July 2021
Revision 1.23

NPCT7xx Trusted Platform Module Family 2.0

General Description

The NPCT7xx single-chip Trusted Platform Module (TPM) device, a member of the Nuvoton SafeKeeper™ family, implements the Trusted Computing Group (TCG) specifications for PC-Client TPM, supporting SPI and I²C host interfaces.

The NPCT7xx is designed to reduce system boot time. It provides a security solution for a wide range of applications.

The NPCT7xx is Microsoft® Windows® compliant.

Note: The TPM firmware is composed of two parts:
- Firmware Upgradeable Software (FW-US)
- Firmware Non-Upgradeable Software (FW-NUS)

Features

General

- Single-chip TPM solution; no external parts required
  - Three package options: TSSOP28, QFN32 and UQFN16
- TCG compliance:
  - *TCG PC Client Platform TPM Profile (PTP) Specification; Family 2.0 (Trusted Platform Module Library; Family 2.0)*
- Supports Windows and Linux operating systems.
- Complies with *FIPS 140-2 level 2* and physical security level 3
- Complies with *ISO/IEC 15408 Common Criteria (CC) Version 3.1 Revision 5* with assurance level EAL 4 augmented (certification pending)
- Pre-loaded EK certificate compliant to *TCG Credential Profile; Family 2.0*
- Low standby power consumption
- Up to six Secure General-Purpose I/O (GPIO) pins
  - Dedicated Physical Presence (PP) pin
- Field Upgrade - allows secure firmware updates

Host Interfaces

- PTP-Compliant SPI:
  - Supports 2 KB size FIFO and CRB
  - Up to 64-byte data transfer size
  - Maximum frequency of 54 MHz
  - Five localities
- PTP-Compliant I²C Slave Bus Interface
  - Up to 1 MHz clock
- Peripheral SPI (using TPM-SPI pins)

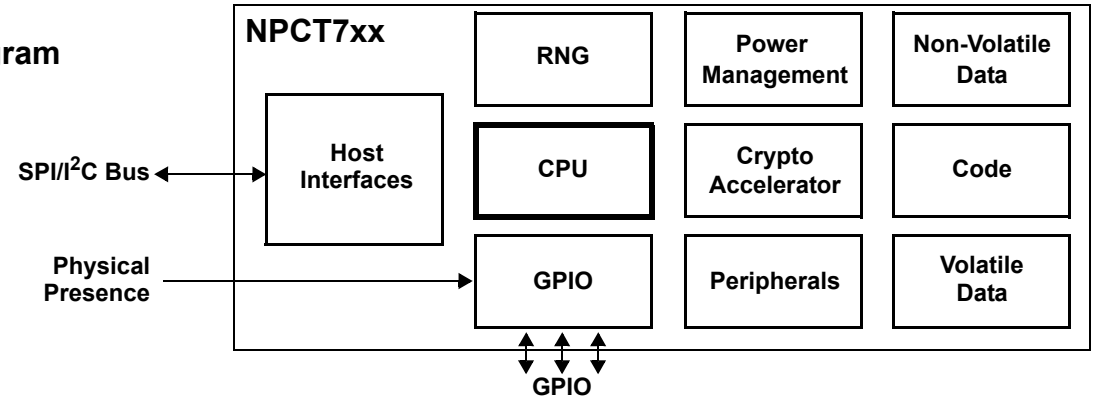
Clocking and Supply

- On-Chip Clock Generator
- Power Supply
  - Separate pins for interface (V_{HIO}) and internal (V_{SB}) power supplies
  - Supply options
    - V_{HIO} = 3.3V or 1.8V
    - V_{SB} = 3.3V or 1.8V
- Temperature options
  - Standard Temp. = 0°C to +70°C
  - Wide Temp. = –40°C to +85°C

Security and Attack Countermeasures

- Defends against:
  - Fault injection attacks
  - Physical attacks
  - Side channel attacks
  - Differential fault analysis attacks
  - RNG attacks
  - Sensor and test mode attacks
  - Dictionary attacks

NPCT7xx Block Diagram



Features (Continued)

Product-Specific Information

The following table lists the products and functionality of the NPCT7xx family. Specify the packaging option in the order form (i.e., "**Tape and Reel packaging**" or "**Tray packaging**").

Order Number[1]	Package[2]	Temperature	TPM 2.0 Library Revision	FW-US Version
NPCT750xAAYX	QFN32	Standard	01.16	7.2.0.1
NPCT750JAAYX[3]	QFN32	Standard	01.16	7.2.0.2
NPCT758xAAYX	UQFN16	Standard	01.16	7.2.0.1
NPCT754xAAYX	QFN32	Wide	01.16	7.2.0.1
NPCT754JAAYX[3]	QFN32	Standard	01.16	7.2.0.2
NPCT75CxAAYX	UQFN16	Wide	01.16	7.2.0.1
NPCT750xACYX	QFN32	Standard	01.16	7.2.0.2
NPCT758xACYX	UQFN16	Standard	01.16	7.2.0.2
NPCT754xACYX	QFN32	Wide	01.16	7.2.0.2
NPCT75CxACYX	UQFN16	Wide	01.16	7.2.0.2
NPCT750xABYX	QFN32	Standard	01.38	7.2.1.0
NPCT758xABYX	UQFN16	Standard	01.38	7.2.1.0
NPCT754xABYX	QFN32	Wide	01.38	7.2.1.0
NPCT75CxABYX	UQFN16	Wide	01.38	7.2.1.0
NPCT750xADYX	QFN32	Standard	01.38	7.2.2.0
NPCT758xADYX	UQFN16	Standard	01.38	7.2.2.0
NPCT754xADYX	QFN32	Wide	01.38	7.2.2.0
NPCT75CxADYX	UQFN16	Wide	01.38	7.2.2.0
NPCT760xAAYX[4]	QFN32	Standard	01.59	7.2.3.0
NPCT768xAAYX[4]	UQFN16	Standard	01.59	7.2.3.0
NPCT764xAAYX[4]	QFN32	Wide	01.59	7.2.3.0
NPCT76CxAAYX[4]	UQFN16	Wide	01.59	7.2.3.0

1. '**x**' = customer-specific letter: H, I, J, L, M, N, R, S, A, V or T.
2. For the TSSOP28 package part number, please contact Nuvoton.
3. Starting from DC 1942.
4. For NPCT76yxAAYX (FW-US ver. 7.2.3.0) part number availability and schedule, please contact Nuvoton.

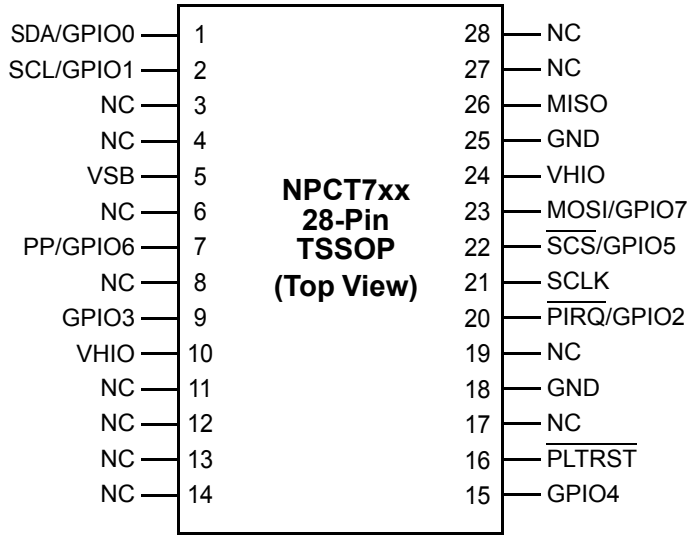
Revision Record

March 2017	Revision 1.0	— Preliminary Datasheet, first revision.
September 2017	Revision 1.1	— Updated Product-Specific Information section. — Updated NV storage size. — Updated Pin Multiplexing table. — Updated maximum leakage current. — Updated SPI clock (SCLK) slew rate. — Updated I2C timing. — Updated QFN marking specification.
October 2017	Revision 1.2	— Fixed typo in Product-Specific Information table.
January 2018	Revision 1.3	— Updated topside marking information (see “Physical Dimensions” starting on page 23).
January 2018	Revision 1.31	— Fixed typo in topside marking information (device name on page 25).
March 2018	Revision 1.4	— Added clarification to t_{SPCSS} and t_{SPCSH} SPI interface timing parameters (Section 2.4.4). — Added the following to Product-Specific Information table (page 2): — “TPM 2.0 Library Revision” column — Four new Product Numbers for TPM 2.0 Library Revision 01.38 support
April 2018	Revision 1.5	— In the Product-Specific Information table (page 2), updated the FW version for the TPM 2.0 Library Revision 01.38 devices.
November 2018	Revision 1.6	— Updated “t_{DIS}” and “Minimum slew rate” in the “Host SPI Interface Timing” table (page 21) and the figure following.
February 2019	Revision 1.7	— Added the following to Product-Specific Information table (page 2): — Four new Product Numbers (...A**C**YX) for firmware version 7.2.0.2.
June 2019	Revision 1.8	— Added the following to Product-Specific Information table (page 2): — Four new Product Numbers (...A**D**YX) for firmware version 7.2.2.0.
August 2019	Revision 1.9	— Added clarification to t_{SB2HIO} parameter description (Section 2.4.2, footnote 2).
December 2019	Revision 1.10	— Added the following to Product-Specific Information table (page 2): — Four new Product Numbers (...A**E**YX) for firmware version 7.2.1.1. — In Section 2.4.3 (“I2C Timing”), added note, at bottom of table, on I2C timeout detection feature.
December 2019	Revision 1.11	— Removed Product Numbers NPCT750xA**E**YX (firmware version 7.2.1.1).
October 2020	Revision 1.20	— Added the following to Product-Specific Information table (page 2): — Four new Product Numbers (NPCT7**6**yxAAYX) for FW version 7.2.3.0. — Prod. Num. NPCT750JAAYX, FW ver. 7.2.0.2 (under NPCT750xAAYX).
October 2020	Revision 1.21	— Product name changed to NPCT7xx. — Added the following to Product-Specific Information table (page 2): — Prod. Num. NPCT754JAAYX, FW ver. 7.2.0.2 (under NPCT754xAAYX).
May 2021	Revision 1.22	— Removed FIPS *140-3*.
July 2021	Revision 1.23	— In General Description, added note that the TPM firmware is composed of two parts: Firmware Upgradable Software (FW-US) and Firmware Non-Upgradeable Software (FW-NUS) — Changed some of the firmware references to “FW-US”.

Table of Contents

1.0 Signal/Pin Connection and Description

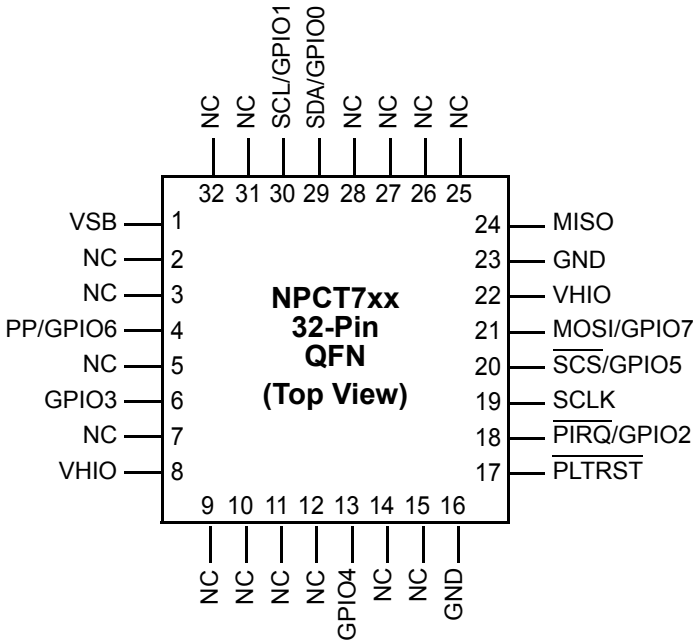
1.1 CONNECTION DIAGRAMS



NC = Not Connected

28-Pin Thin-Shrink Small Outline Package (TSSOP28, 9.7mm x 6.4mm), JEDEC "Green" Package
For further details, see: "Product-Specific Information" on page 2 and "Physical Dimensions of TSSOP28" on page 23

1.0 Signal/Pin Connection and Description (Continued)



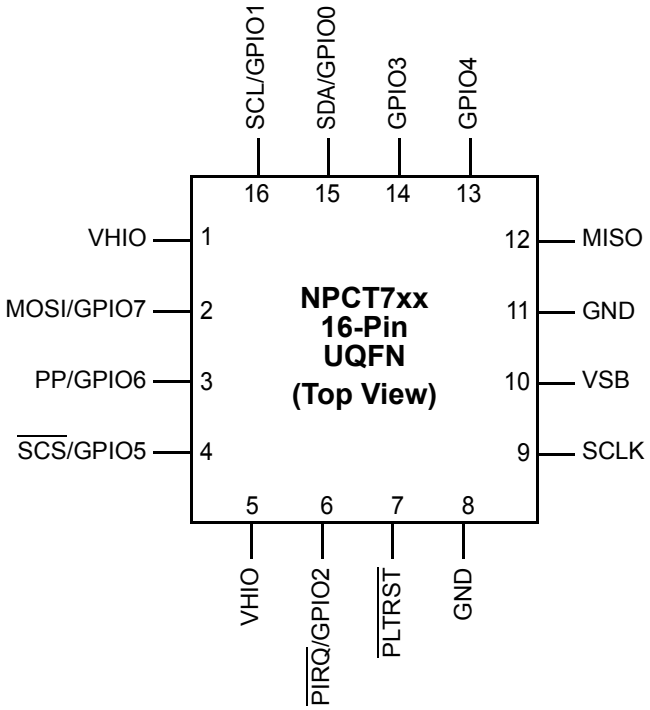
NC = Not Connected

Note: Base Metal (B.M.) on the bottom side of the chip must be connected to GND.

32 Pin Quad Flat No-Lead Package (QFN32, 5mm x 5mm), JEDEC "Green" Package

For further details, see: "Product-Specific Information" on page 2 and "Physical Dimensions of QFN32" on page 24

1.0 Signal/Pin Connection and Description (Continued)



NC = Not Connected

Note: Base Metal (B.M.) on the bottom side of the chip must be connected to GND.

16-Pin Ultra-thin Quad Flat No-Lead Package (UQFN16, 3mm x 3mm), JEDEC "Green" Package

For further details, see: "Product-Specific Information" on page 2 and "Physical Dimensions of UQFN16" on page 25

1.0 Signal/Pin Connection and Description (Continued)

1.2 BUFFER TYPES AND SIGNAL/PIN DIRECTORY

The signal DC characteristics of the pins described in Section 1.3 on page 8 are denoted by buffer type symbols, which are defined in Table 1.

Table 1. Buffer Types

Symbol	Condition	Description
IN_C	V_{HIO} = 3.3V or 1.8V	Input, CMOS/SPI/I^2C compatible; see Section 2.2.1
$O_{p/n}$	V_{HIO} = 3.3V or 1.8V	Output, TTL/CMOS compatible, push-pull buffer capable of sourcing *p* mA and sinking *n* mA; see Section 2.2.2
OD_n	V_{HIO} = 3.3V or 1.8V	Output, TTL/CMOS compatible, open-drain buffer capable of sinking *n* mA; see Section 2.2.3
O_{SPI}	V_{HIO} = 3.3V or 1.8V	Output, SPI 3.3V or 1.8V compatible; see Section 2.2.4
PWR	PWR	Power pin
GND	GND	Ground pin

1.3 SIGNAL/PIN DESCRIPTIONS

This section describes all signals of the NPCT7xx devices. The signals are organized by functional group.

1.3.1 General Purpose Inputs and Outputs (GPIO)

Signal	Pin(s)			I/O	Buffer Type	Power Well	Description
	QFN32	UQFN16	TSSOP28				
PP	4	3	7	I	IN_C	V_{HIO}	**Physical Presence Input.** Indicates owner's physical presence.
GPIO0 GPIO1 GPIO2 GPIO3 GPIO4 GPIO5 GPIO6 GPIO7	29 30 18 6 13 20 4 21	15 16 6 14 13 4 3 2	1 2 20 9 15 22 7 23	I/O	IN_C/OD_4, $O_{4/4}$	V_{HIO}	**General-Purpose I/O Ports.** General-Purpose I/O pins compatible with the *PC Client TPM 2.0 Specification*.

1.3.2 I^2C Interface

Signal	Pin(s)			I/O	Buffer Type	Power Well	Description
	QFN32	UQFN16	TSSOP28				
SCL	30	16	2	I/O	IN_C/OD_8	V_{HIO}	**Serial Clock Input.**
SDA	29	15	1	I/O	IN_C/OD_8	V_{HIO}	**Serial Data I/O.**
$\overline{PIRQ}$	18	6	20	O	OD_4	V_{HIO}	**Parallel Interrupt Request.**

1.0 Signal/Pin Connection and Description (Continued)

1.3.3 SPI Host Interface

Signal	Pin(s)			I/O	Buffer Type	Power Well	Description
	QFN32	UQFN16	TSSOP28				
SCLK	19	9	21	I	IN_C	V_{HIO}	**Serial Clock Input.**
MOSI	21	2	23	I	IN_C	V_{HIO}	**Master Output Slave Input.** TPM serial data in.
MISO	24	12	26	O	O_{SPI}	V_{HIO}	**Master input Slave Output.** TPM serial data out.
$\overline{SCS}$	20	4	22	I	IN_C	V_{HIO}	**SPI Chip Select.**
$\overline{PIRQ}$	18	6	20	O	OD_4	V_{HIO}	**Parallel Interrupt Request.**

1.3.4 Reset

Signal	Pin(s)			I/O	Buffer Type	Power Well	Description
	QFN32	UQFN16	TSSOP28				
$\overline{PLTRST}$	17	7	16	I	IN_C	V_{HIO}	**Platform Reset.** Active low host reset signal. This signal should be connected to the platform reset.

1.3.5 Power and Ground

Signal	Pin(s)			I/O	Buffer Type	Power Well	Description
	QFN32[1]	UQFN16[1]	TSSOP28				
GND	16, 23, B.M.	8, 11, B.M.	18, 25	I	GND		**Ground.** Ground connection for both Core logic and I/O buffers.
VHIO	8, 22	1, 5	10, 24	I	PWR	V_{HIO}	**Host Interface Power Supply.** Powers the I/O buffers of V_{HIO} power well GPIO ports and the Host interface.
VSB	1	10	5	I	PWR	V_{SB}	**Standby Power Supply.** Powers the on-chip Core.

1. Base Metal (B.M.) on the bottom side of the chip must be connected to GND.

1.3.6 NC

Signal	Pin(s)			I/O	Buffer Type	Power Well	Description
	QFN32	UQFN16	TSSOP28				
NC	2, 3, 5, 7, 9, 10, 11, 12, 14, 15, 25, 26, 27, 28, 31, 32	N/A	3, 4, 6, 8, 11, 12, 13, 14, 17, 19, 27, 28				**Not Connected.**

1.0 Signal/Pin Connection and Description (Continued)

1.4 PIN MULTIPLEXING AND RECOMMENDED CONNECTIONS

Signal	Pin(s)			Interface		Internal PU/PD[1]
	QFN32	UQFN16	TSSOP28	SPI	I²C	
SDA[2]/GPIO0	29	15	1	GPIO0	SDA	**PU**[3]
SCL[2]/GPIO1	30	16	2	GPIO1	SCL	**PU**[3]
NC[4]	2, 3, 5, 7, 9, 10, 11, 12, 14, 15, 25, 26, 27, 28, 31, 32	N/A	3, 4, 6, 8, 11, 12, 13, 14, 17, 19, 27, 28	NC		
PP/GPIO6	4	3	7	PP / GPIO6		**PD**
GPIO3	6	14	9	GPIO3		**PU**
GPIO4	13	13	15	GPIO4		**PU**
$\overline{\text{PLTRST}}$	17	7	16	$\overline{\text{PLTRST}}$		
$\overline{\text{PIRQ}}$/GPIO2	18	6	20	$\overline{\text{PIRQ}}$ / GPIO2 / EPU[5]		PU
SCLK	19	9	21	SCLK	EPD[5]/GND	
$\overline{\text{SCS}}$[2]/GPIO5	20	4	22	$\overline{\text{SCS}}$	GPIO5	**PU**[3]
MOSI[2]/GPIO7	21	2	23	MOSI	GPIO7	**PU**[3]
MISO[2]	24	12	26	MISO	NC	**PU**[3]

1. Pull-Up (PU) and Pull-Down (PD) are related to PU_{55}/PD_{55} (as specified in Section 2.3.1 and Section 2.3.2, all pins use the same PU/PD values); **bold** indicates enabled by default, effective t_{SB2ACT} after V_{SB} power-up (see Section 2.4.2).
2. On V_{SB} power-up, both I²C and SPI interfaces are enabled. On NPCT7xx recognition of first host command request (e.g., **`HASH_START`** or **`commandReady`**) the other interface is disabled.
3. Pull-up is disabled if the pin is part of the recognized host interface.
4. Not Connected. Can be connected to any signal on the board or left unconnected.
5. EPU: Connect to external pull-up. EPD: Connect to external pull-down.

2.0 Device Specifications

2.1 GENERAL DC ELECTRICAL CHARACTERISTICS

2.1.1 Recommended Operating Conditions

Symbol	Parameter	Min	Typ	Max	Unit
V_{HIO}	Interface Supply Voltage	3.135	3.3	3.465	V
		1.71	1.8	1.89	V
V_{SB}	Standby Supply Voltage[1]	3.135	3.3	3.465	V
		1.71	1.8	1.89	V
V_{off}	V_{SB} and V_{HIO} power-off voltage [2,3]	-0.3	0	0.5	V
T_A	Operating Temperature - standard	0[3]		+70	°C
T_A	Operating Temperature - wide	-40[3]		+85	°C

1. For UQFN16 package, only the 3.3V range is supported
2. The voltage range for which the respective supply is considered as “off” by the NPCT7xx.
3. Not tested; guarantied by characterization.

2.1.2 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 (GND).

Symbol	Parameter	Conditions	Min	Max	Unit
V_{HIO}	Interface Supply Voltage		-0.3	+3.6	V
V_{SB}	Standby Supply Voltage		-0.3	+3.6	V
V_I	Input Voltage		-0.3	+3.6	V
V_O	Output Voltage		-0.3	+3.6	V
T_{STG}	Storage Temperature		-40	+125	°C
P_D	Power Dissipation			1	W
T_L	Lead Temperature Soldering (10 s)			+260	°C
	ESD Tolerance	C_{ZAP} = 100 pF R_{ZAP} = 1.5 KΩ[1]	2000		V

1. Value based on test complying with RAI-5-048-RA human body model ESD testing.

2.1.3 Capacitance

Symbol	Parameter	Conditions	Min	Max[1]	Unit
C_{IN}	Input Pin Capacitance			6	pF

1. Slew rate > 30 mV/ns; not tested; guaranteed by design

2.0 Device Specifications (Continued)

2.1.4 Power Consumption under Recommended Operating Conditions

Symbol	Parameter	Conditions[1]	Typ[2]	Max[2]	Unit
I_{HIO}	V_{HIO} Supply Current[3]	$0 < V_{IL} < 0.5$, $0.8\ V_{HIO} < V_{IH} < V_{HIO}$,		5	mA
I_{SB}	Max. V_{SB} Supply Current[4]			40	mA
I_{HIOLP}	V_{HIO} Quiescent Supply Current in Idle Mode[5]	$V_{IL} = 0$, $V_{IH} = V_{HIO}$,	18		µA
I_{SBLP}	V_{SB} Quiescent Supply Current in Idle Mode[6]		100		µA

1. All parameters specified for $T_A = 25°C$; V_{SB} = 3.3V or 1.8V and V_{HIO} = 3.3V or 1.8V unless otherwise specified; no resistive load.
2. Not fully tested; characterized only while 0.1 µF and 10 µF capacitors are installed; average over 1 ms period.
3. The specified number relates to a NPCT7xx active state while its interface signals are toggling. Typically, the interface signals toggle rate is very low, therefore, the average current consumption is much lower.
4. The NPCT7xx may enter Idle mode automatically. Therefore, NPCT7xx average power consumption in platform active state (e.g., S0 state in PC) depends on the actual NPCT7xx usage and is typically much lower.
5. The device is not performing any operation; host interface clock is not toggling; V_{HIO} power is on.
6. The device is not performing any operation; host interface clock is not toggling.

2.0 Device Specifications (Continued)

2.2 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 8. The characteristics describe the general I/O buffer types defined in Table 1 on page 8.

2.2.1 Input, CMOS/SPI/I²C Compatible

Symbol: IN_C

Symbol	Parameter	Conditions	Min	Max	Unit
V_{IH}	Input High Voltage	V_{HIO} = 3.3V ±5% or V_{HIO} = 1.8V ±5%	0.7 V_{HIO}	3.6	V
V_{IL}	Input Low Voltage	V_{HIO} = 3.3V ±5% or V_{HIO} = 1.8V ±5%	–0.3	0.3 V_{HIO}	V
I_{ILK}[1]	Input Leakage Current	V_{IN} = 3.3 or V_{IN} = 0		±1	µA

1. Input leakage current includes the output leakage of the bidirectional buffers with TRI-STATE® outputs. For additional conditions, see Section 2.2.5 on page 14.

2.2.2 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	V_{HIO} = 3.3V ±5% I_{OH} = –*p* mA	2.4		V
		V_{HIO} = 1.8V ±5% I_{OH} = –*p* mA	V_{HIO} – 0.4		V
		V_{HIO} = 3.3V ±5% or V_{HIO} = 1.8V ±5% I_{OH} = –100 µA	V_{HIO} – 0.2		V
V_{OL}	Output Low Voltage	V_{HIO} = 3.3V ±5% or V_{HIO} = 1.8V ±5% I_{OL} = *n* mA		0.4	V
		V_{HIO} = 3.3V ±5% or V_{HIO} = 1.8V ±5% I_{OL} = 100 µA		0.2	V
I_{OLK}[1]	Output Leakage Current	V_{OUT} = 3.3 or V_{OUT} = 0		±1	µA

1. Output leakage current includes the input leakage of the bidirectional buffers with TRI-STATE outputs. For additional conditions, see Section 2.2.5 on page 14.

2.2.3 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	V_{HIO} = 3.3V ±5% or V_{HIO} = 1.8V ±5% I_{OL} = *n* mA		0.4	V
		V_{HIO} = 3.3V ±5% or V_{HIO} = 1.8V ±5% I_{OL} = 100 µA		0.2	V
I_{OLK}[1]	Output Leakage Current	V_{OUT} = 3.3 or V_{OUT} = 0		1	µA

1. Output leakage current includes the input leakage of the bidirectional buffers with TRI-STATE outputs. For additional conditions, see Section 2.2.5 on page 14.

2.0 Device Specifications (Continued)

2.2.4 Output, SPI 3.3V and 1.8V

Symbol: O_{SPI}

Symbol	Parameter	Conditions	Min	Max	Unit
V_{OH}	Output High Voltage	V_{HIO} = 3.3V ±5% or V_{HIO} = 1.8V ±5% I_{out} = –100 µA	0.9 V_{HIO}		V
V_{OL}	Output Low Voltage	V_{HIO} = 3.3V ±5% or V_{HIO} = 1.8V ±5% I_{out} = 1500 µA		0.1 V_{HIO}	V
I_{OLK}[1]	Output Leakage Current	V_{OUT} = 3.3 or V_{OUT} = 0		±1	µA

1. Output leakage current includes the input leakage of the bidirectional buffers with TRI-STATE outputs. For additional conditions, see Section 2.2.5 on page 14.

2.2.5 Notes and Exceptions

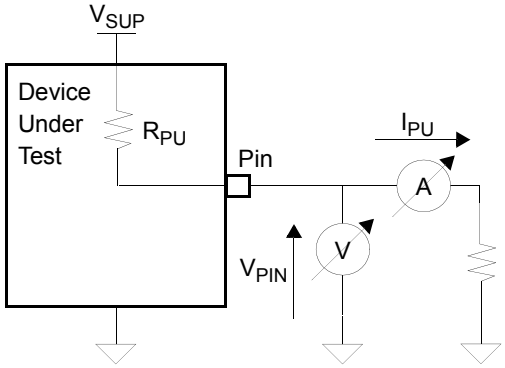
1. I_{ILK} and I_{OLK} are measured in the following cases (where applicable):
   - Internal pull-up or pull-down resistor is disabled
   - Push-pull output buffer is disabled (TRI-STATE)
   - Open-drain output buffer is at high level
2. Some pins have an internal static pull-up resistor (when enabled) and therefore may have leakage current from V_{SUP} (when V_{IN} = 0). See Section 1.4 on page 10 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 10 for a list of the relevant pins.
4. I_{OH} is valid for a GPIO pin only when it is not configured as open-drain.

2.0 Device Specifications (Continued)

2.3 INTERNAL RESISTORS

DC Test Conditions

Pull-Up Resistor Test Circuit



Pull-Down Resistor Test Circuit

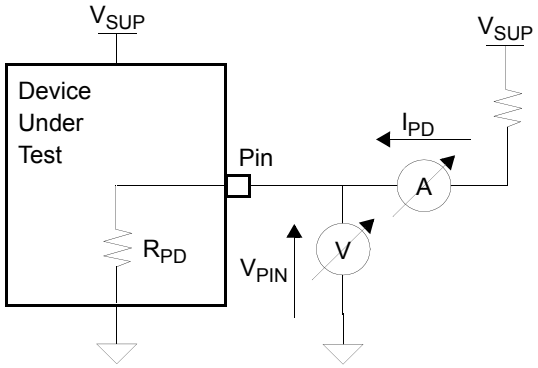
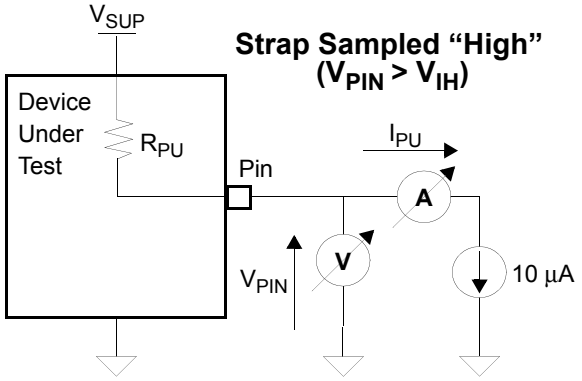


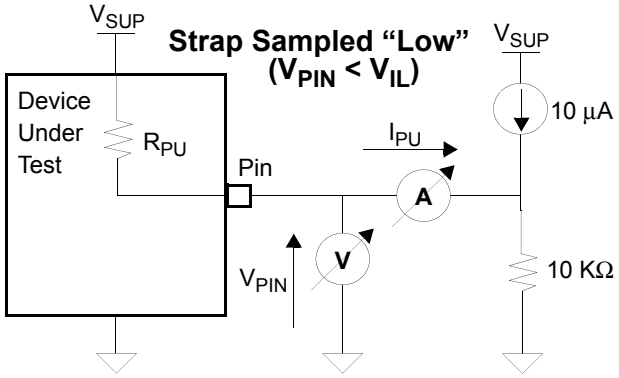
Figure 1. Internal Resistor Test Conditions, T_A = 0°C to 70°C, V_{SUP} = 3.3V or 1.8V

Internal Pull-Up Strap

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

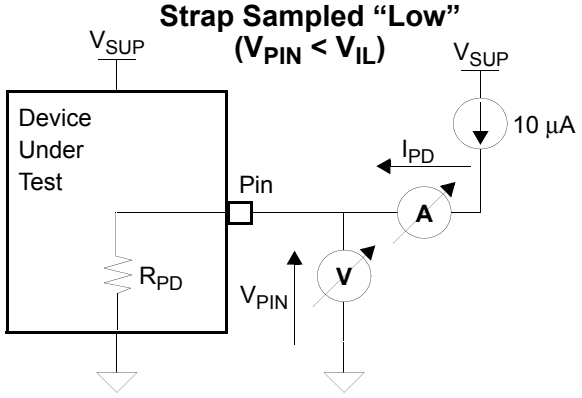


Strap Sampled "Low" ($V_{PIN} < V_{IL}$)



Internal Pull-Down Strap

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



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

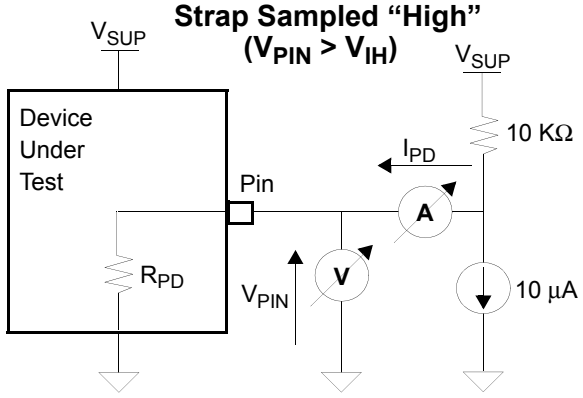


Figure 2. Internal Resistor Design Requirements, T_A = 0°C to 70°C, V_{SUP} = 3.3V or 1.8V

Notes:

1. V_{SUP} is V_{HIO}.
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 $R_{PD} = V_{PIN} / I_{PD}$.

2.0 Device Specifications (Continued)

2.3.1 Pull-Up Resistor

Symbol: PU_{nn}

Symbol	Parameter	Conditions[1]	Min[2]	Typical	Max[2]	Unit
R_{PU}	Pull-up equivalent resistance	V_{SUP} = 3.3.V V_{PIN} = 0V	*nn / 2*	*nn*	*nn * 2*	KΩ
		V_{SUP} = 1.8.V V_{PIN} = 0V	*nn*	*nn * 2*	*nn * 4*	

1. T_A is according to "Recommended Operating Conditions" on page 11.
2. Not tested; guaranteed by characterization.

2.3.2 Pull-Down Resistor

Symbol: PD_{nn}

Symbol	Parameter	Conditions[1]	Min[2]	Typical	Max[2]	Unit
R_{PD}	Pull-down equivalent resistance	V_{SUP} = 3.3.V V_{PIN} = V_{SUP}	*nn / 2*	*nn*	*nn * 2*	KΩ
		V_{SUP} = 1.8V V_{PIN} = V_{SUP}	*nn*	*nn * 2*	*nn * 4*	

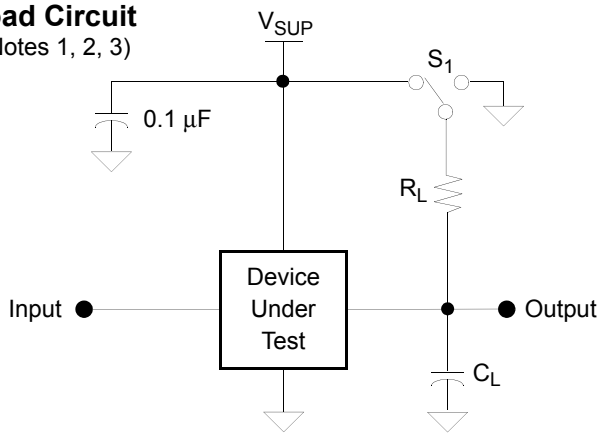
1. T_A is according to "Recommended Operating Conditions" on page 11
2. Not tested; guaranteed by characterization.

2.0 Device Specifications (Continued)

2.4 AC ELECTRICAL CHARACTERISTICS

2.4.1 AC Test Conditions

Load Circuit
(Notes 1, 2, 3)



AC Testing Input, Output Waveform

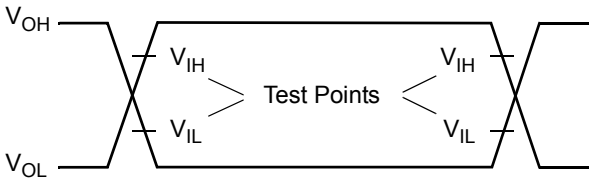


Figure 3. AC Test Conditions, T_A = 0°C to 70°C, V_{SUP} = 3.3V ±5% or V_{SUP} = 1.8V ±5%

Notes:

1. V_{SUP} is V_{HIO}.
2. C_L = 50 pF for all output pins except the following pin groups (values include both jig and oscilloscope capacitance).
   C_L = 400 pF for Standard Mode I2C, 120 pF for Fast mode I2C and Fast mode Plus I2C.
   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 2.4: 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).

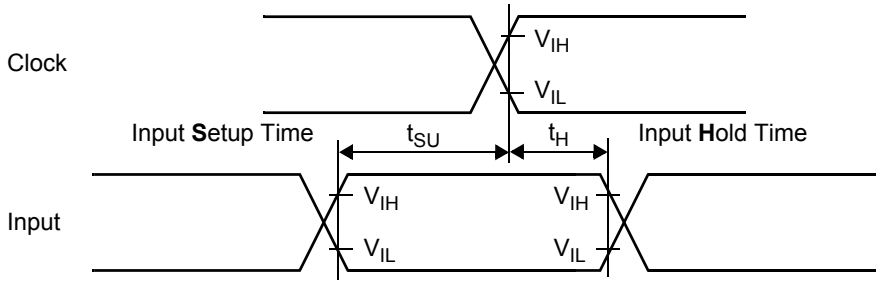


Figure 4. Input Setup and Hold Time

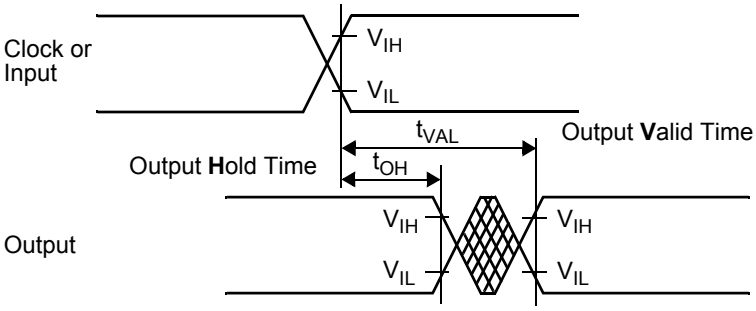


Figure 5. Clock-to-Output and Propagation Delay

2.0 Device Specifications (Continued)

2.4.2 Power and Reset Timing

Symbol	Description	Min[1]	Max[1]
t_{SB2HIO}	V_{SB} power-up to V_{HIO} power-up[2]	0	
t_{SB2RS}	V_{SB} power-up to $\overline{PLTRST}$ deassertion (rise)	5 ms	
t_{SRST}	V_{HIO} power-up to $\overline{PLTRST}$ deassertion (rise)	1 ms	
t_{RSHL}	$\overline{PLTRST}$ assertion to V_{HIO} power-down	0	
t_{RSRF}	$\overline{PLTRST}$ rise and fall time between 0.2 V_{HIO} and 0.8 V_{HIO}[3,4]		5 µs
t_{IORF}	V_{HIO} rise and fall time between 0.8V and 1.6V [4,5]		20 ms
t_{WRS}	Warm reset duration	100 ns	
t_{SB2ACT}	V_{SB} power-up to first TPM transaction	100 ms	
t_{SBR}	V_{SB} rise time from 1.4V to 1.7V [4]	5 µs	3 ms
t_{SBF}	V_{SB} fall time from 1.7V to 1.4V [4,5]	25 µs	20 ms

1. Not Tested; guaranteed by design.
2. V_{SB} and V_{HIO} can be driven by the same source. In such a case, t_{SB2HIO} is defined from V_{SB} start rise to V_{HIO} start rise. In all other cases, t_{SB2HIO} is defined from V_{SB} being stable high to V_{HIO} start rise.
3. In case of power fail, $\overline{PLTRST}$ may be asserted (active low) together with V_{HIO} power negation, but should not at any point exceed V_{HIO} power level.
4. Voltage change within this range must be **monotonic**.
5. When voltage goes below the lower limit, it must not go above it within less than 5 ms.

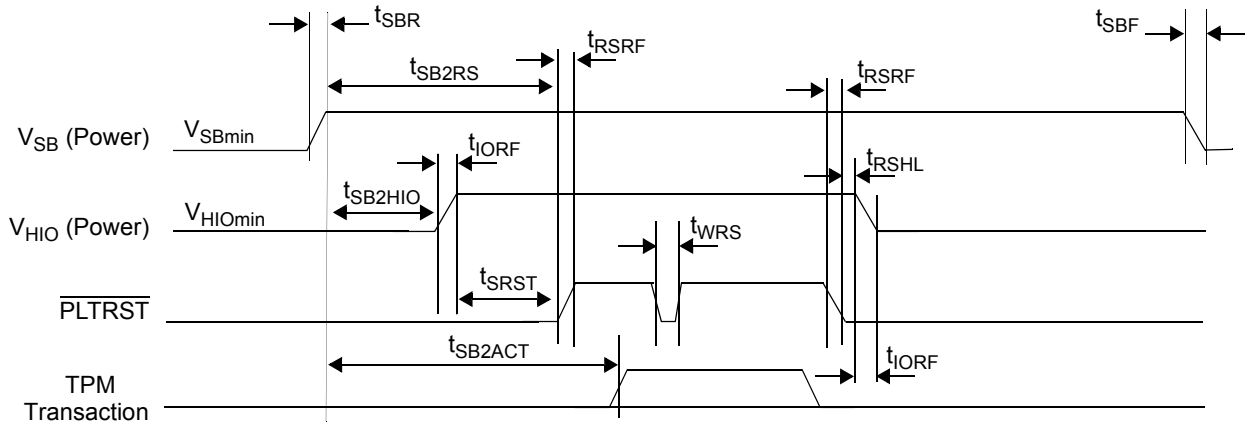


Figure 6. Power and Reset Timing Diagram

2.0 Device Specifications (Continued)

2.4.3 I2C Timing

Symbol[1]	Fig.	Description	Reference Conditions	Std. (100 KHz)		Fast (400 KHz)		Fast-Plus (1 MHz)		Units
				Min	Max	Min	Max	Min	Max	
Input Timing										
F_{SCLI}	7	SCL frequency	At V_{IL} SCL FE to FE		100		400		1000	KHz
t_{SCLLI}	7	SCL low time	At V_{IL} (Both Edges)	4.7		1.3		0.5		µs
t_{SCLHI}	7	SCL high time	At V_{IH} (Both Edges)	4		0.6		0.26		µs
t_{SMBRI}	7	SCL, SDA rise time	From V_{IL} to V_{IH}[2]		1000[3]		300[3]		120[3]	ns
t_{SMBFI}	7	SCL, SDA fall time	From V_{IH} to V_{IL}[2]		300[3]	12	300[3]	12	120[3]	ns
t_{SDASI}	8	SDA setup time	Before SCL RE	250		100		50		ns
t_{SDAHI}	8	SDA hold time	After SCL FE	0		0		0		ns
t_{CSTRSI}	10	SCL setup time	Before Restart condition	4.7		0.6		0.26		µs
t_{CSTRHI}	9, 10	SCL hold time	After Start/Restart condition	4		0.6		0.26		µs
t_{CSTOSI}	9	SCL setup time	Before Stop condition	4		0.6		0.26		µs
t_{BUFI}	9	Bus free time	Between Stop and Start conditions	4.7		1.3		0.5		µs
Output Timing										
F_{SCLO}	7	SCL frequency	At V_{IL} SCL FE to FE		100		400		1000	KHz
t_{SCLLO}	7	SCL low time	At V_{IL} (Both Edges)	4.7		1.3		0.5		µs
t_{SCLHO}	7	SCL high time	At V_{IH} (Both Edges)	4		0.6		0.26		µs
t_{SMBRO}	7	SCL, SDA rise time	From V_{IL} to V_{IH}[2]		1000[3]		300[3]		120[3]	ns
t_{SMBFO}	7	SCL, SDA fall time	From V_{IH} to V_{IL}[2]		250[3]		250[3]		120[3]	ns
t_{SDAHO}	8	SDA hold time	After SCL FE	0		0		0		ns
t_{SDALVO}	8	SDA low valid time	After SCL FE		3.45		0.9	0.26	0.45	µs
t_{SDAHVO}	8	SDA high valid time	After SCL FE		3.45		0.9	0.26	0.45	µs
t_{CSTRSO}	10	SCL setup time	Before Restart condition	4.7		0.6		0.26		µs
t_{CSTRHO}	9, 10	SCL hold time	After Start/Restart condition	4		0.6		0.26		µs
t_{CSTOSO}	9	SCL setup time	Before Stop condition	4		0.6		0.26		µs
t_{BUFO}	9	Bus free time	Between Stop and Start conditions	4.7		1.3		0.5		µs

1. Only slave mode is supported. Not all input and output parameters are relevant for slave mode.
2. Test conditions: R_L = 1 KΩ to V_{HIO} = 3.3V, Standard: C_L = 400 pF to GND, Fast, Fast Plus: C_L = 120 pF to GND.
3. Not tested; based on design simulation.

Notes:

- In the preceding table and in Figure 7 through Figure 10, an “O” is added to parameter names for output signals and an “I” for input signals.
- Nuvoton TPM 2.0, FW-US versions 7.2.2.0 and higher, implements the I2C timeout detection feature. A timeout condition is detected while SCL is stalled low continuously for more than 25 ms or if the time from start condition to stop condition takes more than 35 ms.

2.0 Device Specifications (Continued)

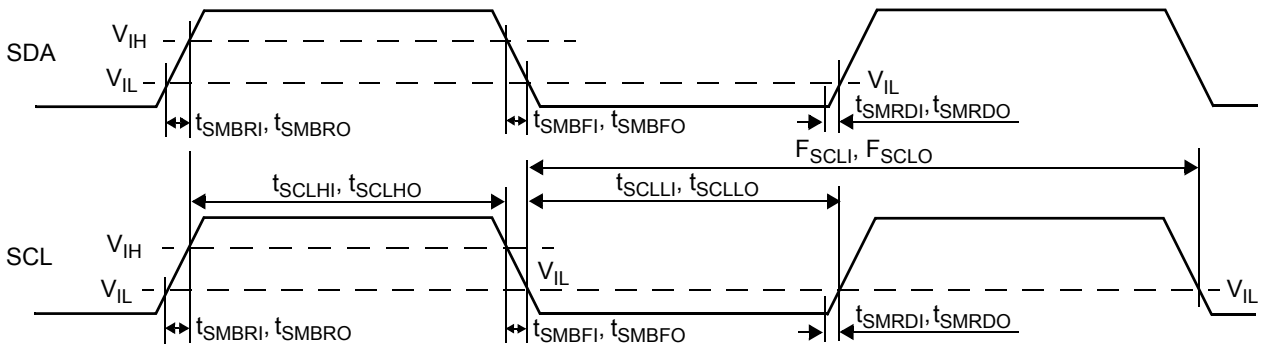


Figure 7. I2C Signal (SDA and SCL) Timing

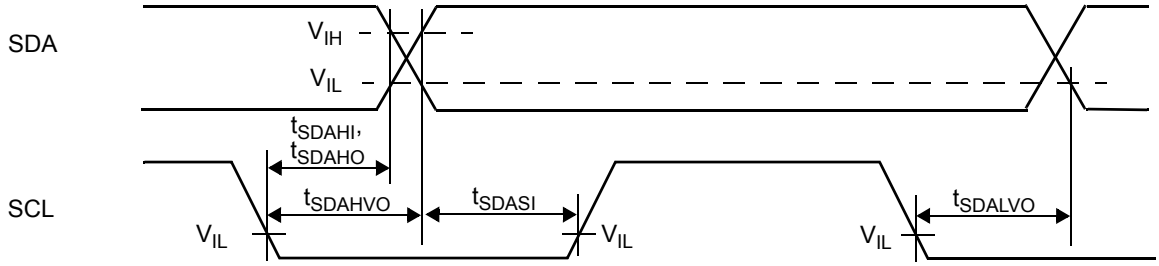


Figure 8. I2C Data Bit Timing

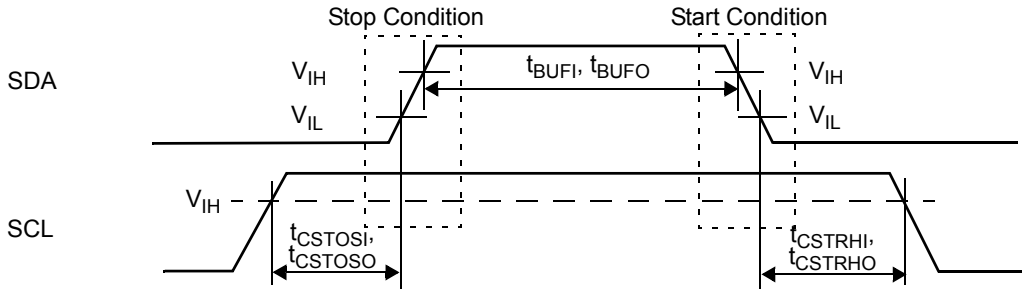


Figure 9. I2C Start and Stop Condition Timing

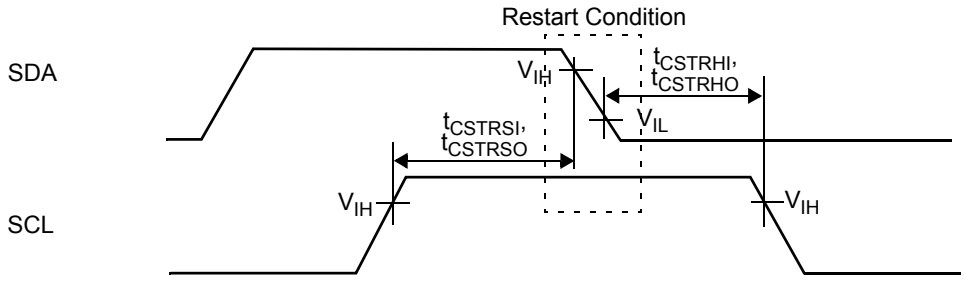


Figure 10. I2C Restart Condition TIming

2.0 Device Specifications (Continued)

2.4.4 TPM SPI Host Interface Timing

Symbol	Figure	Description[1]	Reference Conditions	Min	Max	Units
f_{SPCK}	11	SCLK frequency	V_{HIO} =3.3V ±5%; from RE to RE	2	54	MHz
			V_{HIO} =1.8V ±5%; from RE to RE			
–	11	SCLK slew rate	V_{HIO} = 3.3V ±5% From 0.2 * V_{HIO} to 0.8 * V_{HIO}	1[2]	4	V/ns
			V_{HIO} = 1.8V ±5% From 0.2 * V_{HIO} to 0.8 * V_{HIO}	0.6[3]	4	V/ns
t_{SPCK}	11	SCLK cycle time	From RE to RE	$1/f_{SPCK}$ - 5%	$1/f_{SPCK}$ + 5%	ns
t_{SPCKH}	11	SCLK high time	At V_{IH} (Both Edges), f_{SPCK}>36MHz	0.3 x t_{SPCK}	0.5 x t_{SPCK}	ns
			At V_{IH} (Both Edges), f_{SPCK}<=36MHz	0.4 x t_{SPCK}	0.6 x t_{SPCK}	ns
t_{SPCKL}	11	SCLK low time	At V_{IH} (Both Edges), f_{SPCK}>36MHz	0.5 x t_{SPCK}	0.7 x t_{SPCK}	ns
			At V_{IL} (Both Edges), f_{SPCK}<=36MHz	0.4 x t_{SPCK}	0.6 x t_{SPCK}	ns
t_{SPSU}	11	MOSI setup time at slave input	At V_{IH}/V_{IL} before RE SCLK	2		ns
t_{SPHL}	11	MOSI hold time at slave input	At V_{IH}/V_{IL} after RE SCLK	3		ns
t_{SPVAL}	11	MISO valid time at slave output	At V_{IH}/V_{IL} after FE SCLK	0	6	ns
t_{SPCSS}	11	$\overline{SCS}$ fall to clock rise time at slave input[4]	From $\overline{SCS}$ V_{IL} to SCLK V_{IL}	5		ns
t_{SPCSH}	11	Clock fall to $\overline{SCS}$ rise time at slave input[5]	From SCLK V_{IL} to $\overline{SCS}$ V_{IL}	5		ns
t_{SPCS}	11	$\overline{SCS}$ high time	From RE to FE	50		ns
t_{DIS}	11	MISO disable time	$\overline{SCS}$ rise to MISO HI-Z		20	ns
–		MISO capacitive load		0	50	pF

1. Not tested; guaranteed by characterization.
2. Minimum slew rate of 0.6 V/ns is allowed if: f_{SPCK} max = 40 MHz, t_{SPSU} min = 3 ns and t_{SPVAL} max = 7 ns.
   Minimum slew rate of 0.3 V/ns is allowed if: f_{SPCK} max = 33 MHz, t_{SPSU} min = 4 ns and t_{SPVAL} max = 9 ns.
3. Minimum slew rate of 0.2 V/ns is allowed if: f_{SPCK} max = 33 MHz, t_{SPSU} min = 4 ns and t_{SPVAL} max = 9 ns.
   Minimum slew rate of 0.1 V/ns is allowed if: f_{SPCK} max = 17 MHz, t_{SPSU} min = 7 ns and t_{SPVAL} max = 14 ns.
4. SCLK must be low from before $\overline{SCS}$ fall until the first SPI transaction's SCLK rise.
5. SCLK must be low from the last SPI transaction's SCLK fall until after $\overline{SCS}$ rise.

2.0 Device Specifications (Continued)

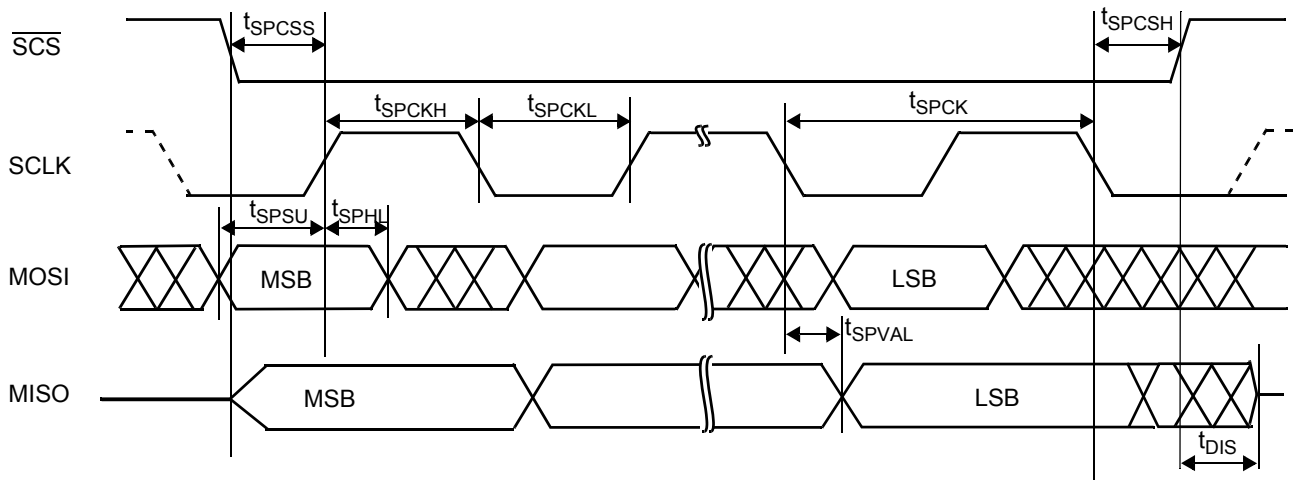


Figure 11. Host SPI Interface Timing

2.5 PACKAGE THERMAL INFORMATION

Thermal resistance (degrees C/W) $Theta_{JC}$ and $Theta_{JA}$ values for the NPCT7xx package are as follows:

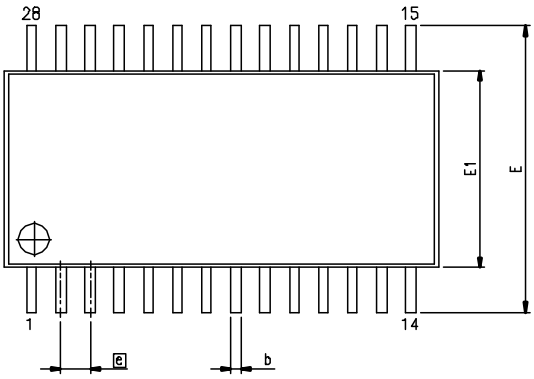
Table 2. Theta (Θ) J Values

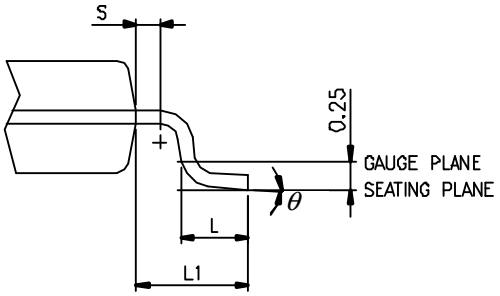
Package Type	$Theta_{JA}$@0 lfpm	$Theta_{JA}$@150 lfpm	$Theta_{JA}$@250 lfpm	$Theta_{JA}$@500 lfpm	$Theta_{JC}$
TSSOP28	29	27	25	23	10
QFN32	36	34.6	32.2	30.8	4.3
UQFN16	77.4				49.1

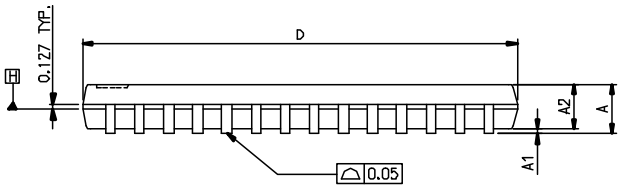
Note: Airflow for $Theta_{JA}$ values is measured in linear feet per minute (lfpm).

Physical Dimensions of TSSOP28

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	0.90	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 "Green" Package
Order Numbers: See "Product-Specific Information" on page 2

Device topside mark specification:

1st Line: **Nuvoton Company Logo.**

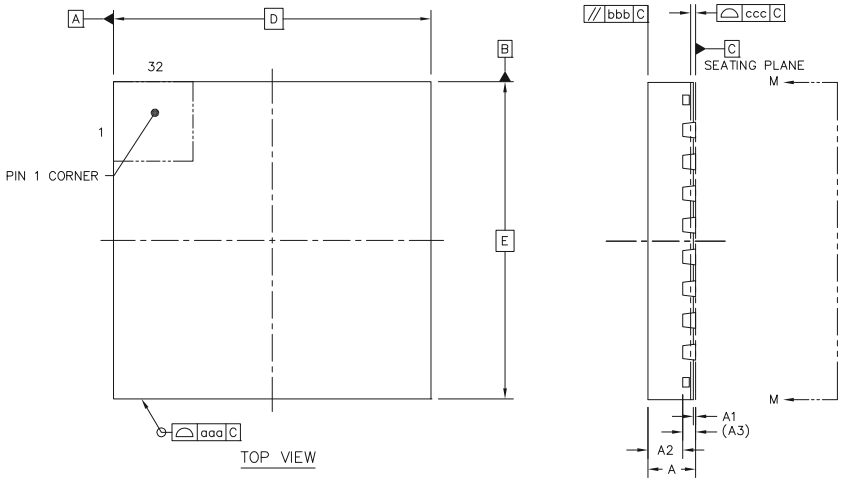
2nd Line: **Part number.**

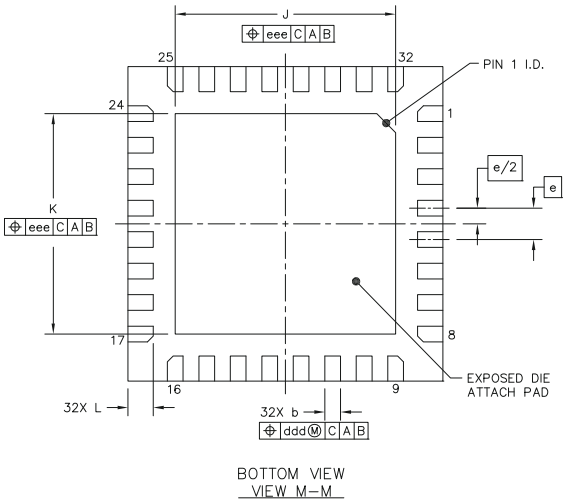
3rd Line: **('XX...XX') Nuvoton proprietary tracking information.**

4th Line: **'YWW' is the date code where 'Y' is the last digit of the year and 'WW' is the week in that year. For example, '112' indicates that device assembly was done in 2021, in week 12 of the year.**
'XXXX' is Nuvoton proprietary information.

Physical Dimensions of QFN32

Control dimensions are in millimeters.





		SYMBOL	MIN	NOM	MAX
TOTAL THICKNESS		A	0.7	0.75	0.8
STAND OFF		A1	0	0.035	0.05
MOLD THICKNESS		A2	---	0.55	0.57
L/F THICKNESS		A3		0.203 REF	
LEAD WIDTH		b	0.2	0.25	0.3
BODY SIZE	X	D		5 BSC	
	Y	E		5 BSC	
LEAD PITCH		e		0.5 BSC	
EP SIZE	X	J	3.4	3.5	3.6
	Y	K	3.4	3.5	3.6
LEAD LENGTH		L	0.35	0.4	0.45
PACKAGE EDGE TOLERANCE		aaa		0.1	
MOLD FLATNESS		bbb		0.1	
COPLANARITY		ccc		0.08	
LEAD OFFSET		ddd		0.1	
EXPOSED PAD OFFSET		eee		0.1	

NOTES

1.0 COPLANARITY APPLIES TO LEADS, CORNER LEADS AND DIE ATTACH PAD.

32-Pin Quad Flat No-Lead (QFN32) “Green” Package
Order Numbers: See ”Product-Specific Information” on page 2

Device topside mark specification:

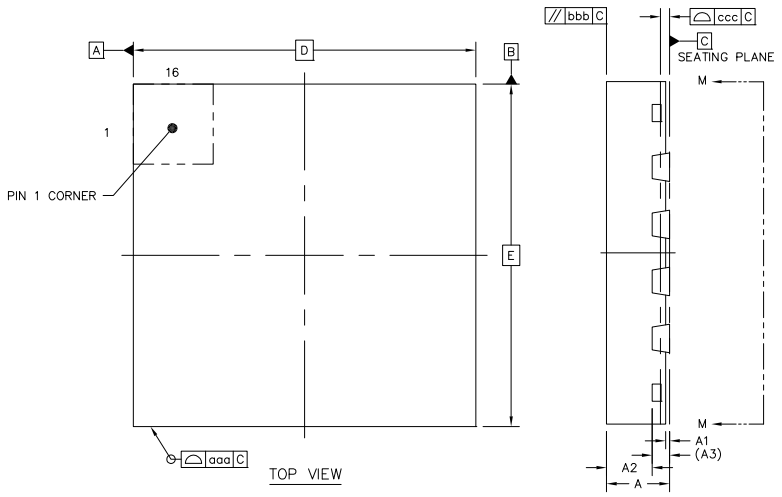
1st & 2nd Lines: **Part number.**

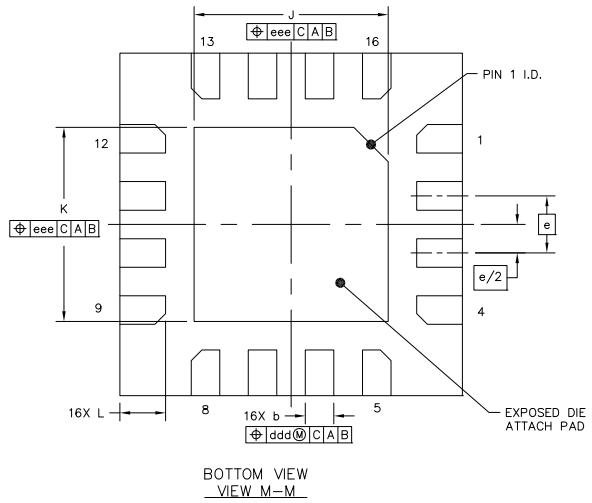
2nd Line: **‘YWW’ is the date code, where ‘Y’ is the last digit of the year and ‘WW’ is the week in that year. For example, ‘112’ indicates that device assembly was done in 2021, in week 12 of the year.**

3rd & 4th Lines: **(‘XX...XX’) Nuvoton proprietary tracking information.**

Physical Dimensions of UQFN16

Control dimensions are in millimeters.





		SYMBOL	MIN	NOM	MAX
TOTAL THICKNESS		A	0.5	0.55	0.6
STAND OFF		A1	0	0.035	0.05
MOLD THICKNESS		A2	---	0.4	0.425
L/F THICKNESS		A3		0.152 REF	
LEAD WIDTH		b	0.2	0.25	0.3
BODY SIZE	X	D		3 BSC	
	Y	E		3 BSC	
LEAD PITCH		e		0.5 BSC	
EP SIZE	X	J	1.6	1.7	1.8
	Y	K	1.6	1.7	1.8
LEAD LENGTH		L	0.35	0.4	0.45
PACKAGE EDGE TOLERANCE		aaa		0.1	
MOLD FLATNESS		bbb		0.1	
COPLANARITY		ccc		0.08	
LEAD OFFSET		ddd		0.1	
EXPOSED PAD OFFSET		eee		0.1	

NOTES

1.0 COPLANARITY APPLIES TO LEADS, CORNER LEADS AND DIE ATTACH PAD.

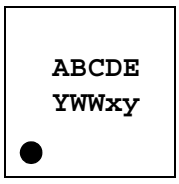
16-Pin Ultra-thin Quad Flat No-Lead (UQFN16) “Green” Package
Order Numbers: See ”Product-Specific Information” on page 2

Device topside mark specification:

ABCDE: **Characters 6-10 of the device part number (e.g., “58AAA” for the NPCT758AAAYX device).**

YWW: **Date code, where ‘Y’ is the last digit of the year and ‘WW’ is the week in that year. For example, ‘112’ indicates that device assembly was done in 2021, in week 12 of the year.**

xy: **Nuvoton proprietary tracking information.**



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.

CONTACT INFORMATION

For Nuvoton Sales Offices in your region, visit us at:

https://www.nuvoton.com/buy/worldwide-sales-offices/

For Cloud Computing Product Line information, contact:

CloudComputing@nuvoton.com