

TRNG98

Preliminary Product Specification

GENERAL DESCRIPTION

The TRNG9880 True Random Number Generator is an SMT module to provide a high reliability source of true bias-free random numbers. The TRNG9880 is made for SMT mounting. The TRNG9880 is driven by a 3.0V-5.0V supply. Six standard pads are provided for power and communication on the module. In addition the device has four test pads that enable easy evaluation and hardware testing. The random numbers are transferred from the module by a digital serial SPI-slave interface. The generated random numbers, that origins in a physical random process, is thoroughly processed and tested for anomalies and bias, before they are transferred to the digital output part of the module.

FEATURES

- 3.0V to 5.0V Power supply
- SMT machine mountable
- Delivered on sticks
- Output random numbers pass any statistical test
- Bit Serial Synchronised Output (SPI-Slave)
- On-line testing of random numbers
- Error Detect pad
- 50 kbit output rate
- Special test pads enable in circuit validation
- Fail-safe internal reset circuit guarantee sustained operation
- Metal EMI/RFI shielding
- 26.5mm x 14.5mm x 3.0mm size

APPLICATIONS

Encryption & Security: PKI accelerators, Key distribution, Session key, and initialisation vector generation.

Gaming applications: Gaming machines, Lottery machines, Lotto number generators.

Network Security: Link encryption modules, Encrypted Radio, Virtual Private Network, Telecom applications.

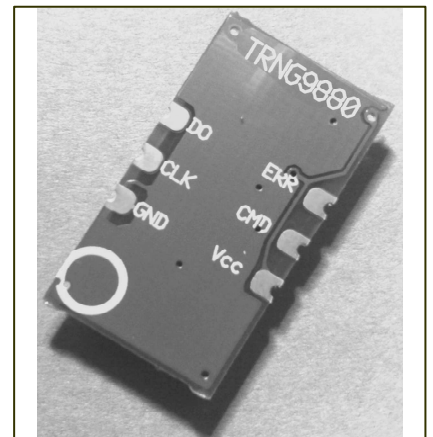
ABSOLUTE MAXIMUM RATINGS

	MINIMUM	MAXIMUM	UNIT
ESD Tolerance (HBM)	1.5		kV
Ambient Temperature with power applied	-40	80	°C
Storage temperature	-40	80	°C
Supply voltage on Vcc relative to GND	-0.4	+5.6	V
DC input voltage (input pad)	-0.4	Vcc +0.4	V
Maximum current on Vcc pad	-1	30	mA
Maximum current on any other pad	-10	10	mA
Convection Reflow Soldering (20 sec)		235	°C

PINOUT AND CONNECTION DIAGRAM

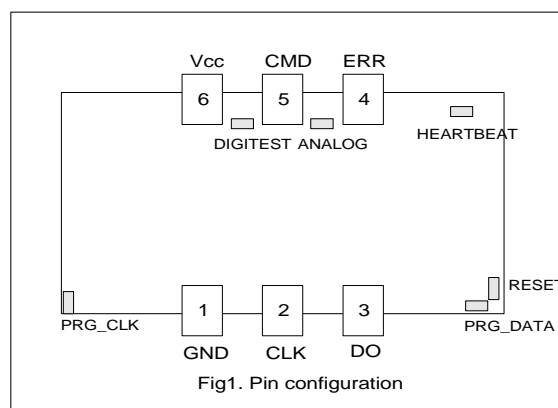
BOTTOM SIDE SMT PADS

PAD NO	NAME	CONNECTION	FUNCTION
1	GND	IN	Ground connection
2	CLK	IN	Input serial clock
3	DO	OUT	Data Out
4	ERR	IN/OUT	Device Error Signal
5	CMD	IN/OUT	Device Command
6	Vcc	IN	Power Supply



TOP SIDE TEST PADS

NAME	DIR	FUNCTION
PRG_DATA	IN/OUT	Reserved for special purpose
RESET	IN/OUT	Reset detect or reset control pad
HEARTBEAT	OUT	Heartbeat signal from digital block
ANALOG	OUT	Analogue noise signal
DIGITEST	OUT	Raw digital stream after sampling
PRG_CLK	Reserved	Reserved for production



POWER SUPPLY

DC SPECIFICATION

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Minimum supply voltage		2.70		V	20 degrees °C
Supply Current			30	mA	
Supply Voltage 3.3 Volts	3.0	3.3		V	
Supply Current 2.5 Volts		8.8		mA	Operating at 20 degrees °C
Supply Current 3.0 Volts		11.5		mA	
Supply Current 3.3 Volts		12.7		mA	
Supply Current 3.5 Volts		13.3		mA	
Supply Current 3.3 Volts		2.1		mA	Device held in reset
Supply Current 3.3 Volts		1.5		mA	Device in low power mode
Supply Voltage 5.0 Volts		5.0	5.5	V	
Supply Current 4.5 Volts		15.3		mA	
Supply Current 5.0 Volts		16.5		mA	
Supply Current 5.5 Volts		18.1		mA	
Supply Current 5.0 Volts		3.8		mA	Device held in reset
Supply Current 5.0 Volts		1.7		mA	Device in low power mode
Ambient Temperature	-40		+70	°C	3.3 V supply
Ambient Temperature	-40		+85	°C	5.0 V supply

Supply current will increase if a communication pad draw or sink current into the device. At high ambient temperature and low supply voltage the unit will report an error if the analogue noise source fail.

AC SPECIFICATION

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Supply maximum drive impedance		2	50	Ω	
Ripple from TRNG9880 on Vcc pad		1.6		mA	Amplitude (0Hz-500MHz) Communication pads open

TRNG9880 Vcc min harmonic ripple rejection for Vcc =3.3V:

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Supply voltage ripple rejection	300			mV	Narrow band harmonic disturbance 0Hz-200Hz.
Supply voltage ripple rejection	100			mV	Narrow band harmonic disturbance 200Hz-1.0MHz.

The TRNG9880 have a 200nF capacitor on the Vcc internally. This will be sufficient Vcc decoupling for most application areas.

COMMUNICATION SPI-S PADS

SPI-S PADS DC SPECIFICATION

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Digital input low voltage	-0.4	0.0	0.8	V	
Digital input high voltage	2.2	V _{CC}	V _{CC} +0.4V	V	
Digital output low voltage			0.5	V	Sink 10 mA
Digital output high voltage	V _{CC} -1.1			V	Source 10 mA
Digital output low sink current			10	mA	May sink 25 mA at 0.75V if modest operating temperature
Digital output high source			10	mA	May source 10 mA max

A digital 'zero' is encoded as a low voltage and a digital 'one' as a high voltage. The input DC specification is 5.0V TTL compatible and 3.3V + 5.0V CMOS compatible. At V_{CC}=3.3V the inputs are **not** 5.0V tolerant. Digital output buffer type is CMOS output driver with high/low drive. The digital output pads are "DO" and "DIGITEST". A typical digital input pad is the "CLK" clock input pad.

SPI-S PADS AC SPECIFICATION

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Digital input hysteresis voltage		60		mV	
Digital CLK input low time	50		Infinite	ns	
Digital CLK input high time	50		Infinite	ns	
Random number generation	20	50	60	kbits/s	Continuous output supported
Output from internal buffer		450		kbits/s	240 bits may be read at high speed
Output SPI-S data rate	0		10000	kbits/s	8 bits or less may be read at high speed
TRNG9880 start up time	1.5	2	5	s	Power on -> to running unit

The SPI-S support a high data rate of 10Mbits/s. The TRNG9880 cannot produce random number at this speed or update status bits as CMD or ERR pads. An application may, however, safely run the SPI-S at 10Mbits/s for one byte (8 bits), and then allow sufficient time for the TRNG9880 to reload the SPI-S with a new byte of random numbers and to update CMD and ERR pads. If the application overrun the TRNG9880 the SPI-S will be filled with zeroes and the ERR pad will go low. A synchronisation problem may exist if the TRNG9880 and the application do not agree on which clock flank represent the first bit of a byte, producing a one-time error.

The TRNG9880 have a 29 bytes internal buffer that can serve the application at 450 kbits/s. If the 8-bit byte rate remain below this rate individual bytes may still be transferred at 10Mb/s. If the buffer go empty the TRNG9880 will signal an error by driving the ERR pad low.

The DO pad is updated (changed) on the rising flank of the clock (CLK pad). The CLK idle state is low. Data is sent MSB bit first and LSB bit last. The normal output is a byte in range 0 to 255 (decimal) 0x00 to 0xFF (hex) with flat distribution; with all 256 values equally probable.

If the TRNG9880 runs with a slow clock, care should be taken so that not a series of high-frequency glitches overrun the SPI-S so that a zero bit is read. An NP0 capacitor may be mounted between CLK and GND close to the TRNG9880, to reduce the AC ripple voltage on the CLK pad. **The SPI-S may clock on a pulse as short as 20 ns.**

In case of an error (ERR pad driven low) the SPI-S will output zeroes (low voltage) on the DO pad. Depending on the application it may be wise to check that the random output contain both ones and zeroes. As an example: If the application need a 64 bit random number the value of all zeroes 00....000....000 may be rejected in the application as an TRNG9880 error. The application may, for test purposes, obtain extra bits of randomness, and check for the all zeroes error, in case the requested block is short.

COMMUNICATION CONTROL AND ERROR PADS: "CMD" "ERR"**CMD+ERR PADS DC SPECIFICATION**

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Input low voltage	-0.4	0.0	0.8	V	
Input high voltage	2.2	V _{CC}	V _{CC} +0.4V	V	
Output low voltage			0.5	V	Sink 10 mA
Output high impedance	4	5.6	8	k Ω	Drive resistance connected to V _{CC}
Output low sink current			10	mA	May sink 25 mA at 0.75V if modest operating temperature
Output high source	V _{CC} /8	V _{CC} /5.6	V _{CC} /4	mA	Output signal grounded to 0V
Output high source	0.12	0.17		mA	Output signal at V _{CC} -1.0V
ERR (when pull-down output) sink	0.06	0.08		mA	Output signal at 0.5V

The CMD and ERR pads are configured with a strong drive-low and a pull-up 5.6k resistor. This enables bi-directional communication on the pads. The normal voltage for CMD and ERR is high. If ERR is low the output (DO pad) may be faulty or have been so for a short while. When the ERR pad is detected low the application shall stop the CLK clock.

During some error conditions the ERR pad will be a pull-down pad (with 5.6 k Ω resistance (Typical)). Therefore should the application connect to the ERR pad using a sufficiently high impedance so that ERR == low is detected at all times. An example of a condition when ERR pad is a pull-down pad is when the TRNG9880 is in reset or when V_{CC} is below the operating range.

TRNG9880 LOW POWER MODE

Holding ERR low will put the TRNG9880 in a low-power mode. Access to the low power mode is available for TRNG9880 operating modes where the ERR pad is high. Should the ERR pad be low due to an error or a command, an external "low" on the ERR pad cannot be detected. The low power mode can also be entered by a command on the CMD pin.

When in low-power mode the pull-up resistor of ERR will be turned off. Some other pads will also be set to high impedance. The application is responsible for keeping the ERR pad low, and not to confuse the low power mode with an operating device.

The application must lift the ERR pad to high to resume normal operation. The TRNG9880 should be expected to immediately drive the ERR pad low upon restart. It is recommended to install a current limiting resistor between the application and the TRNG9880 should the application lack resistor pull-up capability. Floating the ERR pad will normally not be sufficient to exit the low power mode.

The CMD pad will be high when in the low power mode. If the low power mode was entered by a command, driving the CMD pad low will exit the low power mode. This can normally be accomplished by sending a few bytes to the CMD pad.

When the TRNG9880 exit the low power mode, it will perform a hardware reset, and then restart.

TRNG9880 COMMAND PAD: CMD

The CMD pad allows communication with the TRNG9880 using UART-style serial communication. The CMD pad communicates with 9.600 bit/s. The CMD pad may be of value during evaluation, testing, and debugging of the application. We plan for an interface circuit, to allow an easy computer USB connection to the CMD pin during repair, testing and evaluation. Please kindly contact TRNG98 about availability of this circuit.

The CMD pin can be used for:

- Hardware and software version and revision codes
- Clear text error messages, identifying the source of the error
- Access to the raw random number stream for test purposes
- Periodic status messages for unit supervision
- Easy software access to low power mode and hardware boot/reset
- Alternative random number output
- Interface for future upgrades of device
- Customer and application specific operating modes

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
CMD pad bit rate	9100	9600	10100	bit/s	Temperature dependent, varying

STATE	TRNG9880 Voltage	PC computer "serial port" UART voltage
CMD Idle	High: Vcc voltage	Low: -10 volts
CMD start bit	Low: 0 volts	High: +10 volts
CMD data "0"	Low: 0 volts	High: +10 volts
CMD data "1"	High: Vcc voltage	Low: -10 volts

The table above give the UART serial port voltages. A start bit is followed by 8 data bits and one stop bit. The LSB bit of the byte is transmitted first. The stop bit is "CMD idle". Note that the voltages correspond to an inverted PC computer serial port.

The CMD pad is generally used for entering commands to the TRNG9880 unit. As the CMD pad is double directional, the application may have to monitor the CMD pad to find an empty slot to enter the command.

The bit rate of the CMD pad depends on the temperature. To guarantee successful communication with the TRNG9880 the application may have to adapt to the TRNG9880 bit rate. Otherwise may the TRNG9880 misread the command bytes.

TRNG9880 'CMD' COMMAND LIST

The format of the commands is one digit (0-9) followed by optional uppercase letter (A-Z). "0" commands are for power and boot control, "1" commands are test commands, "3" commands are variants of normal operation. You unit may have additional customer-specific commands implemented.

COMMAND CODE	ERR PAD	FUNCTION
0	Go low	The TRNG9880 will enter a null command mode.
0L	High-Z	The TRNG9880 will enter the low power mode. Transmit a few 0x00 bytes to exit.
0X		The TRNG9880 will perform a soft reset, and then load the 3R command.
0B		The TRNG9880 will perform a hardware reset, and then load the 3R command.
1T	Go low	The TRNG9880 will transmit a 192 bytes sample of raw input noise and then go idle (RAW<>). The output format is binary data 0x00-0xFF.
1X	Go low	The TRNG9880 will transmit a 192 bytes sample of raw input noise and then go idle (RAWX<>). The output format is printable text hex data "00"- "FF".
3R	Low->High	The default TRNG9880 start command loaded after reset.
3T	Low->High	The 3R command with additional binary CMD pad output of TRNG9880 random numbers (RN<>). The output format is binary data 0x00-0xFF.
3X	Low->High	The 3R command with additional binary CMD pad output of TRNG9880 random numbers (RX<>). The output format is printable text hex data "00"- "FF".

In response to issued commands, results of internal tests, and error conditions the TRNG9880 output messages on the CMD pad:

STRING	INTERPRETATION	NOTES
CR-LF "TRNG9880A-1243" CR-LF	The TRNG9880 was booted. 3R command follows.	The "A" in "TRNG9880A" is the hardware revision code. The "12" is the year and the "43" the week of the software revision. Revision codes intended for device errata. Customer specific units may report unit ID as "TRNG9881"
"CMD_x." CR-LF "CMD_xx." CR-LF	CMD pad command received.	The code "x" ("xx") represent an one- or two bytes command code received by the TRNG9880. For the 0X, 0B commands the reset/reboot will be delayed until this string is printed.
"STAT_ERROR_xxxx" CR-LF	The TRNG9880 detect a statistical error. ERR->low	A statistical error was detected. The "xxxx" code correspond to a too low test value, printed as four hex characters (0-F).
"STAT_OK_xxxx" CR-LF	ERR->High	The previous error condition (statistical error) is lifted. The "xxxx" code correspond to a test value, printed as four hex characters (0-F).
"OKxxxx" CR-LF	Statistical test performed, result is OK.	The "xxxx" code correspond to a test value, printed as four hex characters (0-F). This message is to be expected regularly during normal operation (3R, 3T, 3X commands).
"OVERRUN" CR-LF	SPI-S overrun. ERR->low	The 8 bit SPI-S of the TRNG9880 was overrun. At least one zero bit was output, that is not a random bit.

"BUFFER_EMPTY" CR-LF	Buffer empty. ERR->low	The TRNG9880 buffer was empty. The CLK data rate was too high for too long time, causing the buffer to go low. This is not a hardware error.
"LOWPOWER MODE" CR-LF	TRNG9880 in low power mode	The TRNG9880 go to low power mode in response to the "0L" command, or the application is driving the ERR pad low during operation (3R, 3T, 3X commands).
"RAW<data>" CR-LF	Test data output, binary	The TRNG9880 output 192 bytes of raw noise bytes (unprocessed data). "data" is 192 bytes.
"RAWX<data>" CR-LF	Test data output, hex	The TRNG9880 output 192 bytes of raw noise bytes (unprocessed data). "data" is 384 bytes of "0"- "9" "A"- "F" characters.
"RN<data>" CR-LF	Random number output, binary.	The TRNG9880 output a string of true random bytes. Transmission of "data" will go on until another message is due for printing. As the "data" is binary the application may check for the ">" end mark only by parsing the output. The ">" will occur occasionally in the random output.
"RNX<data>" CR-LF	Random number output, hex.	The TRNG9880 output a string of true random bytes. Transmission of "data" will go on until another message is due for printing. Output is printable text hex characters. In hex format the ">" random value will be printed in hex, and can not be confused with the ">" end mark.

In the table description the text "CR-LF" refer to ASCII carriage return and line feed characters (0x0D,0x0A), and the quotes are not printed. The "0" and the "1" commands normally set the ERR pad low, to signal to the application that the TRNG9880 is performing a test command. 3R, 3T, 3X commands start up with the statistical error set (and ERR pad low). This is intentional, and not an TRNG9880 malfunction. When the statistical test go OK the message "STAT_OK_xxxx"CR-LF is printed, ERR pad go high, and the application may start using the TRNG9880.

The 3T, 3X commands will schedule printing of random data, as long as no other printing is in progress. This will block the CMD port for input. To stop the 3T, 3X commands the CMD pad may be held low until the RN<data> or RNX<data> string terminates. The TRNG9880 will then detect that the CMD pad is low, and temporarily abort the output. The application may then send a new command.

The application shall turn off the CLK clock in response to an error. In some cases the CMD pad will output errors until the error condition is cleared.

PRG_DATA TEST PAD

The PRG_DATA pad is reserved for future use, depending on the customers application. The pad is reserved for use by customers, not for use by TRNG98. The pad may be an input pad or an output pad or both.

RESET TEST PAD

The RESET pad connects between the TRNG9880 fail-safe reset circuit and the internal reset pad. The reset is a hard reset, and will reset the TRNG9880 as a power cycling would have done.

The fail-safe device is an analogue switch circuit that continuously send reset pulses to the TRNG9880 until the power is turned off or the TRNG9880 starts operating. The reset is an active high reset; and during normal operation the RESET pad is low.

The fail-safe reset circuit connects to the RESET pad by a 2k resistor. An external application (or operator) may reset the TRNG9880 at any time by pulling the RESET pad high to Vcc. An external application can also (for test purposes) hold the RESET low to GND. This will disable the fail-safe reset generator.

An external application may monitor the reset of the TRNG9880 by connecting to the RESET pad using a high-impedance connection (100kΩ (Min)) such as an oscilloscope probe.

When the TRNG9880 is in RESET all pads will be of "pull-down" type. In particular ERR will be low to indicate an error. Also note that if the TRNG9880 "locks" it may take 200 (Typ) ms before the ERR goes to pull-down due to a reset.

RESET PAD DC SPECIFICATION

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Probe input impedance	100			k Ω	To monitor the pad
Reset drive output impedance			0.1	k Ω	To take over reset control of the device
Fail-safe circuit operating voltage	0.8		6.0	V	

RESET PAD AC SPECIFICATION

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Reset pulse "high" from fail-safe circuit		200	350	ms	
Reset pulse "low" timeout by fail-safe circuit	100	200	400	ms	When HEARTBEAT stops
External reset pulse to reset	1		Infinite	μ s	The outcome of a shorter pulse is undefined
Holding RESET low			Infinite	ms	Disabling the fail-safe circuit

HEARTBEAT TEST PAD

The heartbeat signal is generated by an operating TRNG9880 device to inhibit the fail-safe reset circuit. This signal is enabled only during special well-controlled operating conditions. Should an unknown operating state be encountered, either because of a hardware event such as a power glitch or a disturbance by an ionising ray, or due to a software event such as issuing an undocumented software command or similar, the heartbeat signal will stop and a hard reset will follow. The output is analogue and intended for oscilloscope probes only.

DC SPECIFICATION

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Connected external probe resistance	500			k Ω	
Connected external probe capacitance			1000	pF	
Pad "high" level	$V_{cc}-0.3$	V_{cc}		V	
Pad "low" level		0	0.3	V	

AC specification

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Pulse frequency during normal operation	29	32	34	Hz	Accuracy further reduced in low power mode

ANALOG TEST PAD

The analogue test pad gives access to the internal analogue input noise source. The ANALOG test pad is buffered by a dedicated analogue driver to prevent external signals disturbing the analogue noise signal before sampling. The typical use of this pad is when investigating if an external electrical (or other) disturbance have influence on the internal analogue noise source of the TRNG9880.

ANALOG PAD DC SPECIFICATION

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
DC signal level		$V_{cc}/2$		V	
DC analogue->digital sample level		$V_{cc}/2$		V	May depend on module revision code
Output driver resistance		0.001		k Ω	
High output voltage swing	$V_{cc}/2+1.3$			V	50 Ω load to $V_{cc}/2$ (not recommended, test only)
Low output voltage swing			$V_{cc}/2-1.3$	V	50 Ω load to $V_{cc}/2$ (not recommended, test only)
External connected probe resistance	1.0	10		k Ω	To any DC voltage between GND and V_{cc}

ANALOG PAD AC SPECIFICATION

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Output signal amplitude		2.0		V	
Analogue amplification from noise source		100		dB	Noise source->ANALOG pad
Acceptable AC disturbance	200			μ s	Signal may be high/low occasionally during this time
Analogue bandwidth noise signal		100		kHz	
Analogue output buffer bandwidth		2.8		MHz	
Non-random ripple signal		7.35		kHz	Ripple frequency (non-random signal)
Non-random ripple signal			0.5	V	Ripple amplitude (non-random signal)

DIGITEST TEST PAD

The digital test pad gives access to the analogue noise signal after the signal has been sampled into digital form. This pad is of use when investigating the effect of external disturbances. The pad also enable access to the raw bit stream should this be needed or be of value for the application.

Internally is this bit stream read in 8 bit bytes. The bytes is then checked for non-random events which may render the bytes invalid or may trigger an error event (ERR=low). An accepted byte stream is encrypted, using a varying table-processing method, before the byte stream is made available to the application on the DO pad. One or several raw input bytes may be needed to produce a single output byte on the DO pad. Each output byte is normally a function of a minimum of 7 raw input bytes.

If the CLK pad is held idle, so no bytes are read from the DO pad, the input raw random number stream will continuously update the next available byte to be transmitted on the DO pad.

DIGITEST PAD DC SPECIFICATION

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Digital output low voltage			0.5	V	Sink 10 mA
Digital output high voltage	V _{cc} -1.1			V	Source 10 mA
Digital output low sink current			10	mA	May sink 25 mA at 0.75V if modest operating temperature
Digital output high source			10	mA	May source 10 mA max

DIGITEST PAD AC SPECIFICATION

PARAMETER	MIN	TYP	MAX	UNIT	NOTES/CONDITIONS
Output data rate	50	80	100	kbits/s	May depend on model and operating conditions
Sample->Output delay time		8		bits	Time=8*(sample bit time). The bit stream run through an 8-bit buffer.

PRG_CLK TEST PAD

Reserved, **DO NOT CONNECT**, at least no on production units. A disturbance on this pad may influence the analogue noise signal.

APPLICATION INFORMATION

INTERFACE

An application shall normally interface to the TRNG9880 module using the CLK, DO, and ERR pads. If the application cannot interface to the ERR pad it is possible to build an interface based upon the CLK and DO pads only. In that case may the application detect errors by running a test on the output random numbers. When the ERR pin is low the DO pad will output zeroes.

An application may also interface using the CMD pin. For some applications an interface using a single bidirectional pad may be preferable. For an application with an software interface this may be preferred despite interface problems such as fluctuations in the bit rate, and that the TRNG9880 output must be parsed.

In case that the application don't use the CMD pin we recommend that some connection to the CMD pin is arranged for test, debugging, or repair purposes.

DEBUGGING & TESTING

By sending commands to the TRNG9880, various error conditions can easily be simulated, that may not occur at all or with a very low frequency in an actual application. If the "0" command is given the TRNG9880 will set the ERR pad low, and hold it there, until the test operator give a new command. Sending a "0B" command, that hard-boot the TRNG9880, could be used as a simulation of an ESD or other environmental event. The various overrun conditions described above, can be simulated by attaching a square-wave generator to the CLK pin. Due to this it is recommended that the CMD pin is evaluated and decoded during development, and that, to a minimum, an external connection is available for testing and evaluation of your products interface.

EVALUATION MODULE

An TRNG9880 evaluation module "TRNG9880-EVM" is available. The module give access to the six TRNG9880 pads using a contact or a cable. A simple RC-style oscillator is provided as example CLK input. The ERR pad have an attached red LED for visual inspection. An opto-coupler, an amplifier, and a cable enable the evaluation module to be plugged into a PC using a standard 10V serial port. A supplied battery eliminator, that lack a DC connection to the mains ground, enable the use of the evaluation module as a communication amplifier between an application with a mounted TRNG9880 and a PC computer. Test software with source code is provided with the evaluation module, that enable printing of the CMD pad communication on screen.

APPLICATION SPECIFIC MODIFICATIONS

The command structure of the TRNG9880 is intended to provide a framework for application and customer specific additions and modifications. In case the intended application would benefit from some modification in the output, the module pin-out, or in the output format, please contact TRNG98. For a volume order we include reasonable software modifications free of charge.

TRNG9880 RANDOMNESS SOURCE

The TRNG9880 use Johnson noise as the physical noise source. The noise originates in a combination of resistor noise, in an external resistor, and in resistance in the input stage of the first amplifier. Johnson noise has a frequency distribution shaped according to the pass band of the amplifier; the noise is bandwidth-limited by the amplifier's bandwidth. Johnson noise is also well known to have very low amplitude. A very high gain disturbance free amplification is needed. The TRNG9880 use six stages of analogue amplification.

SOFTWARE ACCESS

To lower production costs a customer may contact TRNG98 for obtaining information about a **licence agreement**. Under a license contract the customer may mount the components inside the TRNG9880 unit directly on the customer's PCB. TRNG98 also have several other random number circuits, that may be cost effective in the customer's application as a function of the intended production volume. Some our on-line shop for examples of deliverables and pricing.

Complete software access to the TRNG9880 unit require a licence agreement or other agreement with TRNG98. Customers ordering 300+ units may request partial (algorithmic) software access in response to a signed NDA.

SOFTWARE & DOCUMENTATION UPDATES

The TRNG9880 datasheet revision history:

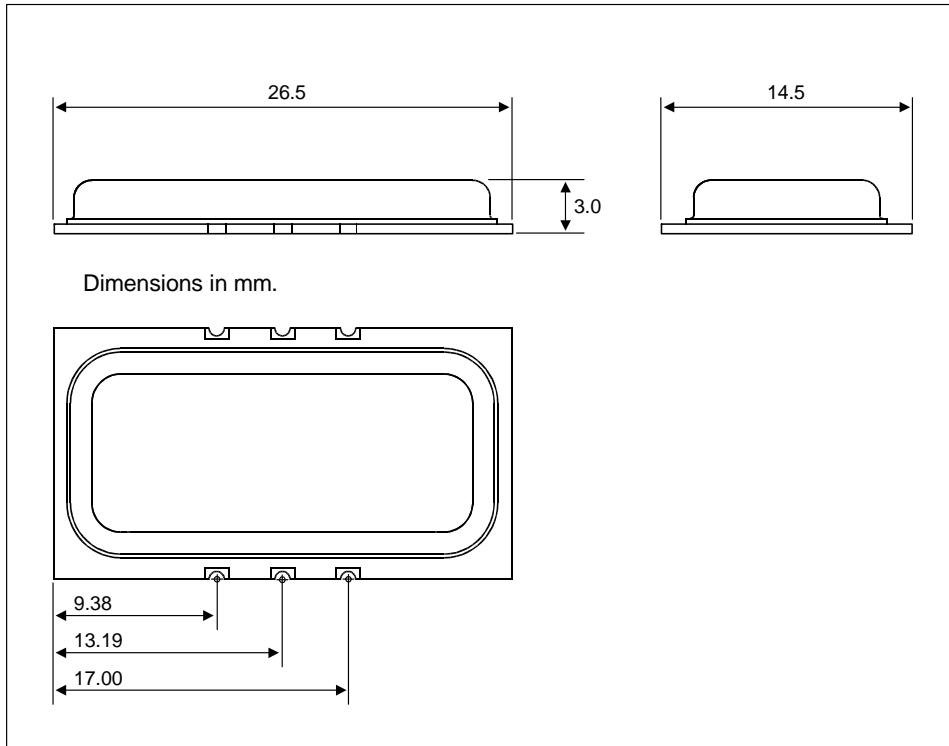
VERSION	NOTES
August 2009	First version
October 2012	Minor corrections of spelling and clarification of operating modes.

The TRNG9880 hardware revision history:

VERSION	NOTES
TRNG9880	

The TRNG9880 software revision history is included in the TRNG9880 evaluation module documentation.

PACKAGE OUTLINES



DOCUMENTATION ERROR: The above picture show the ESD protective can with round corners. The TRNG9880 have 90-segree square corners. This will be corrected in next documentation update. The module size and landing pattern is correct.

An example landing pattern in Gerber format is available on TRNG98's website.

LANDING PATTERN LAYOUT

An example landing pattern in Gerber format is available on TRNG98's webbsite.

DEFINITIONS

OBJECTIVE PRODUCT SPECIFICATION

This datasheet target specifications for product development

PRELIMINARY PRODUCT SPECIFICATION

This datasheet contains preliminary data; supplementary data may be published from TRNG98 later.

PRODUCT SPECIFICATION

This datasheet contains final product specifications. TRNG98 reserves the right to make changes at any time without notice in order to improve design and supply the best possible result.

ABSOLUTE MAXIMUM RATINGS

Stress above one or more of the limiting values may cause permanent and terminal damage to the device. These are stress ratings only and operation of the device at these or other conditions above those given in the "Absolute Maximum Ratings" section of the specification is not implied. Exposure to limiting values for extended periods may affect device reliability.

APPLICATION INFORMATION

When application information is given, it is advisory and does not form a part of the specification.

LIFE SUPPORT POLICY

A hardware random number generator is normally used in demanding situations where the failure or the correct operation of the device may be of critical importance for the success or failure of the application. Nevertheless, we wish to be informed if the device is used in a life support application or generally in a critical application. This information will be used to enforce that best practices are followed when the TRNG9880 is integrated into the application.

TRNG98's products are not authorised for use as critical components in life support devices or systems without the express written approval of the president and general counsel of TRNG98. 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 labelling, can reasonably be 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.*

PRICING AND AVAILABILITY

The TRNG9880 True Random Number Generator Module is currently not in production. Samples of equivalent size and function are available for immediate shipping. For information on product pricing and availability, contact TRNG98 at www.TRNG98.se or call Sweden +46 70 658 79 70, or send us an e-mail to info@trng98.se.

PACKAGING AND ORDER INFORMATION

This is to be included later, when exact information is available about carrier and packaging sizes.

TRNG98
Attn: Bo Dömstedt
Vittnesgränden 17
SE-226 47 LUND
Sweden
Ph +46 70 658 79 70
E-mail: TRNG98 <sales@trng98.se>
<http://www.TRNG98.se>
Skype: TRNG98
Company registration number: SE-6311306614
Our shop: <http://www.TRNG98.se/shop/index.php>
VAT: SE631130661401
Fax +46 46 211 42 04