RTS5912

(Part Number: RTS5912-GR)

32-bit Embedded Controller with Crypto Engine

DATASHEET

Rev. 0.13

27 April 2023

Realtek Semiconductor Corp.
No. 2, Innovation Road II, Hsinchu Science Park, Hsinchu 300, Taiwan Tel.: +886-3-578-0211. Fax: +886-3-577-6047
www.realtek.com

COPYRIGHT

DISCLAIMER

Realtek provides this document “as is”, without warranty of any kind, neither expressed nor implied, including, but not limited to, the particular purpose. Realtek may make improvements and/or changes in this document or in the product described in this document at any time. This document could include technical inaccuracies or typographical errors.

TRADEMARKS

Realtek is a trademark, of Realtek Semiconductor Corporation. Other names mentioned in this document are trademarks/registered trademarks of their respective owners.

USING THIS DOCUMENT

This document is intended for the hardware and software engineer’s general information on the Realtek RTS5912 EC IC.

Though every effort has been made to ensure that this document is current and accurate, more information may have become available

subsequent to the production of this guide. In that event, please contact your Realtek representative for additional information that may help in the development process.

System Features

■ CPU

- Real-M300 Arm v8-M Instruction Processor@ 100MHz
- FPU-Single precision
- MPU-Memory Protection Units

■ Inter Memory Unit

- 64KB of ROM
- 384KB(Code:352KB/Data:32KB) SRAM
- 512KB/1MB Flash
- 256B Battery SRAM
  - VBAT Power domain

System Host Interface – eSPI

- Based Enhanced Serial Peripheral Interface (eSPI) Interface Base Specification, Intel document #327432-005, Revision 1.5
- Enhanced Serial Peripheral Interface (eSPI) Compatibility Specification, Intel document #562633, REV. 0.7
- Supported Channels
  - Peripheral Channel
  - Virtual Wires Channel
  - Out-Of-Band (OOB) Channel
    - ✓ eRPMC(RPMC over eSPI OOB)
  - Run-time Flash Access channel
    - ✓ Master Attached Flash Sharing(MAFS)
    - ✓ Slave Attached Flash Sharing (SAFS)
    - ✓ RPMC
- eSPI Clock frequency of up to 66MHz
- Support in-band Alerts over eSPI IO1 or eSPI Alert# pin

System Host Interface – SPI

- Clock rate support up to 8MHz
- 128-byte Transmit and Receive FIFOs
- Supported basic SPI transactions
  - Read Data
  - Read Status
  - Write Data

System Host Interface – PECI

- Support Intel's low voltage PECI V3.1
- 32-byte Transmit and Receive FIFOs
- Supports adjustable VTT level

Security Engine

- Boot ROM Secure Boot Loader
  - Hardware Root of Trust (RoT) - NIST SP 800-193
  - Supports 2 Code Images in

external SPI Flash

- Multi purpose AES Crypto Engine:
  - Support for 128-bit - 256-bit key length
- Digital Signature Algorithm
  - Support for ECDSA and EC_KCDSA

- Cryptographic Hash Engine
  - Support SHA-256 and SHA-512
  - Support SHA3-256 and SHA3-512
- Public Key Crypto Engine
  - RSA keys length up to 4096 bits
  - ECC Prime/Binary Field keys of 571 bits
- OTP
  - 8K bits FIFO
- PUF(Physically Unclonable Function)
  - 1K bits OTP PUF
  - True Random Number Generator
- 8042 Emulated Keyboard Controller
  - 8042 Style Host Interface
- ACPI Embedded Controller Interfaces
  - Five PM interface ports (legacy 62h/66h; 68h/6Ch; 6Ah/6Eh; 6Bh/6Fh;7A/7E)
- Port 80 BIOS Debug Port
  - Two Ports(80/81), Assignable to Any eSPI IO Address
  - Two 16-Entry FIFO
  - 80Port bypass UART
- Host Mail Box
  - The Host Mail Box provides a standard run-time mechanism for the system host to communicate.

Peripheral Features

- GPIO
  - RTS5912– 128 pins
  - Input
    - All the GPIO pins have event detection capability to generate wake-up/interrupt event
    - Rising, falling and any edge wakeup
    - High Level and Low level condition
    - Configurable input drive disable
  - Output
    - Push Pull or Open Drain output
    - Pull up or pull down resistor control
  - GPIO BYPASS: 6 ports
- I2C(Master/Slave)

- 8 channels, Up to 1 MHz Capable
- Supports Master and Slave mode
- Supports polling or interrupt controlled operation
- Optional internal pull-up on SDA and SCL pins

■ I3C(Master/Slave)

- 2 channels, Support SDR Mode
- Based on I3C Master and Slave functionality per MIPI Alliance Specification for I3C, Version 1.1.1
- Operation volage: 1.8V/3.3V
- I3C Master
  - Automatic SDA buffer configuration as push-pull or open-drain with internal pull-up
- I3C Slave
  - Supports all Common Command Codes (CCCs)
  - Supports Timing Control Asynchronous Mode 0
  - Supports I2C-style static address

■ PWM

- 12 PWM Output Channels
- Multiple Clock Rates: 50MHz or 32.768KHz

■ Fan Tachometer

- 4 channels
- 16-bit Resolution

■ Breathing LED Interface

- 2 LED Output Channels
- Programmable Clock source
- Supported blinking and breathing mode

■ UART

- Both support master mode and slave mode
- Support command and Data transceiver
- 16-byte FIFO for transmit and receive

■ Keyboard Matrix Scan

- 20x10 keyboard matrix scan
- System Wake capability on KSI interrupt

■ Timer32

- Support 6 channel Timer32 controller
- Clock Source: 25MHz
- 32-bit Auto-reloading Timer
- Support one-shot and continuous mode
- Programmable as down counter

■ Slow Timer

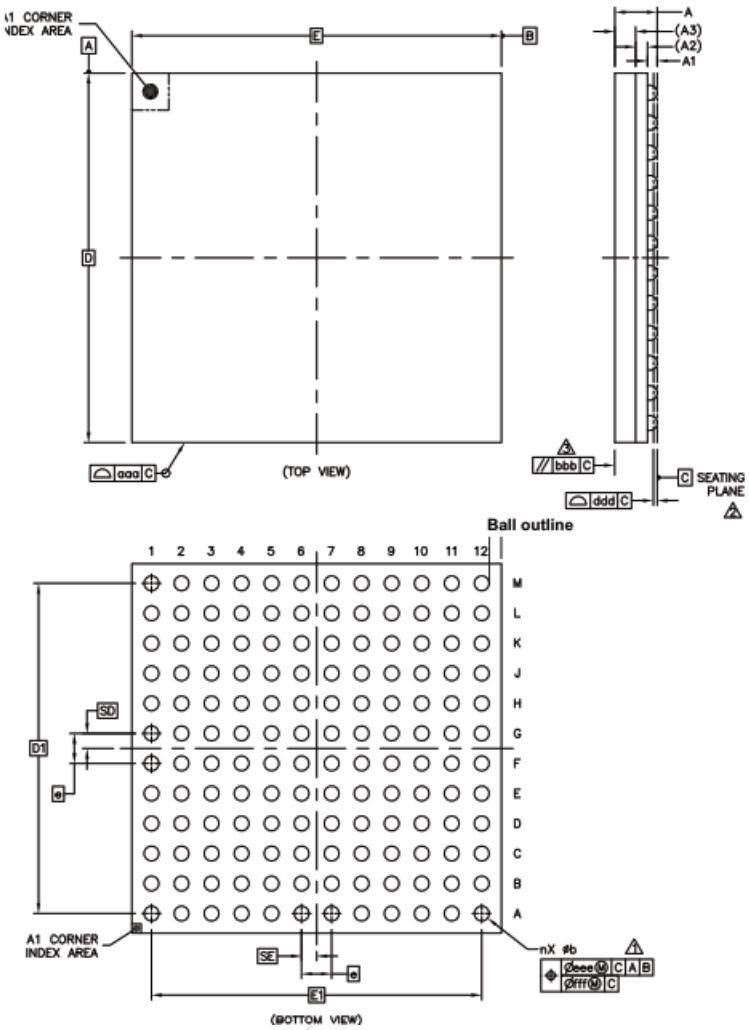
- Support 2 channel Slow Timer controller

- Support 1MHz base timer
- Programmable us level delay
- One-shot or Periodical Modes

- RTOS Timer
  - Runs off 32KHz Clock Source
  - 32bit Timer
  - Support one-shot and periodical mode
- Low power RTC
  - VBAT Powered
  - Time-of-Day and Calendar Registers
  - Programmable Alarms
  - Support Leap Year and Daylight savings time
  - System Wake capability on interrupts
- Watch Dog Timer (WDT)
  - VBAT Powered
  - Programmable pre-scale counter
  - Programmable 8bit count
  - Programmable 16-bit pre-scaler register
- SPI Controller
  - Master SPI Controller-Flash
    - Support Single/Dual/Quad mode
    - Support MCM Flash and External Flash
  - Master SPI Controller-Peripheral
    - 128-byte Receive FIFOs
    - 128-byte Transmit FIFOs
    - Support Single/Dual mode
- PS2 Controller
  - 1 channel(5 volt tolerant)
- Debug Path
  - Serial Wire Debug (SWD) interface
  - JTAG interface
  - ETM/ITM interface
- Operating Conditions
  - Operating Voltages: 3.3V and 1.8V
  - Operating Temperature Range: 0°C to 70°C

1. Package Mechanical Dimensions

1.1. BGA144 Dimension



	Symbol	Common Dimensions (mm)		
		Min	Nor	Max
Total thickness	A	---	---	0.95
Stand off	A1	0.16	0.21	0.26
Substrate thickness	A2	0.17	0.21	0.25
Mold thickness	A3		0.45 REF	
Body size	D	7.9	8	8.1
	E	7.9	8	8.1
Ball diameter			0.3	
Ball opening (UBM size)			0.275	
Ball width	b	0.25	0.3	0.35
Ball pitch	e		0.65 BSC	
Ball count	n		144	
Ball outline			0.265	
Edge ball center to center	D1		7.15 BSC	
	E1		7.15 BSC	
Body center to contact ball	SD		0.325 BSC	
	SE		0.325 BSC	
Package edge tolerance	aaa		0.15	
Mold flatness	bbb		0.1	
Coplanarity	ddd		0.1	
Ball Offset (package)	eee		0.15	
Ball Offset (ball)	fff		0.08	

NOTES:

1. DIMENSION b IS MEASURED AT THE MAXIMUM SOLDER BALL DIAMETER, PARALLEL TO DATUM PLANE C.
2. DATUM C (SEATING PLANE) IS DEFINED BY THE SPHERICAL CROWNS OF THE SOLDER BALLS.
3. PARALLELISM MEASUREMENT SHALL EXCLUDE ANY EFFECT OF MARK ON TOP SURFACE OF PACKAGE.

2. Ordering Information

Part Number	Package	Status
RTS5912-GR	BGA144 8x8mm^2 'Green' Package	MP

Realtek Semiconductor Corp.

Head Quarters

No. 2, Innovation Road II

Hsinchu Science Park, Hsinchu 300, Taiwan

Tel.: +886-3-578-0211. Fax: +886-3-577-6047

www.realtek.com