nuvoTon
founded by winbond

**Preliminary**
March 2011
Revision 1.1

# NPCT42x Trusted Platform Module (TPM)

## General Description

The NPCT42x single-chip Trusted Platform Module (TPM) is a family of third-generation, Nuvoton SafeKeeper™ technology devices. The devices implement the Trusted Computing Group (TCG) version 1.2 specifications for PC-Client TPM.

The NPCT42x devices are designed to reduce system boot time and Trusted OS loading time. They provide a solution for PC security for a wide range of PC applications.

The NPCT42x family of devices are Microsoft® Windows® compliant and are supported by Linux kernel v2.6.18 and higher.

## Features

### General

- Single-chip TPM solution
  - No external parts required
- Compatible with *TPM Main Specification Version 1.2 Revision 116* and *PC Client Specific TPM Interface Specification Version 1.21 Revision 72*
- Host Interface
  - TPM 1.2 standard interface (TIS) with five localities
  - Supports legacy locality by using TIS protocol with I/O mapped registers
- Secure General-Purpose I/O (GPIO)
  - Five GPIO pins
  - I/O pins individually configured as input or output
  - Configurable internal pull-up resistors
  - TCG 1.2-defined interface
  - Dedicated Physical Presence (PP) pin with configurable pull-up or pull-down resistor
- Tick Counter

### Bus Interface

- LPC Bus Interface
  - Based on Intel's *LPC Interface Specification Revision 1.1, August 2002*
  - TPM 1.2 Interface (TIS)

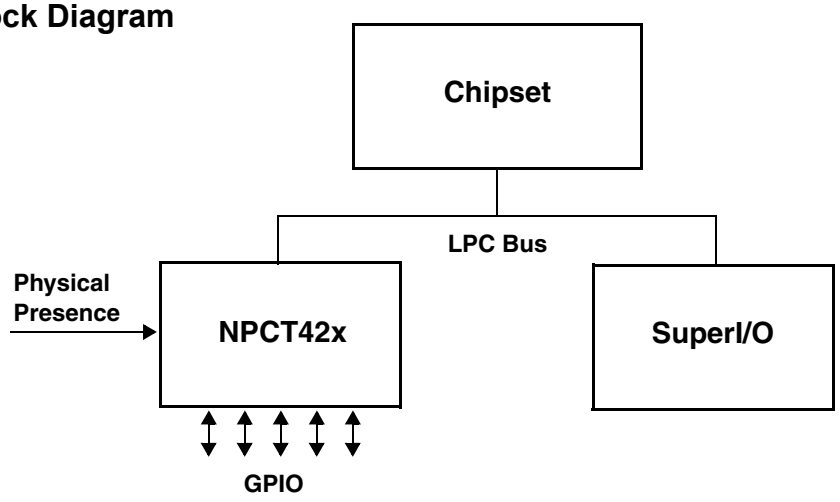
### Clocking and Supply

- On-Chip Clock Generator
- Power Supply
  - 3.3V supply operation
  - Separate pins for main ($V_{DD}$) and standby ($V_{SB}$) power supplies
  - Low standby power consumption

### Software

- TPM BIOS drivers: Memory Absent (MA) and Memory Present (MP)
- TPM Device Driver for Microsoft Windows
- NTRU Cryptosystems (acquired by Security Innovation®) Core TCG Software Stack (CTSS)
- Wave Systems Cryptographic Service Provider (CSP) with either EMBASSY® Security Center (ESC) or EMBASSY Trust Suite (ETS) OEM Edition

## System Block Diagram



## Features (Continued)

### Product-Specific Information

The following table lists the available products in the NPCT42x family.

| Software | NPCT42xA | NPCT42xB | NPCT42xC | NPCT42xD[1] | NPCT42xL |
|---|---|---|---|---|---|
| TPM BIOS drivers | ✔ | ✔ | ✔ | ✔ | ✔ |
| NTRU Cryptosystems CTSS | | ✔ | ✔ | ✔ | |
| Wave Systems CSP and ESC | | | ✔ | ✔ | |
| Wave Systems ETS OEM Edition | | | | ✔ | |

1. Restricted availability; please contact your nearest Nuvoton office. See back cover for details.

## Datasheet Revision Record

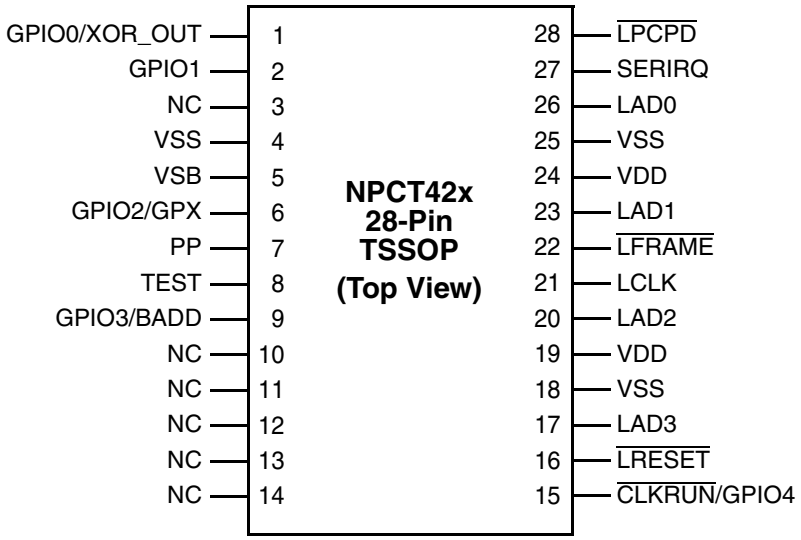
| Revision Date | Status | Comments |
|---|---|---|
| March 2011 | Revision 1.0 | Preliminary NPCT42x Datasheet. |
| May 2011 | Revision 1.1 | NPCT42xL added. |

## Table of Contents

## Table of Contents (Continued)

# 1.0 Signal/Pin Connection and Description

## 1.1 CONNECTION DIAGRAM




NC = Not Connected

**28-Pin Thin Shrink Small Outline Package (TSSOP28), JEDEC**
**Order Numbers:** See Back Cover

## 1.2 BUFFER TYPES AND SIGNAL/PIN DIRECTORY

The signal DC characteristics of the pins described in Section 1.3 on page 7 are denoted by buffer type symbols, which are defined in Table 1.

**Table 1. Buffer Types**

| Symbol | Description |
|---|---|
| $IN_T$ | Input, TTL compatible |
| $IN_{TS}$ | Input, TTL compatible, with 250 mV Schmitt Trigger |
| $IN_{PCI}$ | Input, PCI 3.3V compatible |
| $O_{p/n}$ | Output, TTL/CMOS compatible, push-pull buffer capable of sourcing *p* mA and sinking *n* mA |
| $OD_n$ | Output, TTL/CMOS compatible, open-drain buffer capable of sinking *n* mA |
| $O_{PCI}$ | Output, PCI 3.3V compatible |
| PWR | Power pin |
| GND | Ground pin |

# 1.0 Signal/Pin Connection and Description (Continued)

## 1.3 SIGNAL/PIN DESCRIPTIONS

This section describes all signals of the NPCT42x devices. The signals are organized by functional group.

### 1.3.1 LPC Interface

| Signal | Pin(s) | I/O | Buffer Type | Power Well | Description |
|---|---|---|---|---|---|
| LAD3-0 | 26, 23, 20, 17 | I/O | $IN_{PCI}/O_{PCI}$ | $V_{DD}$ | **LPC Address-Data.** Multiplexed command, address bidirectional data and cycle status. |
| LCLK | 21 | I | $IN_{PCI}$ | $V_{DD}$ | **LPC Clock.** PCI clock used for the LPC bus (up to 33 MHz). |
| $\overline{\text{LFRAME}}$ | 22 | I | $IN_{PCI}$ | $V_{DD}$ | **LPC Frame.** Low pulse indicates the beginning of a new LPC cycle or termination of a broken cycle. |
| $\overline{\text{LRESET}}$ | 16 | I | $IN_{PCI}$ | $V_{DD}$ | **LPC Reset.** PCI system reset used for the LPC bus (Hardware reset). |
| SERIRQ | 27 | I/O | $IN_{PCI}/O_{PCI}$ | $V_{DD}$ | **Serial IRQ.** The interrupt requests are serialized over a single pin, where each IRQ level is delivered during a designated time slot. |
| $\overline{\text{CLKRUN}}$ | 15 | I/OD | $IN_{PCI}/OD_6$ | $V_{DD}$ | **Clock Run.** Indicates that LCLK is going to be stopped and requests full-speed LCLK (same behavior as PCI $\overline{\text{CLKRUN}}$). |
| $\overline{\text{LPCPD}}$ | 28 | I | $IN_{PCI}$ | $V_{DD}$ | **Power Down.** Indicates that power to the LPC interface is about to be turned off. When $\overline{\text{LPCPD}}$ functionality is not required, an internal pull-up resistor allows this pin to be left floating. |

### 1.3.2 Inputs and Outputs

| Signal | Pin(s) | I/O | Buffer Type | Power Well | Description |
|---|---|---|---|---|---|
| PP | 7 | I | $IN_{TS}$ | $V_{DD}$ | **Physical Presence Input.** Indicates owner's physical presence. |
| GPIO4-0 | 15, 9, 6, 2, 1 | I/O | $IN_{TS}/OD_8$, $O_{4/8}$ | $V_{DD}$ | **General-Purpose I/O Ports.** General-Purpose I/O pins compatible with the *PC Client TPM 1.2 Specification*. |
| GPX | 6 | I/O | $IN_{TS}/OD_8$ | $V_{DD}$ | **GPIO-Express-00.** This pin may be configured as GPIO-Express-00 pin as described in the *PC Client TPM 1.2 Specification*. |

### 1.3.3 Configuration Straps and Testing

| Signal | Pin(s) | I/O | Buffer Type | Power Well | Description |
|---|---|---|---|---|---|
| TEST | 8 | I | $IN_{TS}$ | $V_{DD}$ | **Test Mode Enable.** Sampled at $V_{DD}$ Power-Up reset to force the device pins into a XOR tree or TRI-STATE® configuration, as follows:<br>– No pull-up resistor (default) - normal device operation<br>– 4.7 KΩ external pull-up resistor - pins configured for Test mode. |
| BADD | 9 | I | $IN_{TS}$ | $V_{DD}$ | **Base Address.** Sampled at $V_{DD}$ Power-Up reset to determine the base address of the configuration Index-Data register pair:<br>– No pull-down resistor (default) - 7Eh-7Fh<br>– 10 KΩ external pull-down resistor - EEh-EFh<br>**Test Mode Selection.**<br>Test mode (XOR tree or TRI-STATE) is selected by the sampled state of the BADD pin during $V_{DD}$ Power-Up reset. When BADD is sampled high, XOR Tree mode is selected. When BADD is sampled low, TRI-STATE mode is selected, floating all output pins. |
| XOR_OUT | 1 | O | $O_{4/8}$ | $V_{DD}$ | **XOR Tree Output.** This pin is the output of the XOR tree test logic. |

# 1.0 Signal/Pin Connection and Description (Continued)

### 1.3.4 Power and Ground

| Signal | Pin(s) | I/O | Buffer Type | Power Well | Description |
|---|---|---|---|---|---|
| VSS | 4, 18, 25 | I | GND | | **Ground.** Ground connection for both core logic and I/O buffers, for the Main and Standby power supplies. |
| VDD | 19, 24 | I | PWR | | **Main 3.3V Power Supply.** Powers the I/O buffers of the GPIO ports and the LPC interface. |
| VSB | 5 | I | PWR | | **Standby 3.3V Power Supply.** Powers the on-chip core. |

### 1.3.5 Not Connected

| Signal | Pin(s) | I/O | Buffer Type | Power Well | Description |
|---|---|---|---|---|---|
| NC | 3, 10-14 | | | | **Not Connected.** These pins may be either connected to any signal on the board or left unconnected. |

## 1.4 INTERNAL PULL-UP AND PULL-DOWN RESISTORS

The signals listed in Table 2 have internal pull-up (PU) and/or pull-down (PD) resistors. The internal resistors are optional for those signals indicated as “Programmable”.

**Table 2. Internal Pull-Up and Pull-Down Resistors**

| Signal | Pin(s) | Power Well | Type | Comments |
|---|---|---|---|---|
| $\overline{\text{LPCPD}}$ | 28 | $V_{DD}$ | $PU_{110}$ | |
| GPIO4-0 | 15, 9, 6, 2, 1 | $V_{DD}$ | $PU_{110}$ | Programmable[1] |
| GPX | 6 | $V_{DD}$ | $PU_{110}$ | Note[2] |
| PP | 7 | $V_{DD}$ | $PU_{110}/PD_{110}$ | Programmable[3] |
| TEST | 8 | $V_{DD}$ | $PD_{110}$ | Strap |

1. Default at reset: GPIO0,2,3 enabled, GPIO1,4 disabled.
2. When GPIO-Express-00 (GPX) is selected for pin 6, the pull-up is enabled by default.
3. Default at reset: pull-down enabled.

# 2.0 Trusted Platform Module (TPM) Overview

The NPCT42x devices provide TPM functionality in TCG 1.2-compliant systems and is designed to best meet the requirements of PC systems.

## 2.1 SYSTEM CONNECTIONS

Figure 1 shows the system connections of the NPCT42x in a typical PC application.

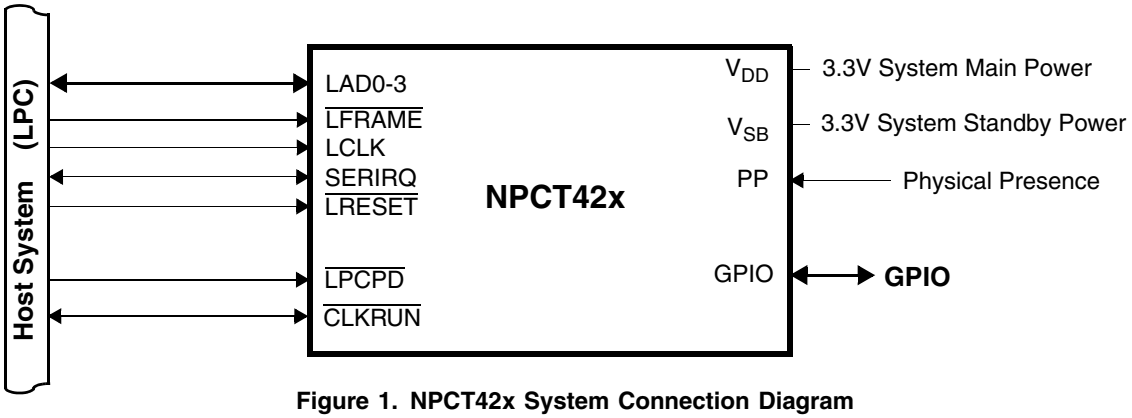



**Figure 1. NPCT42x System Connection Diagram**

TPM functions are all integrated on-chip. The major elements of the NPCT42x interface are:

- Host interface based on an LPC bus, with interrupt request.
- A physical presence input signal (PP) to indicate owner physical presence.
- GPIO signals (GPIO0-4), operated by TCG commands.

## 2.2 POWER MANAGEMENT (PM)

The NPCT42x devices have an advanced power management scheme. The wake-up scheme enables the NPCT42x to respond to any kind of event that may require its attention. Power consumption is minimized by dynamically adjusting the internal power modes to the activity required by the host commands and other operations.

The security functions (core and associated peripherals) are supplied by $V_{SB}$, which must be connected to the system standby power source (must exist in ACPI S3 state).

## 2.3 HOST INTERFACE

The Host Bus Interface is based on Intel's Low Pin Count (LPC) interface, as defined in the *LPC Interface Specification, Revision 1.1*. This interface enables the host to perform read and write cycles using I/O space accesses as well as TPM accesses. The host interface works in either legacy or TPM 1.2-compliant mode.

# 3.0 I/O Configuration Registers

The NPCT42x host-controlled functions consist of a single logical device (TPM interface), the host interface and a central set of configuration registers.

The NPCT42x support two register mapping and configuration modes:

- Legacy mode (as described throughout this document). This mode requires configuration, as described in the next section.
- TPM-LPC mode (see Section 4.1 on page 12 and the *TCG 1.2 PC Client Specific TPM Interface Specification*). This mode is self-contained and requires no additional configuration.

The Configuration and Control register set supports ACPI-compliant PnP configuration, defined in Appendix A of the *Plug and Play ISA Specification, Revision 1.0a* by Intel and Microsoft.

## 3.1 CONFIGURATION REGISTER STRUCTURE AND ACCESS

The configuration register is accessed via the Index-Data register pair.

### 3.1.1 The Index-Data Register Pair

Access to the NPCT42x configuration registers is via an Index-Data register pair, using two system I/O byte locations. The base address of this register pair is determined during $V_{DD}$ Power-Up, according to the BADD strap pin. Table 3 shows the selected base addresses as a function of BADD.

**Table 3. BADD Strapping Options**

| BADD Strap | I/O Address | |
|---|---|---|
| | Index Register (Base) | Data Register (Base + 1) |
| High | 7Eh | 7Fh |
| Low | EEh | EFh |

The Index register is an 8-bit read/write register located at the base address (Base+0). It is used as a pointer to the configuration register structure and holds the index of the configuration register that is currently accessible via the Data register.

The Data register is an 8-bit register located at the base address (Base+1) used as a data path to any configuration register. Accessing the Data register actually accesses the configuration register that is currently pointed by the Index register.

### 3.1.2 TPM Configuration Records

The NPCT42x TPM Interface (TIS) is associated with Logical Device Number (LDN) 1Ah. Access to the registers in indexes 30h-71h is available only when the LDN register (index 07h) is set to 1Ah.

**Table 4. Configuration Register Map**

| Index | Register Name | Type | Reset | Comments |
|---|---|---|---|---|
| 07h | Logical Device Number | R/W | 00h | TPM is PnP LDN 1Ah. |
| 20h | TPM Device ID (DID) | RO | FEh | Vendor-defined registers |
| 27h | TPM Revision ID (RID) | RO | - | |
| 30h | Logical Device Control (Activate) | R/W | 00h | |
| 60h | I/O Base Address Descriptor 0 Bits 15-8 | R/W | 00h | |
| 61h | I/O Base Address Descriptor 0 Bits 7-0 | R/W | 00h | Bits 3-0 (for A3-A0) are read only, '0000'. |
| 70h | Interrupt Number and Wake-Up on IRQ Enable | R/W | 00h | |
| 71h | IRQ Type Select | R/W | 03h | Bit 1 is read/write; other bits are read only. |

# 3.0 I/O Configuration Registers (Continued)

## 3.1.3 Reset Configuration Setup

The default configuration setup of the NPCT42x is:

- The configuration base address is according to Table 3 on page 10.
- TPM logical device is disabled.
- The TPM interface is in Legacy mode.
- All host configuration registers are set to their default values unless explicitly stated otherwise.

## 3.1.4 Register Type Abbreviations

The following abbreviations are used to indicate the Register Type:

- R/W= Read/Write.
- RO= Read-only.

Write 0 to reserved bits unless another “required value” is specified. This method can be used for registers containing bits of all types.

# 4.0 TPM Host Interface

This chapter describes the TPM 1.2-compliant host interface.

## 4.1 TPM INTERFACE MODULE (TIS)

The TPM interface module implements a communication channel between the host and the TPM. The communication channel is compatible with the *TCG PC Client Specific TPM Interface Specification Version 1.2*.

The TPM interface module provides a mechanism for command and response transfers between the host and the NPCT42x. The host sends TPM commands via the TPM Interface Data FIFO. The TPM executes the command and sends a response via the same Data FIFO. See the *TPM Main Specification, Version 1.2* for TPM command set definitions.

### 4.1.1 Features

- Access to TPM using dedicated LPC TPM transactions with locality levels 0 to 4. For details, see the *TCG PC Client Specific TPM Interface Specification Version 1.2*.
- Legacy locality support using LPC I/O transactions. For details see Section 4.1.3.
  - Resource configuration via PnP configuration space.

### 4.1.2 Host Interrupt Support

The NPCT42x have one SERIRQ interrupt to the host. When SERIRQ is enabled, it can be set by any of the following events:

- Locality change - whenever a new locality becomes active either because it seized control or because a previous locality relinquished control; i.e., this event is not set if no previous locality was active.
- Command Ready - on **`commandReady`** bit transition from 0 to 1 (in TPM_STS register).
- Status Valid - on **`stsValid`** bit transition from 0 to 1 (in TPM_STS register).
- Data Available - on **`dataAvail`** bit transition from 0 to 1 (in TPM_STS register), if **stsValid** bit is 1; or on **`stsValid`** transition from 0 to 1, if **`dataAvail`** bit is 1.

### 4.1.3 Host TPM Legacy Interface Registers

The I/O base address is set via the I/O space configuration registers (index 60,61) of the TPM interface configuration registers. Table 5 shows the TPM Legacy Interface register mapping.

All Host TPM legacy interface registers correspond, in both name and structure, to the TPM Interface registers defined in the *TCG PC Client Specific TPM Interface Specification Version 1.2*.

**Note:** Addresses that do not appear in this table are not responded to by the TPM.

**Table 5. Host TPM Legacy Interface Run-Time Registers**

| TPM Interface Register | Offset in Legacy LPC I/O Address Space | Comments |
|---|---|---|
| TPM_INT_ENABLE | 00h | Interrupt type is configured via index 71h.<br>Reserved bits and **`GlobalIntEnable`** bit are not implemented in the legacy address space. |
| TPM_INT_STATUS | 01h | Reserved bits 31-8 are not implemented in the legacy address space |
| TPM_INTF_CAPABILITY | 02h | Reserved bits 31-9 and **`burstCountStatic`** bit are not implemented in the legacy address space. |
| TPM_STS(7-0) | 03h | |
| TPM_STS(15-8) | 04h | **`burstCount`** (TPM_STS(24-16) are 0) |
| TPM_DATA_FIFO | 05h | |

# 5.0 Device Specifications

## 5.1 GENERAL DC ELECTRICAL CHARACTERISTICS

### 5.1.1 Recommended Operating Conditions

| Symbol | Parameter | Min | Typ | Max | Unit |
|---|---|---|---|---|---|
| $V_{DD}$ | Main 3V Supply Voltage | 3.0 | 3.3 | 3.6 | V |
| $V_{SB}$ | Standby 3V Supply Voltage | 3.0 | 3.3 | 3.6 | V |
| $T_A$ | Operating Temperature | 0 | | +70 | °C |

### 5.1.2 Absolute Maximum Ratings

Absolute maximum ratings are values beyond which damage to the device may occur. Unless otherwise specified, all voltages are relative to ground ($V_{SS}$).

| Symbol | Parameter | Conditions | Min | Max | Unit |
|---|---|---|---|---|---|
| $V_{SUP}$ | Supply Voltage[1] | | -0.3 | +4.1 | V |
| $V_I$ | Input Voltage | | -0.3 | $V_{DD}$ + 0.5 | V |
| $V_O$ | Output Voltage | | -0.3 | $V_{DD}$ + 0.5 | V |
| $T_{STG}$ | Storage Temperature | | -65 | +165 | °C |
| $P_D$ | Power Dissipation | | | 1 | W |
| $T_L$ | Lead Temperature Soldering (10 s) | | | +260 | °C |
| | ESD Tolerance | $C_{ZAP}$ = 100 pF<br>$R_{ZAP}$ = 1.5 KΩ[2] | 2000 | | V |

1. $V_{SUP}$ is $V_{DD}$, $V_{SB}$.
2. Value based on test complying with RAI-5-048-RA human body model ESD testing.

### 5.1.3 Capacitance

| Symbol | Parameter | Conditions | Min | Typ[1] | Max | Unit |
|---|---|---|---|---|---|---|
| $C_{IN}$ | Input Pin Capacitance | | | 4 | 5 | pF |
| $C_{INC}$ | LPC Clock Input Capacitance | LCLK | 5 | 8 | 12 | pF |
| $C_{PCI}$ | LPC Pin Capacitance | LAD3-0, $\overline{\text{LFRAME}}$, $\overline{\text{LRESET}}$, SERIRQ, $\overline{\text{CLKRUN}}$, $\overline{\text{LPCPD}}$ | | 8 | 10 | pF |
| $C_{IO}$ | I/O Pin Capacitance | | | 8 | 10 | pF |
| $C_O$ | Output Pin Capacitance | | | 6 | 8 | pF |

1. $T_A$ = 25°C; f = 1 MHz.

# 5.0 Device Specifications (Continued)

## 5.1.4 Power Consumption under Recommended Operating Conditions

| Symbol | Parameter | Conditions[1] | Typ | Max | Unit |
|---|---|---|---|---|---|
| $I_{DD}$ | $V_{DD}$ Average Supply Current | $V_{IL}$ = 0.5V, $V_{IH}$ = 2.4V, No Load | 5 | 10 | mA |
| $I_{SB}$ | $V_{SB}$ Average Supply Current | $V_{IL}$ = 0.5V, $V_{IH}$ = 2.4V, No Load | 20 | 50 | mA |
| $I_{SBLP}$ | $V_{SB}$ Quiescent Supply Current in Idle Mode[2] | $V_{IL}$ = $V_{SS}$, $V_{IH}$ = $V_{SB}$, No Load | 300 | 700 | µA |

1. All parameters specified for $0°C \le T_A \le 70°C$; $V_{DD}$ and $V_{SB}$ = 3.3V ±10% unless otherwise specified.
2. Device is not performing any operation; no LPC bus activity.

# 5.0 Device Specifications (Continued)

## 5.2 DC CHARACTERISTICS OF PINS BY I/O BUFFER TYPES

The tables in this section summarize the DC characteristics of all device pins described in Section 1.2 on page 6. The characteristics describe the general I/O buffer types defined in Table 1 on page 6. The DC characteristics of the LPC interface meet the *PCI Local Bus Specification (Rev 2.2 December 18, 1998)* for 3.3V DC signaling.

### 5.2.1 Input, TTL Compatible

**Symbol:** $IN_T$

| Symbol | Parameter | Conditions | Min | Max | Unit |
|---|---|---|---|---|---|
| $V_{IH}$ | Input High Voltage | | 2.0 | $V_{SUP}$[1]+0.5 | V |
| $V_{IL}$ | Input Low Voltage | | –0.3 | 0.8 | V |
| $I_{ILK}$[2] | Input Leakage Current | $V_{SUP}$[3] = 3.0V - 3.6V and 0 < $V_{IN}$ < $V_{SUP}$ | | ±10 | µA |
| | | $V_{SUP}$ = 3.0V - 3.6V and $V_{SUP}$ < $V_{IN}$ | | ±10 | µA |

1. $V_{SUP}$ is $V_{DD}$ or $V_{SB}$ according to the power well of the input.
2. Input leakage current includes the output leakage of the bidirectional buffers with TRI-STATE outputs. For additional conditions, see Section 5.2.7 on page 17.
3. $V_{SUP}$ is $V_{DD}$ or $V_{SB}$ according to the power well of the input.

### 5.2.2 Input, TTL Compatible, with Schmitt Trigger

**Symbol:** $IN_{TS}$

| Symbol | Parameter | Conditions | Min | Max | Unit |
|---|---|---|---|---|---|
| $V_{IH}$ | Input High Voltage | | 2 | $V_{SUP}$[1]+0.5 | V |
| $V_{IL}$ | Input Low Voltage | | –0.3 | 0.8 | V |
| $V_H$ | Input Hysteresis | | 300 | | mV |
| $I_{ILK}$[2] | Input Leakage Current | $V_{SUP}$ = 3.0V - 3.6V and 0 < $V_{IN}$ < $V_{SUP}$ | | ±10 | µA |
| | | $V_{SUP}$ = 3.0V - 3.6V and $V_{SUP}$ < $V_{IN}$ | | ±10 | µA |

1. $V_{SUP}$ is $V_{DD}$ or $V_{SB}$ according to the power well of the input.
2. Input leakage current includes the output leakage of the bidirectional buffers with TRI-STATE outputs. For additional conditions, see Section 5.2.7 on page 17.

### 5.2.3 Input, PCI 3.3V Compatible

**Symbol:** $IN_{PCI}$

| Symbol | Parameter | Conditions | Min | Max | Unit |
|---|---|---|---|---|---|
| $V_{IH}$ | Input High Voltage | | 0.5 $V_{DD}$ | $V_{DD}$+0.5 | V |
| $V_{IL}$ | Input Low Voltage | | –0.3 | 0.3 $V_{DD}$ | V |
| $I_{ILK}$[1] | Input Leakage Current | $V_{DD}$ = 3.0V - 3.6V and 0 < $V_{IN}$ < $V_{DD}$ | | ±10 | µA |
| | | $V_{DD}$ = 3.0V-3.6V and $V_{DD}$<$V_{IN}$< $V_{DD}$+0.5V | | ±10 | µA |

1. Input leakage current includes the output leakage of the bidirectional buffers with TRI-STATE outputs. For additional conditions, see Section 5.2.7 on page 17.

# 5.0 Device Specifications (Continued)

## 5.2.4 Output, TTL/CMOS Compatible, Push-Pull Buffer

**Symbol:** $O_{p/n}$

Output, TTL/CMOS Compatible, rail-to-rail push-pull buffer that is capable of sourcing *p* mA and sinking *n* mA.

| Symbol | Parameter | Conditions | Min | Max | Unit |
|---|---|---|---|---|---|
| $V_{OH}$ | Output High Voltage | $I_{OH}$ = –*p* mA | 2.4 | | V |
| | | $I_{OH}$ = –50 µA | $V_{SUP}$[1] – 0.2 | | V |
| $V_{OL}$ | Output Low Voltage | $I_{OL}$ = *n* mA | | 0.4 | V |
| | | $I_{OL}$ = 50 µA | | 0.2 | V |
| $I_{OLK}$[2] | Output Leakage Current | $V_{SUP}$ = 3.0V - 3.6V and 0 < $V_{IN}$ < $V_{SUP}$ | | ±10 | µA |
| | | $V_{SUP}$ = 3.0V - 3.6V and $V_{SUP}$ < $V_{IN}$ < $V_{SUP}$+0.5V | | ±10 | µA |

1. $V_{SUP}$ is $V_{DD}$ or $V_{SB}$ according to the power well of the input.
2. Output leakage current includes the input leakage of the bidirectional buffers with TRI-STATE outputs. For additional conditions, see Section 5.2.7 on page 17.

## 5.2.5 Output, Open Drain Buffer

**Symbol:** $OD_n$

Output, Open Drain capable of sinking *n* mA.

| Symbol | Parameter | Conditions | Min | Max | Unit |
|---|---|---|---|---|---|
| $V_{OL}$ | Output Low Voltage | $I_{OL}$ = *n* mA | | 0.4 | V |
| | | $I_{OL}$ = 50 µA | | 0.2 | V |
| $I_{OLK}$[1] | Output Leakage Current | $V_{SUP}$ = 3.0V - 3.6V and 0 < $V_{IN}$ < $V_{SUP}$ | | 10 | µA |
| | | $V_{SUP}$ = 3.0V - 3.6V and $V_{SUP}$ < $V_{IN}$ < $V_{SUP}$+0.5V | | 10 | µA |

1. Output leakage current includes the input leakage of the bidirectional buffers with TRI-STATE outputs. For additional conditions, see Section 5.2.7 on page 17.

## 5.2.6 Output, PCI 3.3V Compatible

**Symbol:** $O_{PCI}$

| Symbol | Parameter | Conditions | Min | Max | Unit |
|---|---|---|---|---|---|
| $V_{OH}$ | Output High Voltage | $I_{out}$ = –500 µA | 0.9 $V_{DD}$ | | V |
| $V_{OL}$ | Output Low Voltage | $I_{out}$ = 1500 µA | | 0.1 $V_{DD}$ | V |
| $I_{OLK}$[1] | Output Leakage Current | $V_{DD}$ = 3.0V - 3.6V and 0 < $V_{IN}$ < $V_{DD}$ | | ±10 | µA |

1. Output leakage current includes the input leakage of the bidirectional buffers with TRI-STATE outputs. For additional conditions, see Section 5.2.7 on page 17.

## 5.0 Device Specifications (Continued)

### 5.2.7 Notes and Exceptions

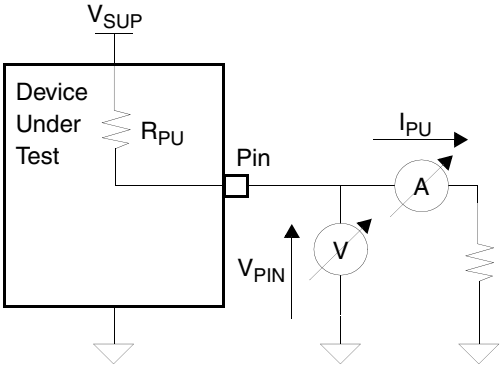
1. $I_{ILK}$ and $I_{OLK}$ are measured in the following cases (where applicable):
   - Internal pull-up or pull-down resistor is disabled
   - Push-pull output buffer is disabled (TRI-STATE mode)
   - Open-drain output buffer is at high level
2. Some pins have an internal static pull-up resistor (when enabled) and therefore may have leakage current from $V_{SUP}$ (when $V_{IN}$ = 0). See Section 1.4 on page 8 for a list of the relevant pins.
3. Some pins have an internal static pull-down resistor (when enabled) and therefore may have leakage current to GND (when $V_{IN} = V_{SUP}$). See Section 1.4 on page 8 for a list of the relevant pins.
4. The following strap pins have an internal static pull-up resistor enabled during Power-Up reset and therefore may have leakage current from $V_{SB}$ (when $V_{IN}$ = 0): BADD, $\overline{TEST}$.
5. $I_{OH}$ is valid for a GPIO pin only when it is not configured as open-drain.
6. In XOR Tree mode, the buffer type of the input pins included in the XOR tree is $IN_T$ (Input, TTL compatible), regardless of the buffer type of these pins in normal device operation mode.

## 5.0 Device Specifications (Continued)

### 5.3 INTERNAL RESISTORS

**DC Test Conditions**

**Pull-Up Resistor Test Circuit**




**Pull-Down Resistor Test Circuit**

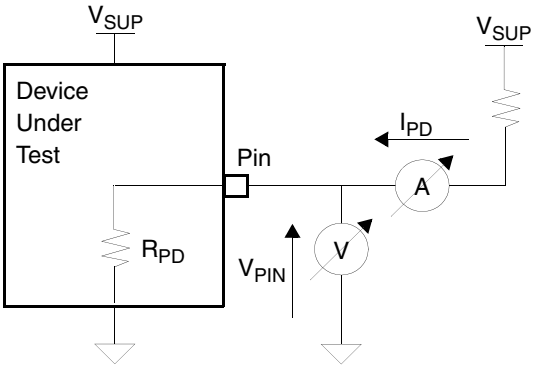
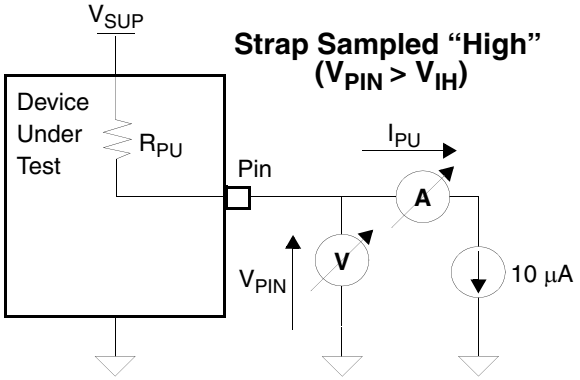


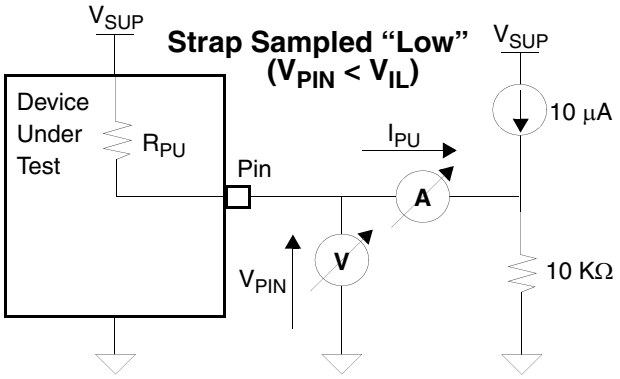

**Figure 2. Internal Resistor Test Conditions, $T_A$ = 0°C to 70°C, $V_{SUP}$ = 3.3V**

**Internal Pull-Up Strap**

**Strap Sampled "High" ($V_{PIN} > V_{IH}$)**

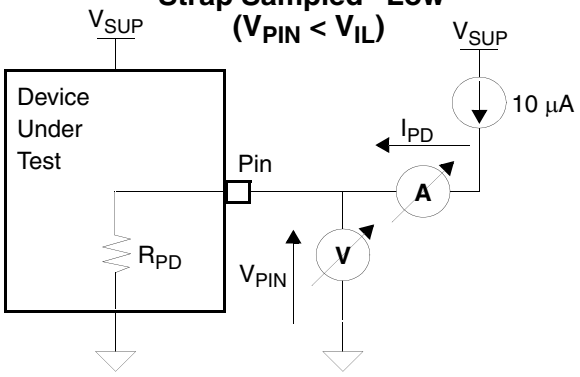



**Strap Sampled "Low" ($V_{PIN} < V_{IL}$)**




**Internal Pull-Down Strap**

**Strap Sampled "Low" ($V_{PIN} < V_{IL}$)**




**Strap Sampled "High" ($V_{PIN} > V_{IH}$)**

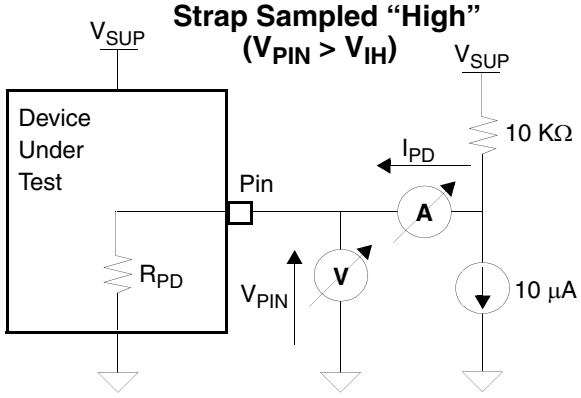



**Figure 3. Internal Resistor Design Requirements, $T_A$ = 0°C to 70°C, $V_{SUP}$ = 3.3 V**

**Notes**:

1. $V_{SUP}$ is $V_{DD}$ or $V_{SB}$, according to the pin power well.
2. The equivalent resistance of the pull-up resistor is calculated by $R_{PU} = (V_{SUP} - V_{PIN}) / I_{PU}$.
3. The equivalent resistance of the pull-down resistor is calculated by $R_{PD} = V_{PIN} / I_{PD}$.

## 5.0 Device Specifications (Continued)

### 5.3.1 Pull-Up Resistor

**Symbol:** $PU_{nn}$

| Symbol | Parameter | Conditions[1] | Min[2] | Typical | Max[2] | Unit |
|---|---|---|---|---|---|---|
| $R_{PU}$ | Pull-up equivalent resistance | $V_{PIN}$ = 0V | *nn* – 50% | *nn* | *nn* + 66% | KΩ |

1. TA = 0°C to 70°C, $V_{SUP}$ = 3.3V.
2. Not tested; guaranteed by characterization.

### 5.3.2 Pull-Down Resistor

**Symbol:** $PD_{nn}$

| Symbol | Parameter | Conditions[1] | Min[2] | Typical | Max[2] | Unit |
|---|---|---|---|---|---|---|
| $R_{PD}$ | Pull-down equivalent resistance | $V_{PIN}$ = $V_{SUP}$ | *nn* – 50% | *nn* | *nn* + 120% | KΩ |

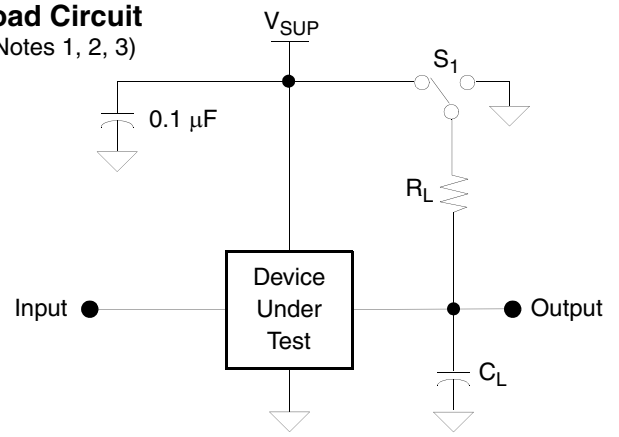
1. TA = 0°C to 70°C, $V_{SUP}$ = 3.3V.
2. Not tested; guaranteed by characterization.

# 5.0 Device Specifications (Continued)

## 5.4 AC ELECTRICAL CHARACTERISTICS

### 5.4.1 AC Test Conditions

**Load Circuit**
(Notes 1, 2, 3)




**AC Testing Input, Output Waveform**

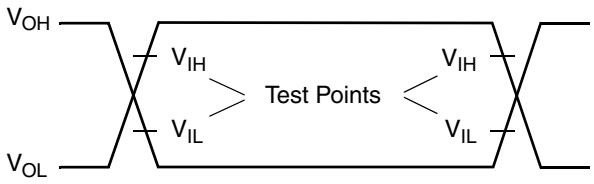



**Figure 4. AC Test Conditions, $T_A$ = 0°C to 70°C, $V_{SUP}$ = 3.0V - 3.6V**

**Notes**:

1. $V_{SUP}$ is $V_{DD}$ or $V_{SB}$ according to the power well of the pin.
2. $C_L$ = 50 pF for all output pins except the following pin groups (values include both jig and oscilloscope capacitance):
   $S_1$ = Open – for push-pull output pins.
   $S_1$ = $V_{SUP}$ – for high impedance to active low and active low to high-impedance transition measurements.
   $S_1$ = GND – for high impedance to active high and active high to high-impedance transition measurements.
   $R_L$ = 1.0 KΩ – for all pins.
3. The following abbreviations are used in Section 5.4: RE = Rising Edge; FE = Falling Edge

### Definitions

The timing specifications in this section are relative to $V_{IL}$ or $V_{IH}$ (according to the specific buffer type) on the rising or falling edges of all the signals, as shown in the following figures (unless specifically stated otherwise).

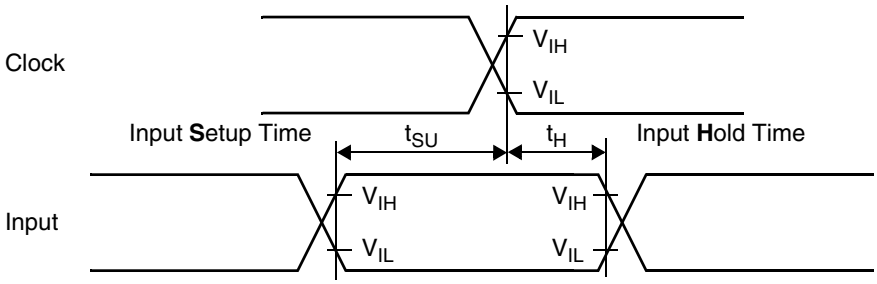



**Figure 5. Input Setup and Hold Time**

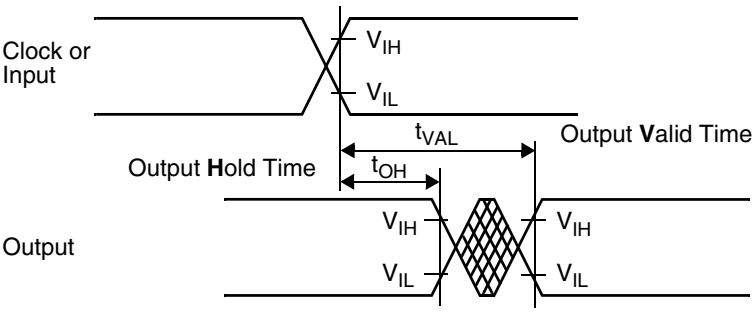



**Figure 6. Clock-to-Output and Propagation Delay**

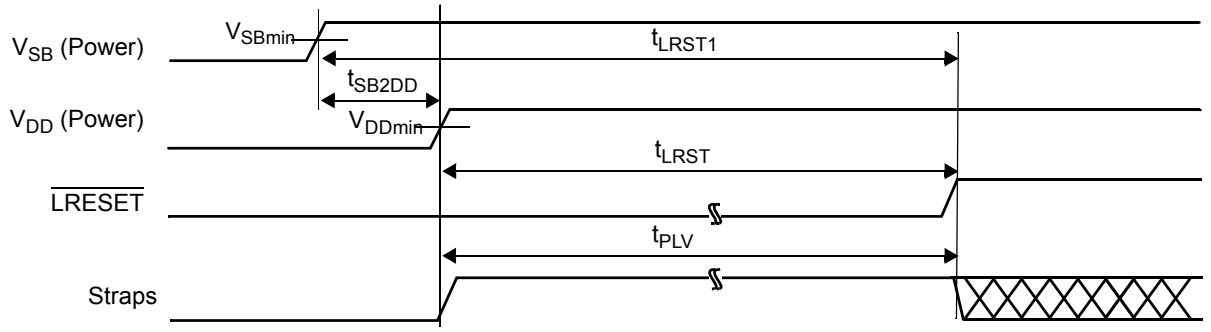
## 5.0 Device Specifications (Continued)

### 5.4.2 Reset Timing

**Power-Up Reset**

| Symbol | Description | Reference Conditions | Min[1] | Max |
|---|---|---|---|---|
| $t_{SB2DD}$ | $V_{SB}$ power-up to $V_{DD}$ power-up | | 0 ms | |
| $t_{LRST1}$ | $V_{SB}$ power-up to end of $\overline{\text{LRESET}}$ | LPC interface | 100 ms | |
| $t_{LRST}$ | $\overline{\text{LRESET}}$ active time | $V_{DD}$ power-up to end of $\overline{\text{LRESET}}$ | 10 ms | |
| $t_{PLV}$ | Strap valid time | Before end of $\overline{\text{LRESET}}$ | 10 ms | |

1. Not Tested; guaranteed by design.



# 5.0 Device Specifications (Continued)

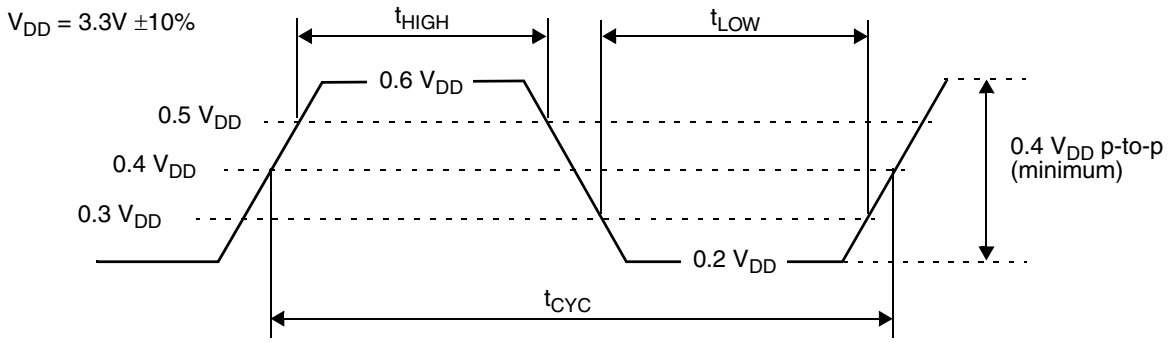
## 5.4.3 LPC Interface Timing

The AC characteristics of the LPC interface meet the PCI Local Bus Specification *(Rev 2.2 December 18, 1998)* for 3.3V DC signaling.

### LCLK and $\overline{\text{LRESET}}$

| Symbol | Parameter | Min | Max | Units |
|---|---|---|---|---|
| $t_{CYC}$[1] | LCLK Cycle Time | 30 | | ns |
| $t_{HIGH}$ | LCLK High Time[2] | 11 | | ns |
| $t_{LOW}$ | LCLK Low Time[2] | 11 | | ns |
| – | LCLK Slew Rate[2,3] | 1 | 4 | V/ns |
| – | $\overline{\text{LRESET}}$ Slew Rate[2,4] | 50 | | mV/ns |

1. The LPC may have any clock frequency between nominal DC and 33 MHz. Device operational parameters at frequencies under 16 MHz are guaranteed by design rather than by testing. The clock frequency may be changed at any time during the operation of the system as long as the clock edges remain “clean” (monotonic) and the minimum cycle high and low times are not violated. The clock may only be stopped in low state.
2. Not tested; guaranteed by characterization.
3. Rise and fall times are specified in terms of the edge rate measured in V/ns. This slew rate must be met across the minimum peak-to-peak portion of the clock wavering (0.2 * $V_{DD}$ to 0.6 * $V_{DD}$) as shown below.
4. The minimum $\overline{\text{LRESET}}$ slew rate applies only to the rising (de-assertion) edge of the reset signal and ensures that system noise cannot make an otherwise monotonic signal appear to bounce in the switching range.



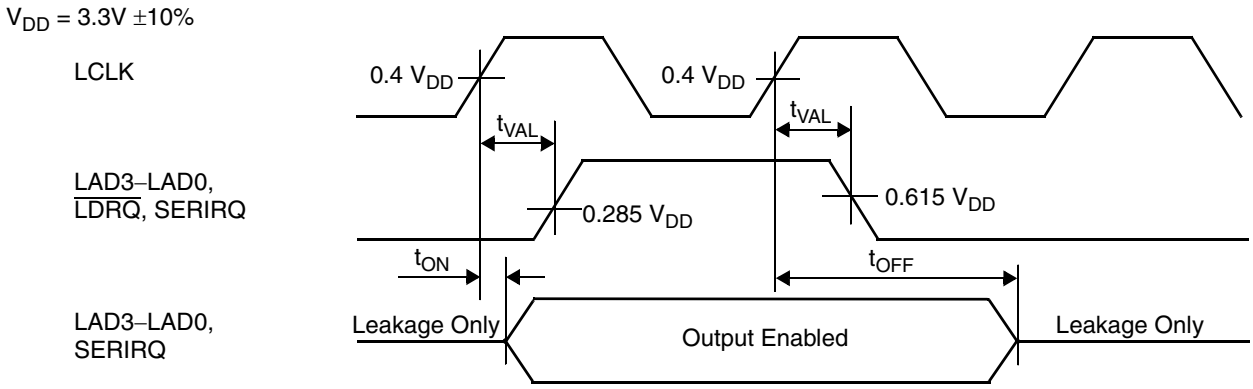
## 5.0 Device Specifications (Continued)

### LPC Signals

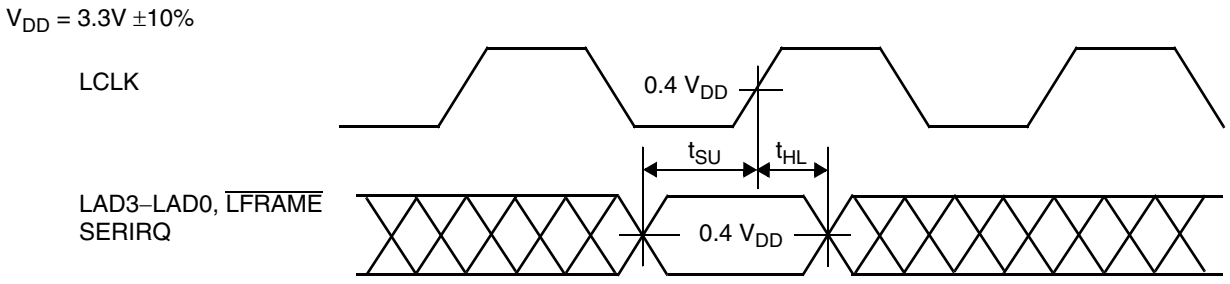
| Symbol | Figure | Description | Reference Conditions | Min | Max | Unit |
|---|---|---|---|---|---|---|
| $t_{VAL}$ | Outputs | Output Valid Delay | After RE of CLK | 2 | 11 | ns |
| $t_{ON}$[1] | Outputs | Float to Active Delay | After RE of CLK | 2 | | ns |
| $t_{OFF}$[1] | Outputs | Active to Float Delay | After RE of CLK | | 28 | ns |
| $t_{SU}$ | Inputs | Input Setup Time | Before RE of CLK | 7 | | ns |
| $t_{HL}$ | Inputs | Input Hold Time | After RE of CLK | 0 | | ns |
| $t_{WLPD}$ | $\overline{\text{LPCPD}}$ Asserted | $\overline{\text{LPCPD}}$ Active Pulse Width | | 2 | | $t_{CYC}$ |

1. Not tested; guaranteed by characterization.

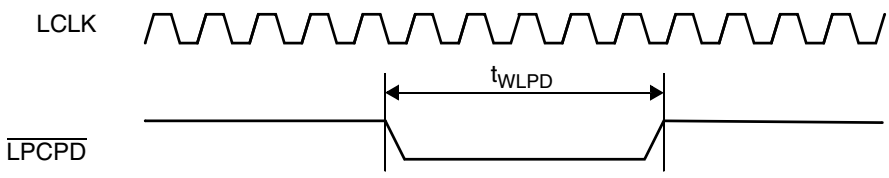
**Outputs**




**Inputs**




**$\overline{\text{LPCPD}}$ Asserted**



## 5.0 Device Specifications (Continued)

### 5.5 PACKAGE THERMAL INFORMATION

Thermal resistance (degrees C/W) $Theta_{JC}$ and $Theta_{JA}$ values for the NPCT42x package are as follows:

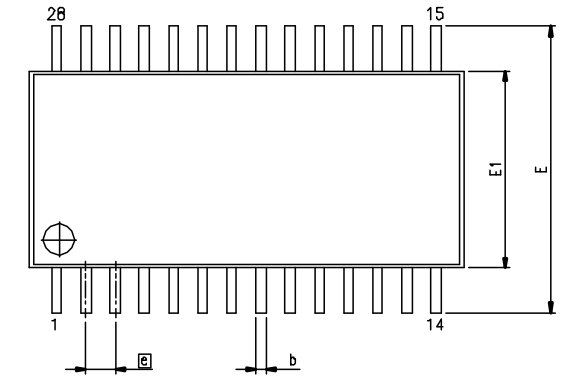
**Table 6. Theta (Θ) J Values**

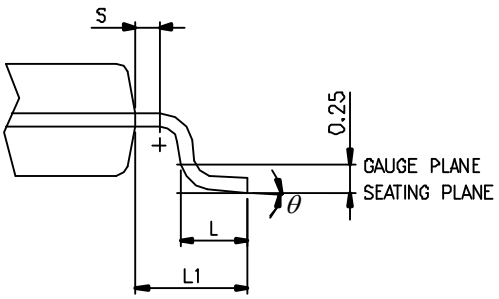
| Package Type | $Theta_{JA}$@0 lfpm | $Theta_{JA}$@150 lfpm | $Theta_{JA}$@250 lfpm | $Theta_{JA}$@500 lfpm | $Theta_{JC}$ |
|---|---|---|---|---|---|
| TSSOP28 | 29 | 27 | 25 | 23 | 10 |

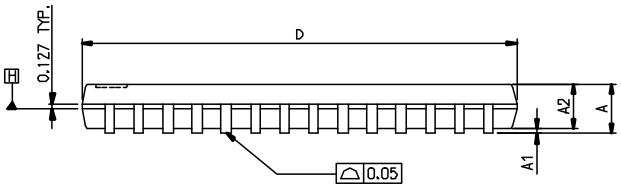
**Note:** Airflow for $Theta_{JA}$ values is measured in linear feet per minute (lfpm).

## Physical Dimensions

All dimensions are in millimeters.




VARIATIONS (ALL DIMENSIONS SHOWN IN MM)

| SYMBOLS | MIN. | NOM. | MAX. |
|---|---|---|---|
| A | – | – | 1.20 |
| A1 | 0.00 | – | 0.15 |
| A2 | 0.80 | 1.00 | 1.05 |
| b | 0.19 | – | 0.30 |
| D | 9.60 | 9.70 | 9.80 |
| E1 | 4.30 | 4.40 | 4.50 |
| E | 6.40 BSC | | |
| e | 0.65 BSC | | |
| L1 | 1.00 REF | | |
| L | 0.45 | 0.60 | 0.75 |
| S | 0.20 | – | – |
| θ | 0° | – | 8° |

**28-Pin Thin Shrink Small Outline Package (TSSOP28), JEDEC**

**Order Numbers: NPCT42xA: NPCT42xAA0WX**
**NPCT42xB: NPCT42xBA0WX**
**NPCT42xC: NPCT42xCA0WX**
**NPCT42xD: NPCT42xDA0WX**
**NPCT42xL: NPCT42xLA0WX**

Note: 'x' = '0' or '1'

**Important Notice**

**Nuvoton products are not designed, intended, authorized or warranted for use as components in systems or equipment intended for surgical implantation, atomic energy control instruments, airplane or spaceship instruments, transportation instruments, traffic signal instruments, combustion control instruments, or for other applications intended to support or sustain life. Furthermore, Nuvoton products are not intended for applications wherein failure of Nuvoton products could result or lead to a situation wherein personal injury, death or severe property or environmental damage could occur.**

**Nuvoton customers using or selling these products for use in such applications do so at their own risk and agree to fully indemnify Nuvoton for any damages resulting from such improper use or sales.**

**Headquarters**
No. 4, Creation Rd. 3,
Science-Based Industrial Park,
Hsinchu, Taiwan, R.O.C
TEL: 886-3-5770066
FAX: 886-3-5665577
http://www.nuvoton.com.tw (Chinese)
http://www.nuvoton.com (English)

**Nuvoton Technology Corporation America**
2727 North First Street,
San Jose, CA 95134, U.S.A.
TEL: 1-408-544-1718
FAX: 1-408-544-1787

**Nuvoton Technology (Shanghai) Ltd.**
27F, 2299 Yan An W. Rd.
Shanghai, 200336 China
TEL: 86-21-62365999
FAX: 86-21-62365998

**Taipei Office**
9F, No.480, Rueiguang Rd.,
Neihu District, Taipei, 114,
Taiwan, R.O.C.
TEL: 886-2-2658-8066
FAX: 886-2-8751-3579

**Winbond Electronics Corporation Japan**
NO. 2 Ueno-Bldg., 7-18, 3-chome
Shinyokohama Kohoku-ku,
Yokohama, 222-0033
TEL: 81-45-4781881
FAX: 81-45-4781800

**Nuvoton Technology (H.K.) Ltd.**
Unit 9-15, 22F, Millennium City 2,
378 Kwun Tong Rd.,
Kowloon, Hong Kong
TEL: 852-27513100
FAX: 852-27552064

For Advanced PC Product Line information contact: APC.Support@nuvoton.com