National Semiconductor

August 1994

DP83222 CYCLONE™ Twisted Pair FDDI Stream Cipher Device

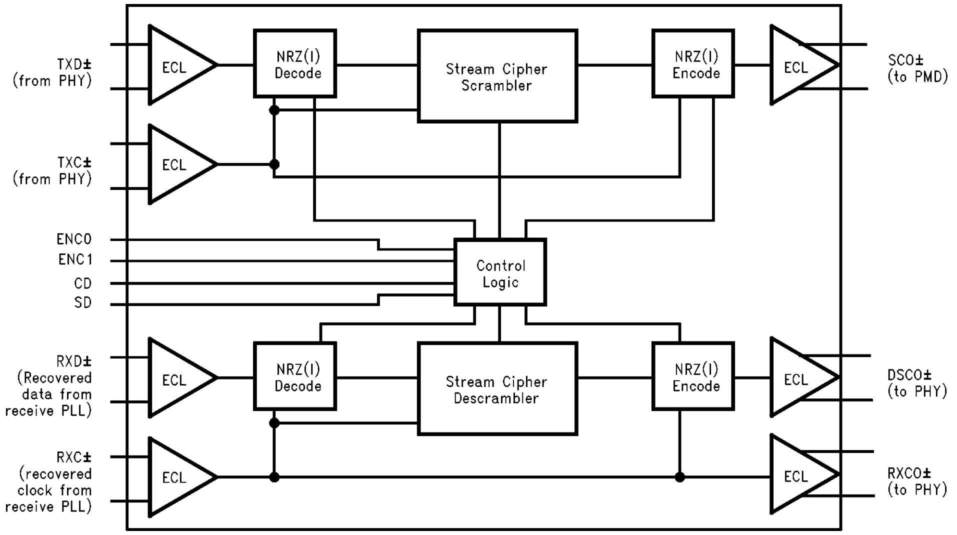
General Description

The DP83222 CYCLONE Stream Cipher Scrambler/Descrambler Device is an integrated circuit designed to interface directly with the serial bit streams of a Twisted Pair FDDI PMD. The DP83222 is designed to be fully compatible with the National Semiconductor FDDI Chip Sets, including the DP83223 TWISTER™ (Twisted Pair Transceiver). The DP83222 requires a 125 MHz Transmit Clock and corresponding Receive Clock for synchronous data scrambling and descrambling. The DP83222 is compliant with the ANSI X3T9.5 TP-PMD draft standard and is required for the reduction of EMI emission over unshielded media. The DP83222 is specified to work in conjunction with existing twisted pair transceiver signalling schemes such as MLT-3 or NRZI and enables high bandwidth transmission over Twisted Pair copper media.

Features

- Enables 100 Mbps FDDI signalling over Category 5 Unshielded Twisted Pair (UTP) cable and Type 1 Shielded Twisted Pair (STP)
- Reduces EMI emissions over Twisted Pair media
- Compatible with ANSI X3T9.5 TP-PMD Standard
- Requires a single +5V supply
- Transparent mode of operation
- Flexible NRZ and NRZI format options
- Advanced BiCMOS process
- Signal Detect and Clock Detect inputs provided for enhanced functionality
- Suitable for Fiber Optic PMD replacement applications

Block Diagram



TL/F/11885–1

FIGURE 1. DP83222 Block Diagram

1.0 Functional Description

1.1 OVERVIEW

The DP83222 Stream Cipher Scrambler/Descrambler Device consists of 7 major functional blocks as shown in *Figure 1*.

The Scrambler section is comprised of an Encoder, a Decoder, a linear Feedback Shift Register with support gates and the Control Logic block. The Decoder accepts synchronous differential clock and data (data can be either NRZ or NRZI formatted) from the Physical Layer and delivers NRZ data to the 11-bit LFSR block.

The LFSR scrambler and support gates exclusive-OR the incoming unscrambled data stream with the resultant data stream of the LFSR. This data becomes the scrambled data stream. The Encoder accepts scrambled data from the 11-bit LFSR block and delivers either NRZ or NRZI asynchronous data to the external PMD Transceiver.

The Control Logic block functions as the Encode/Decode switch, selecting NRZ or NRZI formats, and also controls the disabling of the scrambler for use in transparent mode.

The Descrambler section is comprised of an Encoder, a Decoder, the Descrambler Logic block and the Control Logic block (shared with the Scrambler section). The Encoder and Decoder blocks work in conjunction with the corresponding blocks within the Scrambler section. A truth table describing the available encode/decode format algorithms can be found in Table II.

The Stream Cipher Logic functions as a "Sample and Hold" state machine that, when in sample mode, continuously evaluates incoming words by searching for identifiable FDDI line states. When valid line states are detected, the Stream Cipher enters the hold state. During the hold state, an 11-bit LFSR operates to descramble the incoming data completing the translation. A more in-depth analysis of the stream cipher algorithm is given in Section 1.3.

The descrambled data is accompanied by a time aligned version of the descramble clock allowing for synchronous delivery of the data to the Physical Layer device.

Finally, the Control Logic block, which is shared by both the Scramble and Descramble sections, controls several functions. The Encode/Decode switch controls the selection of NRZ or NRZI conversion as well as the transparent mode of operation. Clock Detect (CD) and Signal Detect (SD) inputs, also part of the Control Logic block, control certain stream cipher logic modes.

1.2 DATA SCRAMBLING

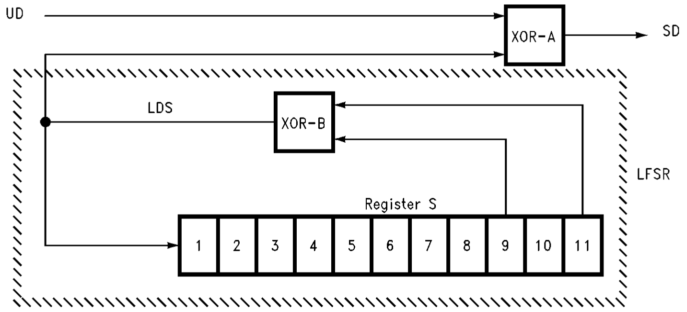
A more in-depth analysis of the scrambler function, as illustrated in *Figure 2*, reveals a fairly elementary design. The scrambler logic requires that the incoming data be NRZ formatted, which the DP83222 accomplishes via the input decoder. After being decoded to NRZ, the data, UD, is routed to one input of the Exclusive OR gate, XOR-A. The other input to XOR-A is connected to the output of a closed loop 11-bit Linear Feedback Shift Register (LFSR).

Register S includes data taps at registers 9 and 11 connected to another XOR function, XOR-B, is performed. The result of XOR-B, LDS, is then routed to the input of Register S (this circuit forms a linear feedback shift register, LFSR). LDS is also routed to the other input of XOR-A which, in turn, outputs the final scrambled data stream SD. The data sequences shown in *Figure 2* are defined as:

UD = Unscrambled Data (originating from PHY)

LDS = Scrambler LFSR Feedback data

SD = (LFSR__S xor UD)



TL/F/11885–2

FIGURE 2. Stream Cipher Scrambler Logic

1.0 Functional Description (Continued)

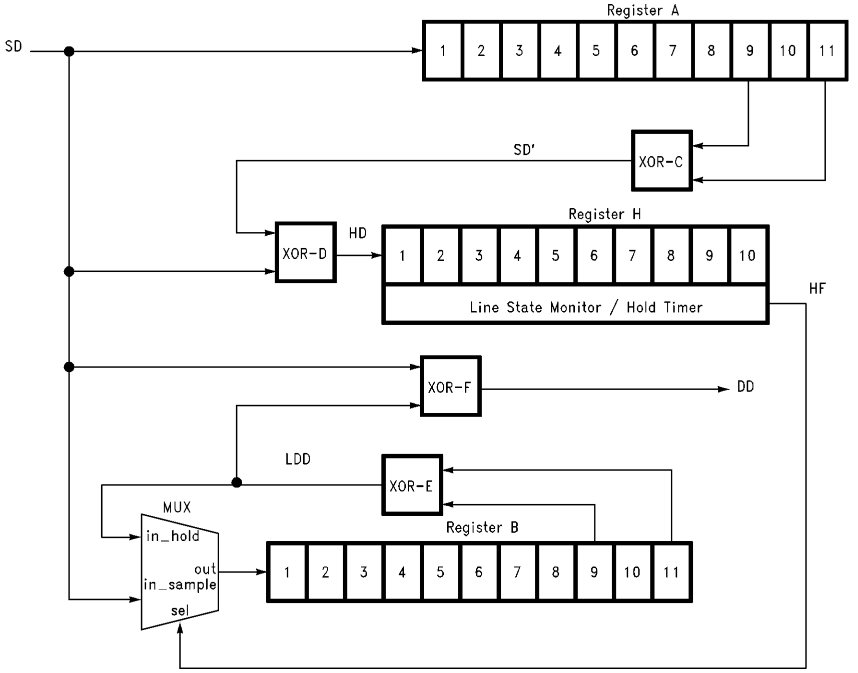
1.3 STREAM CIPHER (DATA DESCRAMBLING)

The analysis of the Stream Cipher descrambler design is somewhat more complex than the scrambler circuit shown below. The concept of the stream cipher is based upon hypothetical comparison. Because FDDI signalling includes known line states comprised of unique 5-bit patterns, it is possible to utilize these patterns as comparison information when analyzing the incoming scrambled datastream.

Four FDDI line state patterns are commonly transmitted within an FDDI ring during ring initialization and sustained ring operation. Three of these line state patterns, HALT, MASTER and QUIET, are used during PCM initialization and ring fault indication. The fourth pattern, the IDLE, is employed during PCM initialization and normal ring operation.

The stream cipher operates in two modes, Sample mode and Hold mode. While it is possible to become synchronized in the Sample mode during the reception of HALT, MASTER or QUIET patterns, synchronization is lost as soon as anything other than these patterns are received. It is only the IDLE line state that allows synchronization and assertion of the Hold mode. The Hold mode allows fully synchronized descrambling of all incoming data regardless of symbol type. The IDLE line state is both sufficient and required for assertion of the Hold mode of synchronization due to frequent interspersion among normal FDDI traffic such as Tokens and Frames.

The IDLE line state pattern will be analyzed for this example. The IDLE symbol pair, in the NRZ 5B format, becomes ten ones or 11111 11111. The analysis begins by examining the logic design provided in *Figure 3*. The NRZ scrambled data, SD, is routed to Register A which is an 11-bit serial shift register with taps at registers 9 and 11. Taps 9 and 11 are input to the XOR-C gate which outputs the SD′ datastream. SD′ is connected to one input of XOR-D. The other input to XOR-D is the original SD datastream.



TL/F/11885–3

FIGURE 3. Simplified Stream Cipher Descrambler Logic

1.0 Functional Description (Continued)

The result from XOR-D is a hypothetical data sequence, HD, that should match the original unscrambled NRZ IDLE data, barring any noise events. The Boolean progression in *Figure 4* demonstrates that HD should equal the original unscrambled IDLE bits. Over time, Register H is loaded with the hypothetical data sequence, HD.

Before the Line State Monitor detects a valid IDLE sequence (no less than 50 consecutive IDLE bits), the Stream Cipher logic remains in the Sample mode. While in Sample mode, the MUX select input ''sel'' routes the ''in_sample'' input to Register B. The MUX input ''in_sample'' is connected to the original SD datastream which continuously loads and updates Register B so that its contents dynamically match Register A. This dynamic match is important as it ensures synchronization with the LFSR in the scrambler section.

When the Line State Monitor logic within the Register H block recognizes sufficient consecutive IDLE bits, it will output a Hold Flag, HF, which controls the MUX feeding Register B. When HF becomes true, the MUX ''in_hold'' input is selected which routes the LDD data sequence back into Register B. This configures Register B and XOR-E into an LFSR (identical to that in the scrambler logic in Section 1.2). Register B, now an LFSR, is synchronized with the incoming datastream, SD, allowing XOR-F to descramble SD by a simple XOR function with LDD. To ensure continuous synchronization for valid conditions, the Hold Timer in the Register H block will hold HF true for a sufficient time until more IDLE bits can be decoded which resets the timer. The Hold Timer time-out period is based on the maximum time, under normal operation, between IDLE occurrences (>722 µs).

If IDLE symbols cease to be decoded, the Hold Timer will time out, forcing HF false. This will cause the stream cipher to fall into the sample mode again awaiting further valid line states for resynchronization.

This analysis is intended to provide a general understanding of the mechanisms involved in the stream cipher process. Some circuit details were omitted for simplification. A more detailed logical and Boolean description of the stream cipher process is generally available.

1.4 STREAM CIPHER BOOLEAN

The following Boolean analysis supports the stream cipher logic for IDLE reception example stated herein.

Given that the character ! denotes an exclusive OR function:

UD[n] = Unscrambled Data (''IDLE'' ones)
LDS[n] = Scrambler's LFSR feedback data (Pseudo Random)
SD[n] = scrambled data (LDS[n] ! UD[n])
SD′[n] = result of XOR-C
HD[n] = Hypothetical Data (SD[n] ! SD′[n])
HF = Hold Flag
LDD[n] = Descrambler LFSR feedback data
DD[n] = Descrambled Data (SD[n] ! LDD[n])

Since LDS[n] = (LDS[n-9] ! LDS[n-11])
Then SD = (UD[n] ! LDS[n])
And Since UD[n] = 1 . . . IDLE bits
Then SD[n] = $\overline{\text{LDS[n]}}$

Since SD′[n] = SD[n-9] ! SD[n-11]
And SD′[n] = ($\overline{\text{LDS[n-9]}}$! $\overline{\text{LDS[n-11]}}$)
Then SD′[n] = (LDS[n-9] ! LDS[n-11]) = LDS[n]
And Since SD[n] = $\overline{\text{LDS[n]}}$
Then HD[n] = (SD[n] ! SD′[n]) = ($\overline{\text{LDS[n]}}$! LDS[n]) = 1 . . . IDLE bits

If HF = 1 . . . due to the detection of sufficient valid IDLE symbols
And LDD[n] = LDS[n] . . . because LDD dynamically tracks LDS
And Since DD[n] = (LDS[n] ! SD) = (LDS[n] ! UD[n] ! LDS[n])
Then DD[n] = UD[n]

FIGURE 4. Stream Cipher Boolean Analysis

2.0 Pin Table

TABLE I. Pinout Summary

Signal	Pin No.	Description	Type
V_{CC}	7, 16, 28	V_{CC}	Supply
GND	1, 4, 11, 15	GND	Supply Return
$ECLV_{CC}$	21	$ECLV_{CC}$	Supply
ECLGND	22	ECLGND	Supply Return
$EXTV_{CC}$	23	External V_{CC}	Supply
RXD ±	3, 2	Received Data from PMD Receiver	Diff. 100K ECL In
RXC ±	5, 6	125 MHz Clock from Receiver PLL	Diff. 100K ECL In
TXD ±	18, 17	Transmit Data from PHY PMRD	Diff. 100K ECL In
TXC ±	13, 14	125 MHz Clock from PHY	Diff. 100K ECL In
SCO ±	19, 20	Scrambled Data to PMD Transmitter	Diff. ECL Out
DSCO ±	27, 26	Descrambled Data to PHY	Diff. ECL Out
RXCO ±	24, 25	Realigned 125 MHz Clock to PHY	Diff. ECL Out
ENC0	9	Encode 0	TTL Compatible CMOS In
ENC1	8	Encode 1	TTL Compatible CMOS In
CD	10	Clock Detect Input from Receive PLL	TTL Compatible CMOS In
SD	12	Signal Detect Input from PMD Receiver	Single-Ended ECL In

3.0 Pin Definitions and Connection Diagrams

28-Pin PLCC

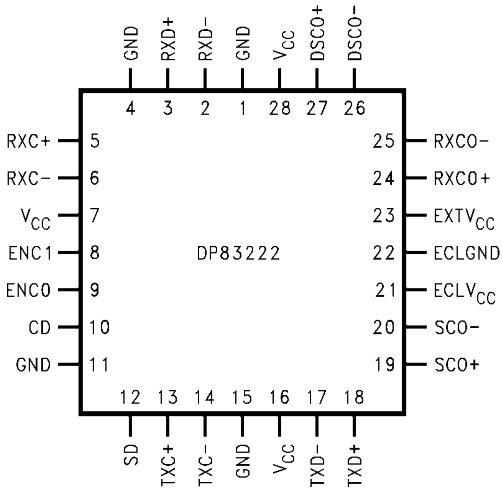


FIGURE 5. DP83222 Pinout

V_{CC} (7, 16, 28): Positive power supply for all internal CMOS circuitry. The Stream Cipher Scrambler/Descrambler operates from a single +5V DC power supply.

GND (1, 4, 11, 15): Return path for internal CMOS circuitry power supply.

$ECLV_{CC}$ (21): Positive power supply for all internal ECL circuitry. This power supply is intentionally separated from others to reduce coupled supply noise.

ECLGND (22): Return path for all internal ECL circuitry. This Power supply return is intentionally separated from others to reduce coupled supply noise.

$EXTV_{CC}$ (23): Positive power supply for emitter follower output circuitry.

RXD ± (3, 2): Differential 100K ECL data inputs. These inputs receive the ECL signals generated by the National Semiconductor DP83231 Clock Recovery Device (CRD™) or the DP83256/7VF-AP Enhanced Physical Layer Devices (PLAYER+™).

RXC ± (5, 6): Differential 100K ECL clock inputs. These inputs receive the 125 MHz clock regenerated by the National Semiconductor DP83231 Clock Recovery Device (CRD), the DP83257VF or the DP83256VF-AP Enhanced Physical Layer Devices (PLAYER+).

3.0 Pin Definitions and Connection Diagrams (Continued)

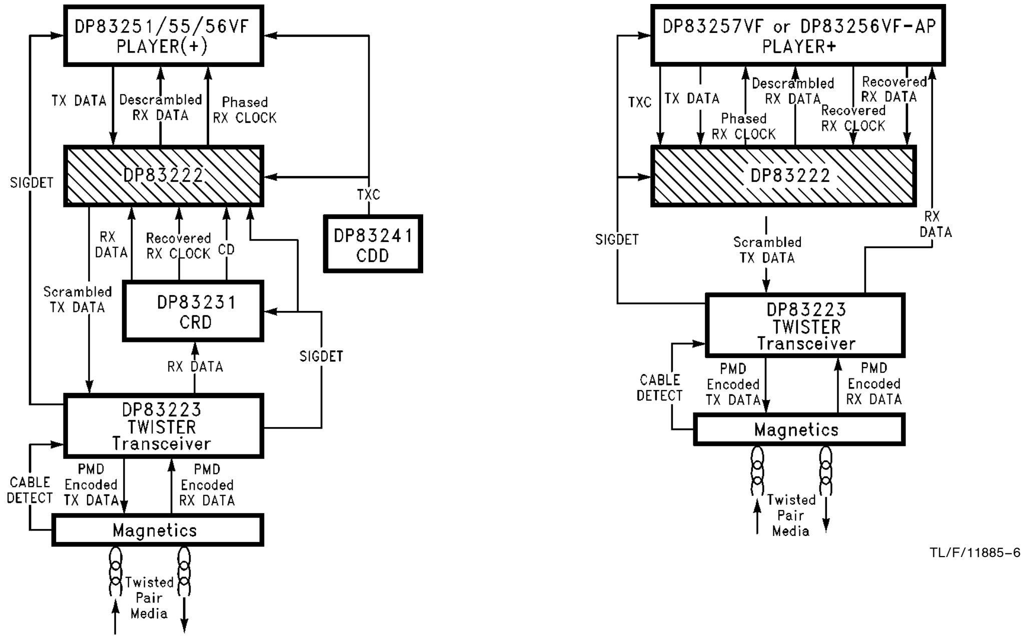


FIGURE 6. System Connection Diagrams

TXD± (18, 17): Differential 100K ECL data inputs. This is the NRZ or NRZI transmit data originating from the DP83251/5 Physical Layer Devices (PLAYER™), the DP83256/7VF or the DP83256VF-AP Enhanced Physical Layer Devices (PLAYER+).

TXC± (13, 14): Differential 100K ECL clock inputs. This is the transmit clock generated by the National Semiconductor Clock Distribution Device (CDD™), the DP83257 or the DP83256VF-AP Enhanced Physical Layer Devices (PLAYER+).

SCO± (19, 20): Differential 100K ECL data outputs. These outputs present the scrambled transmit data to the PMD transmitter.

DSCO± (27, 26): Differential 100K ECL outputs. These outputs present the descrambled data back to the National Semiconductor DP83251/55 PLAYER, the DP83256/7VF or DP83256VF-AP devices (PLAYER+).

RXCO± (24, 25): Differential 100K ECL clock outputs. These outputs supply a time aligned version of RXC± (insuring proper set and hold times relative to DSCO±) to the National Semiconductor DP83251/55 PLAYER, the DP83256/7VF or DP83256VF-AP devices (PLAYER+) for clocking-in the final descrambled data stream, DSCO±.

ENC0, 1 (9, 8): TTL compatible inputs. These pins work in conjunction with one another to select different encoding schemes or to place the DP83222 device into transparent mode where no scrambling or encoding occurs. Refer to Table II for details of operation.

CD (10): TTL compatible input data. This input accepts the CD (Clock Detect) signal from the receive Clock Recovery circuit if available. If CD goes to a logic low level, due to insufficient data edges for clock recovery, the Stream Cipher will switch to Sample mode in order to restart the synchronization process.

SD (12): Single-ended ECL data input. This input accepts the SD+ signal from the PMD. If SD goes to a logic low level, due to loss of signal from the media, the DP83222 will switch to Sample mode in order to restart the synchronization process.

4.0 Electrical Characteristics

4.1 ABSOLUTE MAXIMUM RATINGS

If Military/Aerospace specified devices are required, please contact the National Semiconductor Sales Office/Distributors for availability and specifications.

Logic Power (V_{CC}) Referenced to GND	−0.5V to +6.0V
ECL Power ($ECLV_{CC}$) Referenced to ECLGND	−0.5V to +6.0V
ECL Output Power ($EXTV_{CC}$) Referenced to GND	−0.5V to +6.0V
DC Output Current (High) (I_{ECL})	−50 mA
ESD (Electrostatic Discharge Human Body Model)	1500V
Storage Temperature (T_{STG})	−65°C to +150°C
Lead Temperature (T_L) (Soldering 10 Seconds) (IR or Vapor) (Phase Reflow)	230°C

4.2 RECOMMENDED OPERATING CONDITIONS

	Min	Max	Units
Supply Voltage (V_{CC})	4.5	5.5	V
Operating Temperature (T_A)	0	70	°C
Power Dissipation (P_D)		690	mW

4.3 DC ELECTRICAL CHARACTERISTICS $T_A = 25°C$, $V_{CC} = 5V$

Symbol	Parameter	Conditions	Min	Typ	Max	Units
V_{IHt}	TTL High Level Input		2.0			V
V_{ILt}	TTL Low Level Input				0.8	V
V_{IHe}	ECL High Level Input		$V_{CC} - 1165$		$V_{CC} - 880$	mV
V_{ILe}	ECL Low Level Input		$V_{CC} - 1810$		$V_{CC} - 1475$	mV
I_{IH}	CMOS Current In (Logic High)		−10		10	μA
I_{IL}	CMOS Current In (Logic Low)		−10		10	μA
V_{OHe}	ECL High Level Output		$V_{CC} - 1090$		$V_{CC} - 880$	mV
V_{OLe}	ECL Low Level Output		$V_{CC} - 1850$		$V_{CC} - 1600$	mV
I_{CCecl}	ECL Supply Current	Refer to *Figure 7*			65	mA
I_{CCcmos}	CMOS Supply Current	Refer to *Figure 7*			40	mA
I_{CCext}	External Supply Current	Refer to *Figure 7*			95	mA
I_{CCT}	Total Supply Current	Refer to *Figure 7*			200	mA

4.4 AC ELECTRICAL CHARACTERISTICS

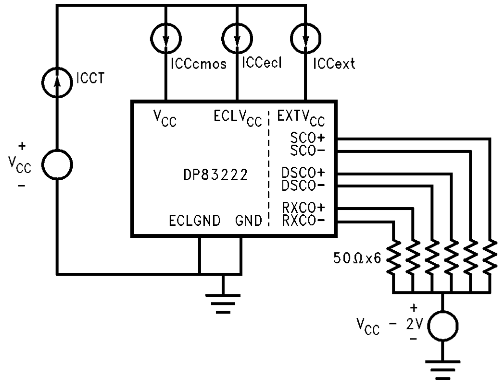
The AC Characteristics are specified over the operating range, unless otherwise noted.

Symbol	Parameter	Conditions	Min	Typ	Max	Units
T_1	TXD/TXC Setup Time	Refer to *Figure 8*	1.0			ns
T_2	TXD/TXC Hold Time	Refer to *Figure 8*	3.0			ns
T_3	RXD/RXC Setup Time	Refer to *Figure 9*	3.0			ns
T_4	RXD/RXC Hold Time	Refer to *Figure 9*	1.0			ns
T_5	RXCO/DSCO Change Time	Refer to *Figure 10*	0.5		3.0	ns
T_6	RXCO+ Pulse Width (High) RXCO− Pulse Width (Low)	Refer to *Figure 10*	4.0		6.0	ns
T_7	Transition Time 20%–80%	Refer to *Figure 11,* (Note 1)			1.5	ns
T_8	Transition Time 80%–20%	Refer to *Figure 11,* (Note 1)			1.5	ns
T_9	Scrambler Data Valid TXC+ to SCO+ (Mode 1)	Refer to *Figure 12,* (Note 2), Table 2 (Includes Asynchronous Delay of 15 ns)			39	ns
T_9	Scrambler Data Valid TXC+ to SCO+ (Mode 2)	Refer to *Figure 12,* (Note 2), Table 2 (Includes Asynchronous Delay of 15 ns)			39	ns
T_9	Scrambler Data Valid TXC+ to SCO+ (Mode 3)	Refer to *Figure 12,* (Note 2), Table 2 (Includes Asynchronous Delay of 15 ns)			47	ns
T_9	Scrambler Data Valid TXC+ to SCO+ (Mode 4)	Refer to *Figure 12,* (Note 2), Table 2 (Includes Asynchronous Delay of 15 ns)			47	ns
T_{10}	Descrambler Data Valid RXC+ to DSCO+ (Mode 1)	Refer to *Figure 13,* (Note 2), Table 2 (Includes Asynchronous Delay of 15 ns)			231	ns
T_{10}	Descrambler Data Valid RXC+ to DSCO+ (Mode 2)	Refer to *Figure 13,* (Note 2), Table 2 (Includes Asynchronous Delay of 15 ns)			239	ns
T_{10}	Descrambler Data Valid RXC+ to DSCO+ (Mode 3)	Refer to *Figure 13,* (Note 2), Table 2 (Includes Asynchronous Delay of 15 ns)			239	ns
T_{10}	Descrambler Data Valid RXC+ to DSCO+ (Mode 4)	Refer to *Figure 13,* (Note 2), Table 2 (Includes Asynchronous Delay of 15 ns)			159	ns
T_{10}	Stream Cipher Hold Mode Acquisition Time (Modes 1, 2, 3)	From Receipt of First Valid Line, Symbol (Includes Async. Delay of 15 ns)			400	ns
T_{12}	Clock Period	TXC = RXC, (Note 3)	8			ns
T_{13}	Total Jitter/Scrambler	Referenced to TXC+, (Note 1)			1	ns
T_{14}	Total Jitter/Descrambler	Referenced to RXCO+, (Note 1)			1	ns

Note 1: This parameter is not tested, but is assured by correlation with characterization data.

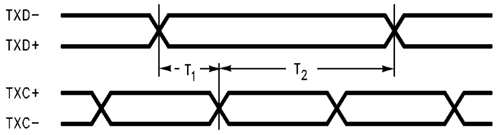
Note 2: Data Valid and Hold Acquisition timing specifications are based on Transmit and Receive clocks of 125 MHz (8 ns period) and include finite asynchronous delay.

Note 3: The DP83222 is FDDI compliant and will perform to specification over typical ±50 ppm variation in clock frequency.



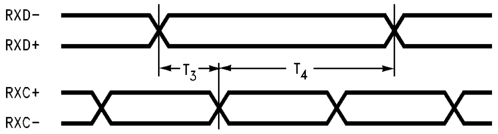
TL/F/11885–7

FIGURE 7. ICC Diagram



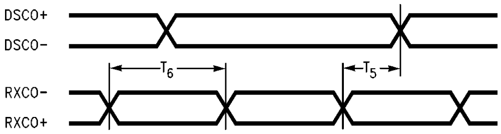
TL/F/11885–8

FIGURE 8. TX Set and Hold Times



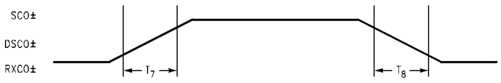
TL/F/11885–9

FIGURE 9. RX Set and Hold Times



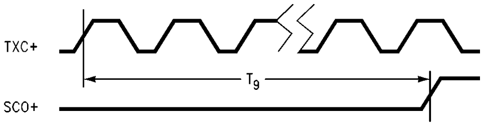
TL/F/11885–10

FIGURE 10. Descramble Change Time



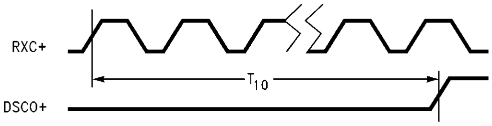
TL/F/11885–11

FIGURE 11. ECL Transition Times



TL/F/11885–12

FIGURE 12. Scrambler Data Valid Time



TL/F/11885–13

FIGURE 13. Descrambler Data Valid Time

TABLE II. Datastream Encoding Truth Table

Mode	ENC1	ENC0	PHY Interface (TXD and SCO) Expected Data Format	PMD Interface (RXD and DSCO) Expected Data Format
1	0	0	NRZI	NRZI
2	0	1	NRZI	NRZ
3	1	0	NRZ	NRZ
4	1	1	*Transparent	*Transparent

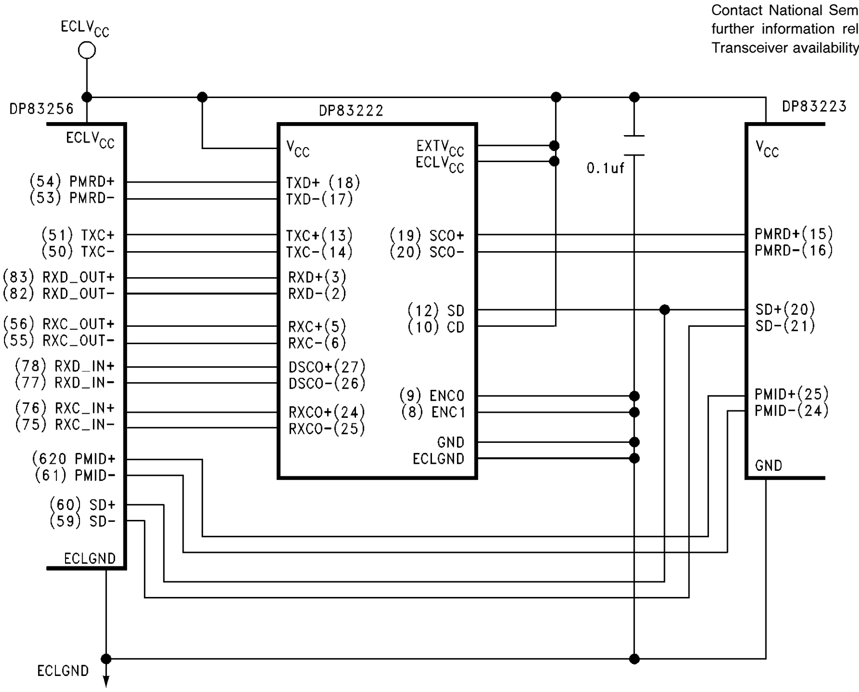
*Transparent mode of operation refers to the ability of the DP83222 to pass a given datastream through without imposing any scrambling or descrambling on the data.
(i.e. Data into Scrambler = Data out of Scrambler also Data into Descrambler = Data out of Descrambler)

TABLE III. Clock Detect and Signal Detect

CD	SD	Stream-Cipher Logic
0	0	Sample Mode
0	1	Sample Mode
1	0	Sample Mode
1	1	*Stream Cipher Initialization

*Stream-Cipher Initialization refers to the algorithm employed by the Stream Cipher logic which, by processing the encoded datastream, ultimately enters the Hold state allowing for synchronized descrambling.

Contact National Semiconductor for further information relating to PMD Transceiver availability.

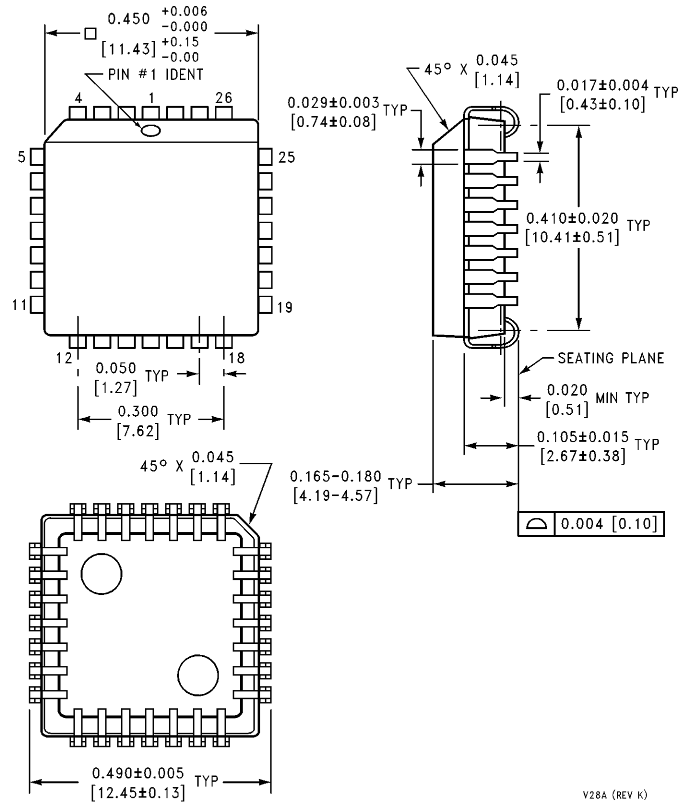


TL/F/11885-14

All ECL signals require a standard ECL termination of 50Ω to $V_{CC} - 2V$ or equivalent for proper functionality.

FIGURE 14. Typical Schematic for TP-PMD Application

Physical Dimensions inches (millimeters)



28-Pin Plastic Leaded Chip Carrier (V)
Order Number DP83222V
NS Package Number V28A

LIFE SUPPORT POLICY

NATIONAL'S PRODUCTS ARE NOT AUTHORIZED FOR USE AS CRITICAL COMPONENTS IN LIFE SUPPORT DEVICES OR SYSTEMS WITHOUT THE EXPRESS WRITTEN APPROVAL OF THE PRESIDENT OF NATIONAL SEMICONDUCTOR CORPORATION. As used herein:

1. Life support devices or systems are devices or systems which, (a) are intended for surgical implant into the body, or (b) support or sustain life, and whose failure to perform, when properly used in accordance with instructions for use provided in the labeling, can be reasonably expected to result in a significant injury to the user.
2. A critical component is any component of a life support device or system whose failure to perform can be reasonably expected to cause the failure of the life support device or system, or to affect its safety or effectiveness.

National Semiconductor Corporation
1111 West Bardin Road
Arlington, TX 76017
Tel: 1(800) 272-9959
Fax: 1(800) 737-7018

National Semiconductor Europe
Fax: (+49) 0-180-530 85 86
Email: cnjwge@tevm2.nsc.com
Deutsch Tel: (+49) 0-180-530 85 85
English Tel: (+49) 0-180-532 78 32
Français Tel: (+49) 0-180-532 93 58
Italiano Tel: (+49) 0-180-534 16 80

National Semiconductor Hong Kong Ltd.
13th Floor, Straight Block,
Ocean Centre, 5 Canton Rd.
Tsimshatsui, Kowloon
Hong Kong
Tel: (852) 2737-1600
Fax: (852) 2736-9960

National Semiconductor Japan Ltd.
Tel: 81-043-299-2309
Fax: 81-043-299-2408

National does not assume any responsibility for use of any circuitry described, no circuit patent licenses are implied and National reserves the right at any time without notice to change said circuitry and specifications.