SD-421-485 RS-485 expansion card provides a serial data output at RS-485 signal levels. If your Sync Defender has the optional RS-485 output card fitted, an additional SERIAL PORT submenu will appear in the SYSTEM SETUP menu.

7.3.1 - Connecting to the RS-485 output

The RS-485 serial output option has a three pin terminal block connector. Table 7.4 shows the pin connections.

Label	Source	Description
A	Output	RS-485 data A (non-inverting)
B	Output	RS-485 data B (inverting)
GND	-	Ground ref.

Table 7.4 - SD-421-485 option card RS-485 serial port pin connections

7.3.2 - RS-485 data message format

RS-485 serial data is transmitted in one of 27 different formats. The message format can be adjusted in the SYSTEM SETUP > SERIAL PORT menu. Available message formats are listed in appendix C.

7.3.3 - RS-485 transmission parameters

RS-485 messages can be transmitted at various different baud rates and with different numbers of data bits, stop bits and parity settings. All of these parameters can be adjusted by the user in the SYSTEM SETUP > SERIAL PORT menu. Table 7.5 lists the available transmission parameters.

RS-485 data messages are transmitted aligned with the second edge. The serial port can be user-programmed to output an RS-485 data string every second, or periodically.

When set to the 'on demand' repetition rate, the serial port will only output serial data on receipt of a valid transmission request character. Valid characters are 's' (0x73), 'S' (0x53), 't' (0x74), 'T' (0x54) and '?' (0x3f). The data transmission starts on the second edge after a valid request character has been received.

Serial Output Menu Option	Description Of Function	Available options
Message format	Format of RS-485 data messages.	Please refer to appendix C
Baud rate	Data transmission speed (bits per second)	1200, 2400, 4800, 9600, 19200
Data bits	Number of data bits	7, 8
Parity	Error checking	none, odd, even
Stop bits	Number of stop bits	1, 2
Repetition rate	Time period between message transmissions	1 sec, 1 min, 5 mins, 1 hr, 24 hours (at 00:00), 24 hours (at 03.30), on demand
Serial port time zone	Time & date to which the RS-485 output is referenced	local, utc

Table 7.5 - SD-421-485 option card RS-485 output options

7.3.4 - RS-485 time zone

As standard, the serial port transmits RS-485 time and date information referenced to the local time zone (*please refer to section 3.5 for further details*). If required, RS-485 data can be referenced to UTC by adjusting the 'Serial port time zone' in the SERIAL PORT setup menu

7.3.5 - Checking the status of the RS-485 card

The status of the RS-485 output card can be visually checked via the relevant front panel EXPANSION LED. If the card is detected, the LED will be illuminated. As the card is outputting data, the LED will flash.

7.4 - PPS output

The optional SD-425-PPS Pulse Per Second expansion card provides a high accuracy PPS (pulse per second) output. If your Sync Defender has the optional PPS output card fitted, an additional PPS OUTPUT submenu will appear in the SYSTEM SETUP menu.

7.4.1 - Connecting to the PPS output

The PPS output is available on the rear BNC connector and is output at TTL levels into 50 ohms.

7.4.2 - Configuring the PPS output

The PPS output is configured via the SYSTEM SETUP > PPS OUTPUT menu.

PPS Output Menu Option	Description Of Function	Available options
PPS output polarity	The polarity of the PPS output pulse	standard, inverted, disabled
PPS pulse width	Length of each PPS pulse	20 msec, 100 msec, 200 msec

Table 7.3 - SD-425-PPS option card PPS output menu options

7.4.3 - Checking the status of the PPS output card

The status of the PPS output card can be visually checked via the relevant front panel EXPANSION LED. If the card is detected, the LED will be illuminated. As the card is outputting data, the LED will flash.

7.5 - IRIG-B output

The optional SD-426-IRIG output expansion card provides a 1KHz amplitude modulated IRIG-B timecode output. If your Sync Defender has the optional IRIG-B output card fitted, an additional IRIG-B OUTPUT submenu will appear in the SYSTEM SETUP menu.

7.5.1 - Connecting to the IRIG-B output

The IRIG-B output is available on a rear BNC connector. The output is a 3V p-p into 50 ohms

7.5.2 - Checking the status of the IRIG-B output card

The status of the IRIG-B output card can be visually checked via the relevant front panel EXPANSION LED. If the card is detected, the LED will be illuminated. As the card is outputting data, the LED will flash.

A - Specifications

A.1 - Model variations and option codes

Model Variations:	
Sync Defender 50:	1 timing LAN, GNSS support
Sync Defender 100:	1 timing LAN, TCXO, GNSS support
Sync Defender 200:	2 timing LANs, TCXO, GNSS support

Time Reference Options:	
SD-101-GNSS:	Multi-constellation GNSS decoder card
SD-102-EXT:	External time reference interface card
SD-103-RTC:	Realtime clock module

Oscillator Options:	
SD-301-TCXO:	TCXO oscillator
SD-302-OCXO:	OCXO oscillator
SD-303-OCXO-HS:	High stability OCXO oscillator

Output Options:	
SD-401-ETH:	Timing LAN card
SD-420-232:	RS-232 expansion card
SD-421-485:	RS-485 expansion card
SD-425-PPS:	Pulse per second output expansion card
SD-426-IRIG:	IRIG-B timecode output expansion card

Dual Redundant Mains / DC Power Input Options:	
SD-501-DUAL-MAINS:	Dual redundant mains power
SD-502-DC-9-36:	9-36V DC power supply
SD-503-DC-NEG-48:	Negative 48V DC power

Antenna Options, Cables and Accessories:	
SD-105-ANT:	High-gain anti-jam timing antenna
SD-106-BRK:	L bracket for timing antenna
SD-107-SRG:	Standard lightning arrester
SD-108-SRG-PLUS:	Advanced lightning arrester
SD-201-TT03:	3m TNC-TNC antenna / arrester cable
SD-202-TT10:	10m TNC-TNC antenna / arrester cable
SD-203-TT25:	25m TNC-TNC antenna / arrester cable
SD-211-TS03:	3m TNC-SMA arrester / SD cable
SD-212-TS10:	10m TNC-SMA arrester / SD cable
SD-213-TS25:	25m TNC-SMA arrester / SD cable

A.2 - Performance specifications

Timing LAN Specifications:	
Supported protocols:	NTP v2/v3/v4, SNTP v3/v4, DHCP
NTP performance:	5000 NTP packets per sec (each port)
NTP timestamp accuracy:	Within 30 μ sec of internal timebase
Link speed:	10Base-T / 100Base-TX auto-sensing

Holdover Performance (at 20 °C, after 24 hours GPS sync):	
SD-301-TCXO:	2 msec per day
SD-302-OCXO:	500 μ sec per day
SD-303-OCXO-HS:	75 μ sec per day

Firmware Update Port:	
Update port:	USB spec. 2.0 compliant type B full speed

Internal GNSS decoder (version SD-101-GNSS) Specifications:	
GNSS engine:	32 satellite parallel tracking
GNSS constellations:	GPS, GLONASS, Galileo
Min. acquisition sensitivity:	-148dBm (cold start)
Min. tracking sensitivity:	-160dBm
Synchronised accuracy:	30 nsec (1 sigma)
RF input:	SMA connector

Front Panel:	
Display:	20 x 2 alphanumeric backlit LCD
Keypad:	Capacitive touch sensing
Status LEDs:	18 x white status LEDs

PPS Expansion Card (SD-425-PPS) Specifications:	
PPS accuracy:	50 nsec
Output:	BNC, TTL into 50 ohms

RS-232 Expansion Card (SD-420-232) Specifications:	
RS-232 data accuracy:	50 μ sec
RS-232 PPS accuracy:	1 μ sec
Connector:	DB-9 (DE-9) female D-Sub (DCE)

RS-485 Expansion Card (SD-421-485) Specifications:	
RS-485 data accuracy:	50 μ sec
Connector:	Detachable screw terminal block

IRIG-B Expansion Card (SD-426-IRIG) Specifications:	
Data format:	1KHz amplitude modulated IRIG-B
Output:	BNC, 3V p-p into 50 ohms

A.3 - Mechanical specifications and approvals

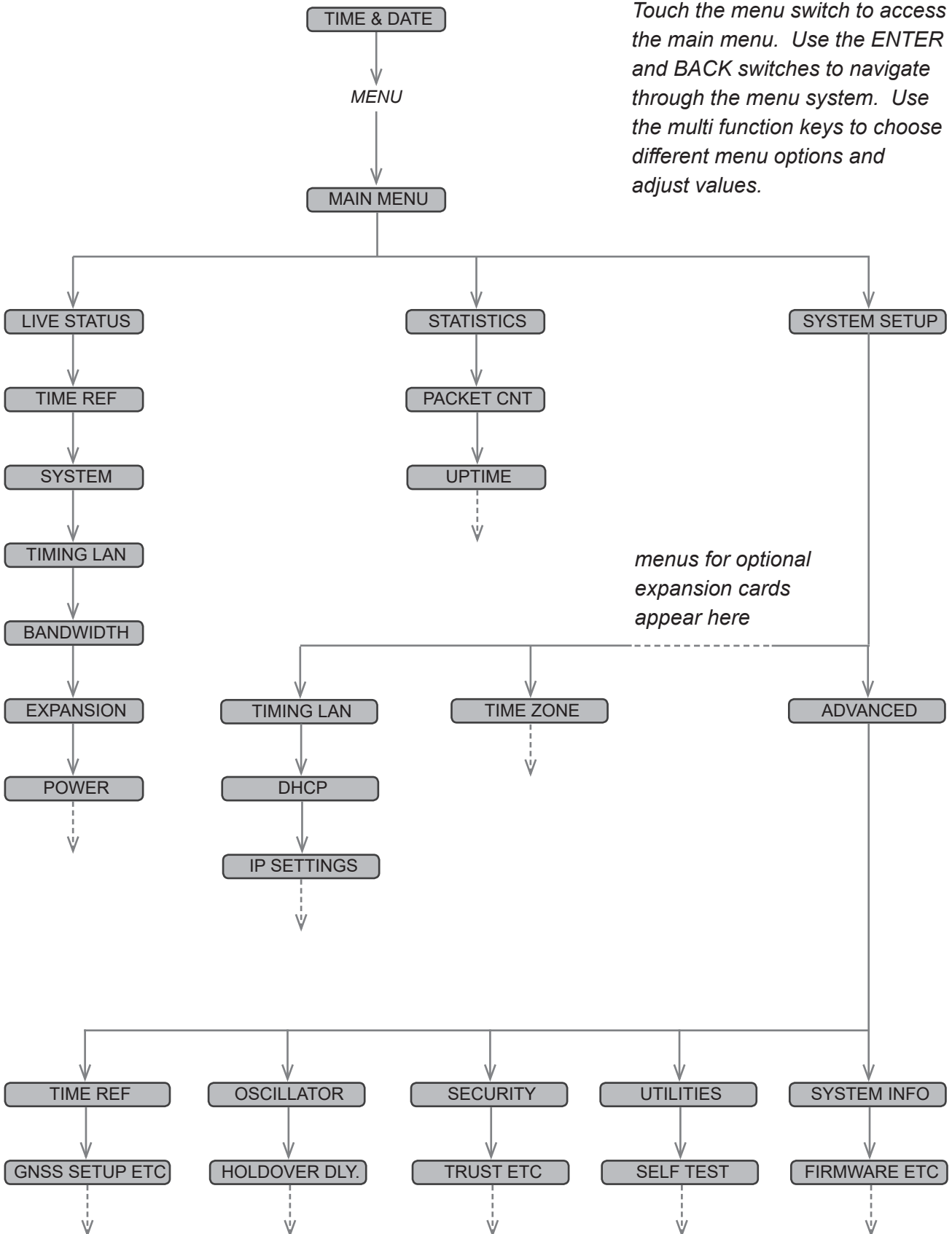
Mechanical, Electrical and Environmental Specifications:	
Enclosure dimensions:	430 x 220 x 44 mm (excl. rack brackets)
19" rack configuration:	1 U high 19" rack mounting
Enclosure weight:	3 kg
Packed weight:	4 kg
Power consumption:	< 40 watts
Power inlet:	100-250VAC 50/60Hz dble. fused IEC C14
Optional 2nd power inlet:	100-250VAC 50/60Hz dble. fused IEC C14
Operating temperature:	0 to 50 °C
Relative humidity:	0% - 95%, noncondensing
Warranty:	5 years from date of supply

Certification Approvals:	
Safety requirements:	BS EN 62368-1: 2024
Emission requirements:	BS EN 55032: 2015 +A1:2020
Immunity requirements:	BS EN 55035: 2017 +A11:2020
Radio equipment directive:	EN 303 413: V1.2.1 (2021-04)
CE / UKCA:	Meets all applicable directives
RoHS:	RoHS compliant

(Specifications subject to change without notice)

B - Menu structure

Touch the menu switch to access the main menu. Use the ENTER and BACK switches to navigate through the menu system. Use the multi function keys to choose different menu options and adjust values.



C - Serial formats

The table below lists the available message formats for the optional RS-232 and RS-485 serial ports. Please refer to chapter 7 for further details.

No.	Message format	Notes
1	World Time Solutions standard format	
2	World Time Solutions long format	
3	World Time Solutions short format	
4	NMEA GGA	
5	NMEA RMC	
6	NMEA ZDA	
7	Spectracom NetClock/2 format 0	
8	Spectracom NetClock/2 format 1	
9	Spectracom NetClock/2 format 2	
10	Spectracom NetClock/2 format 3	
11	Spectracom NetClock/2 format 4	
12	EES M100	
13	EES M201	
14	Meinberg Standard time string	
15	Computime Time String	
16	Sysplex 1	
17	Wtn. format 1	
18	Wtn. format 1 (without status)	
19	Wtn. format 2	
20	Wtn. format 2 (with day of week)	
21	Racal XGU	
22	Tecton Darlex	(03:30 & 03:31 only)
23	TAIP AL (Altitude / Vertical Velocity)	
24	TAIP CP (Compact Position)	
25	TAIP LN (Long Navigation)	
26	TAIP PV (Position / Velocity)	
27	TAIP TM (Time / Date)	

Table C.1 - Serial port message formats

D - Time zones

The table below lists the preprogrammed time zones. Time zone offsets followed by a * character indicates that the time zone has daylight saving changes.

UTC Offset	City / Time Zone
0	UTC/Reykjavik
0*	London/Dublin/Lisbon
0*	Casablanca
+1	Lagos/Algiers
+1*	CET/Paris
+2	Cape Town/Johannesburg/Harare
+2*	Athens/Sofia
+2	Cairo
+2*	Jerusalem
+2*	Beirut
+2*	Amman
+3	Khartoum/Nairobi/Baghdad
+3*	Moscow (old)
+3.5*	Tehran
+4	Dubai/Moscow
+4.5	Kabul
+5	Karachi
+5.5	Mumbai/New Delhi
+5.75	Kathmandu
+6	Almaty/Dhaka
+6.5	Yangon
+7	Bangkok/Jakarta
+8	Singapore/Hong Kong/Beijing
+8*	Perth
+9	Seoul/Tokyo
+9.5	Darwin
+9.5*	Adelaide
+10	Brisbane
+10*	Vladivostok
+10*	Melbourne/Canberra/Sydney
+11	-
+12	Suva
+12*	Kamchatka/Anadyr
+12*	Auckland
+12.75*	Chatham Island
+13	-
+14	Kiritimati

Table D.1 - Preprogrammed Time Zones

UTC Offset	City / Time Zone
-10	Honolulu
-9	-
-9*	Anchorage
-8	-
-8*	Vancouver/San Francisco
-7	Phoenix
-7*	Edmonton/Denver
-6	Guatemala/San Salvador/Managua
-6*	Winnipeg/Houston/Chicago
-6*	Mexico City
-5	Lima/Kingston/Bogota
-5*	New York/Toronto/Nassau
-5*	Havana
-4.5	Caracas
-4	Santo Domingo/La Paz/San Juan
-4*	Halifax
-4*	Santiago
-3.5*	Newfoundland
-3	-
-3*	Brasilia/Sao Paulo
-3*	Montevideo
-3	Buenos Aires
-2	-
-1	-

Table D.1 - Preprogrammed Time Zones (cont..)

E - Firmware updates

The system firmware in your Sync Defender can be updated via the USB interface using the “Sync Defender Update Tool” Windows PC software. To update the system firmware in your Sync Defender, please complete the procedure below.

- I. Download the “Sync Defender Update Tool” to your Windows PC.
- II. Run the installer and follow the on-screen prompts to install the “Sync Defender Update Tool” on your PC.
- III. Apply power to your Sync Defender and connect to your Windows PC via the USB port.
- IV. Download the new firmware release version to your Windows PC.
- V. Unzip the new firmware release version.
- VI. Run the “Sync Defender Update Tool” software.
- VII. Select the new firmware release folder.
- VIII. Click the “Install Update” button to update the firmware in your Sync Defender.

F - Troubleshooting

If you are experiencing problems with your Sync Defender, please run the hardware self-test procedure in the SYSTEM SETUP > ADVANCED > UTILITIES menu.

Problem	Possible Cause	Solution
Time synchronisation error	Time reference not synchronised	Check time reference status (<i>see section 4.4</i>) Check antenna installed correctly (<i>see chapter 2</i>)
	Cabling fault	Check time reference status (<i>see section 4.4</i>)
Not responding to NTP requests	No connection to network	Check connection to network switch/hub Check patch cable integrity
	Sync Defender time not set	Refer to Time synchronisation error section above If not using a GNSS antenna, manually set local time and date (<i>see section 3.10</i>)
Liquid crystal display hard to read	Contrast set incorrectly	Adjust LCD contrast (<i>see section 3.15</i>)
Liquid crystal display backlight switching off automatically	Low power mode enabled	Disable low power mode (<i>see section 3.13</i>)
Optional RS-232 output not functional	RS-232 output configured incorrectly	Check all RS-232 output settings (<i>see section 7.2</i>)
Optional RS-485 output not functional	RS-485 output configured incorrectly	Check all RS-485 output settings (<i>see section 7.3</i>)
Optional PPS output not working as expected	PPS output configured incorrectly	Check PPS settings (<i>see section 7.4</i>)

Table F.1 - Troubleshooting guide

G - Revision history

Version	Description	Date
1.2	Added RTC and power options. Added advanced lightning arrester option. Added holdover specs for oscillator upgrades.	Feb 2025
1.1	Amended Firmware Updates section. Updated Certifications.	Aug 2024
1.0	First release	Oct 2023

Index

Symbols

19" rack installation 6

A

active antenna monitoring 3, 11
active short circuit protection 11
ALARM LED 16
anti-jamming mode 21
anti-jamming technology 3
anti-jam timing antenna 29
audible alarm notifications 14
audible indications 14

B

baud rate 24, 25, 27

C

cable delay compensation 3, 10
cable propagation delays 10

D

data bits 24, 25, 27
DATA LED 15
DC power 4
DHCP 11
double pole/neutral fusing 7
dual redundant mains power 4
dual redundant time reference 6

E

ERROR LED 15
expansion card slots 2
expansion card status 16
EXPANSION LEDS 16, 26, 27, 28

F

factory reset 14
firmware update recovery 2
firmware updates 23, 36
firmware version 18
front panel layout 2
front panel trust level 8, 13, 19

G

Galileo (GNSS constellation) 3, 10
gateway 11
GLONASS 3, 10
GMT 12
GNSS 1
GNSS antenna 2, 5
GNSS anti-jamming mode 8, 9, 21
GNSS constellation 10
GNSS operation 16
GNSS oscillator steering allowance 21
GNSS patch antenna 2, 3
GNSS time discontinuity allowance 21
GNSS timing antenna 5
GPS 3, 10
GPS6000 system 3, 7
guided security setup 8, 13, 19, 20

H

hardware self-test 37
high stability OCXO oscillator 29
holdover 9, 10, 12, 17
holdover configuration 12
HOLDOVER LED 16

I

INPUT REFERENCE LEDs 15
IP address 11
IRIG-B timecode output 4, 28

L

LCD contrast 14
LCD display 2, 15, 16
LCD display backlight 14
leap seconds 13
lightning arrester 3, 5, 29
LIVE STATUS submenu 15, 16
local time zone 12
LOCK LED 15
low power mode 14

M

modular design 1

N

NTP 11, 12, 17
NTP broadcast 11, 12, 17
NTP client accuracy 17
NTP performance 30
NTP timestamp 17
NTP timestamp accuracy 30

O

OCXO oscillator 10, 21, 22, 29
OK LED 16
optional expansion cards 4
oscillator steering allowance 8, 10, 21
oscillator upgrades 3

P

parity 24, 25, 27
password 8, 13, 19
password recovery pin 21
patch cable 2, 7
power cord 2, 7
power inlet 2
POWER LED 15
PPS 4, 24, 26, 28
PPS output 28

PPS output polarity 28
PPS pulse width 28

Q

quick start guide 2

R

rack brackets 2
realtime clock 14, 29
real time diagnostics 3
recovery pin 8, 13, 19
remote access 23
repetition rate 25, 27
revision history 38
RF connector 6
RF input 11, 30
RS-232 4, 23, 24, 25, 26
RS-232 data message format 24
RS-232 serial port PPS output 25
RS-232 time zone 25
RS-232 transmission parameters 24
RS-485 4, 23, 26, 27
RS-485 data message format 26
RS-485 output 26
RS-485 time zone 27
RS-485 transmission parameters 27

S

SD-101-GNSS decoder card 3, 29
SD-102-EXT external time reference interface card 3, 7, 29
SD-105-ANT high gain anti-jam timing antenna 3
SD-301-TCXO 3, 29
SD-302-OCXO 3, 12, 29
SD-303-OCXO-HS 4, 12, 29
SD-401-ETH timing LAN card 4, 24, 29
SD-420-232 RS-232 expansion card 4, 24, 29, 30
SD-421-485 RS-485 expansion card 4, 26, 29, 30
SD-425-PPS PPS expansion card 4, 28, 29, 30
SD-426-IRIG IRIG-B output expansion card 4, 28, 29, 30

SEARCH LED 15
security features 19
self-amalgamating tape 6
serial data output 24
serial formats 33
serial port 23, 24, 25, 26
serial port time zone 25, 27
SMA connector 6, 30
statistics 18
STATUS LEDs 2, 15, 16
stop bits 24, 25, 27
stratum 1
subnet 11
summertime 12, 13
supported protocols 30
Sync Defender 50 12, 29
Sync Defender 100 3, 12, 29
Sync Defender 200 3, 4, 12, 29
system information 17
system passwords 20
system security 19

T

TCP/IP network 7
TCXO oscillator 21, 29
time and date (setting manually) 13
time discontinuity allowance 8, 9, 21
time reference sync prefer 11
time reference trust level 8, 19, 21, 22
time zones 34
timing LAN 1, 2, 4, 7, 11, 12, 16, 22, 23, 24, 29, 30
timing LAN bandwidth utilisation 16
TIMING LAN LEDs 16
timing LAN security 22
timing LAN status 16
timing LAN submenu 24
timing reference options 3
touch interface 2
troubleshooting 37

U

Unicast 11, 17
uptime 18
USB 23, 30
USB cable 2
USB interface 2, 7
USB interface trust level 8, 13, 19, 20
UTC 12

W

wintertime 12, 13

World Time Solutions Limited
Unit 2 Oxford Court, St James Road, Brackley, NN13 7XY, United Kingdom
+44 (0) 1280 830 380 - sales@worldtimesolutions.com
www.worldtimesolutions.com