

# **MEC1322**

# Keyboard and Embedded Controller for Notebook PC

### **Product Features**

- ARM<sup>®</sup> Cortex<sup>®</sup>-M4 Processor Core
  - 32-Bit ARM v7-M Instruction Set Architecture
  - Hardware Floating Point Unit (FPU)
  - Single 4GByte Addressing Space (Von Neumann Model)
  - Little-Endian Byte Ordering
  - Bit-Banding Feature Included
  - NVIC Nested Vectored Interrupt Controller
  - Up to 240 Individually-Vectored Interrupt Sources Supported
  - 8 Levels of Priority, Individually Assignable By Vector
  - Chip-Level Interrupt Aggregator supported, to expand number of interrupt sources or reduce number of vectors
  - System Tick Timer
  - Complete ARM-Standard Debug Support
    - JTAG-Based DAP Port, Comprised of SWJ-DP and AHB-AP Debugger Access Functions
    - Full DWT Hardware Functionality: 4 Data Watchpoints and Execution Monitoring
    - Full FPB Hardware Breakpoint Functionality: 6 Execution Breakpoints and 2 Literal (Data) Breakpoints
  - Comprehensive ARM-Standard Trace Support
    - Full DWT Hardware Trace Functionality for Watchpoint and Performance Monitoring
    - Full ITM Hardware Trace Functionality for Instrumented Firmware Support and Profiling
    - Full ETM Hardware Trace Functionality for Instruction Trace
    - Full TPIU Functionality for Trace Output Communication
- 128K SRAM (Code or Data)
  - 96K Optimized for Code
  - 32K Optimized for Data
- LPC Interface
  - Supports LPC Bus frequencies of 19MHz to 33MHz
  - LPC I/O Cycles Decoded
  - LPC Memory Cycles Decoded
  - Clock Run Support
  - Serial IRQ
  - ACPI SCI interface
  - SMI# output
- Two SPI Memory Interfaces
  - 3-pin Full Duplex serial communication interface
  - Two Private and Two Shared Chip Selects
  - DMA Support

- 8042 Style Host Interface
  - Mailbox Registers Interface
    - Forty-three 8-Bit scratch registers
  - Two Register Mailbox Command Interface
  - Two Register SMI Source Interface
- Two ACPI Embedded Controller Interface
  - 1 or 4 Byte Data transfer capable
- ACPI Power Management Interface
   SCI Event-Generating Functions
- Embedded Memory Interface
  - Host Serial IRQ Source
  - Provides Two Windows to On-Chip SRAM for Host Access
- Two Register Mailbox Command Interface
- Battery Backed (VCC0/VBAT) Resources
  - Power Fail Register
  - Power-Fail Status Register
  - Battery backed 64 byte memory
- Real Time Clock (RTC)
  - VCC0 (VBAT) Powered
  - 32KHz Crystal Oscillator
  - 32KHz Clock output available under VCC1 power
  - Time-of-Day and Calendar Registers
  - Programmable Alarms
  - Supports Leap Year and Daylight Savings Time
- Hibernation Timers
- General Purpose Analog to Digital Converter
   10-bit conversion precision
  - 10-bit conversion per channel is completed in less than 12us
  - 5 ADC channels
    - 10-bit Conversion with 2.9mV resolution
    - 0 to 3.3 VDC Conversion Range
  - Optional continuous sampling at a programmable rate
  - Internal Analog Voltage Reference (3.0V +/-1%)
- Watch Dog Timer
- Four Programmable 16-bit and Two 32-bit Timers
   Wake-capable Auto-reloading Timers
- Four Independent Hardware Driven PS/2 Ports
   Fully functional on Main and/or Suspend Power
  - PS/2 Edge Wake Capable
- Four Programmable Pulse-Width Modulator Outputs
  - Independent Clock Rates
  - 16-Bit Duty Cycle Granularity
  - Operational in both Full on and Standby modes

- Four EC-based SMBus 2.0 Host Controllers
  - Allows Master or Dual Slave Operation
  - Controllers are Fully Operational on Standby Power
  - DMA-driven I<sup>2</sup>C Network Layer Hardware
  - I<sup>2</sup>C Datalink Compatibility Mode
  - Multi-Master Capable
  - Supports Clock Stretching
  - Programmable Bus Speeds
    - 400 KHz Fast-mode Capable
    - 1 Mbps Fast-mode Plus Capable
  - Hardware Bus Access "Fairness" Interface
  - SMBus Time-outs Interface
  - 5 Ports
  - 2 Port Flexible Multiplexing
- PECI 3.0 Interface
- Keyboard Matrix Scan Interface
  - 18 x 8 Interrupt/Wake Capable Multiplexed Keyboard Scan Matrix
    - Row Predrive Option
- Four Breathing/Blinking LED Interfaces
  - Programmable Blink Rates
  - Piecewise Linear Breathing LED Output Controller
  - Operational in EC Sleep States
- Dual Fan Tachometer Inputs
- RPM-Based Fan Speed Control Algorithm
  - Utilizes one TACH input and one PWM output
  - 3% accurate from 500 RPM to 16k RPM
  - Automatic Tachometer feedback
  - Aging Fan or Invalid Drive Detection
  - Spin Up Routine
  - Ramp Rate Control
  - RPM-based Fan Speed Control Algorithm
- Fast GATEA20 & Fast CPU\_RESET
- RSMRST# Functionality Supporting System Deep
   Sleep
  - Compatible with south bridge SUSCLK/ RSMRST# gating rules
  - Replacement 32K distribution available when RSMRST# is asserted
- Integrated Power-on Reset Generator
  - VCC1\_RST# open drain output
  - Accepts External driven Reset
- Anti-Glitch Protection on Power-on
- All Blocks Support Low Power Sleep Modes
- General Purpose Input/Output Pins
- Low Power
- High Configurability
- Two pin Debug Port with standard 16C550A register interface
  - Accessible from both Host and EC
- BC-Link Interconnection Bus
- One High Speed Bus Master Controller
- Package Options
  - 128-pin VTQFP
  - 132-pin DQFN
  - 144-pin WFBGA

### Description

The MEC1322 incorporates a high-performance 32-bit ARM<sup>®</sup> Cortex<sup>®</sup>-M4 embedded microcontroller with 128 Kilobytes of SRAM and 32 Kilobytes of Boot ROM. It communicates with the system host using the Intel<sup>®</sup> Low Pin Count (LPC) bus.

The MEC1322 has two SPI memory interfaces that allow the EC to read its code from external SPI flash memory: private SPI and/or shared SPI. The Shared SPI interface allows for EC code to be stored in a shared SPI chip along with the system BIOS. The private SPI memory interface provides for a dedicated SPI flash that is only accessible by the EC.

The MEC1322 provides support for loading EC code from the private or shared SPI flash device on a VCC1 power-on. Before executing the EC code loaded from a SPI Flash Device, the MEC1322 validates the EC code using a digital signature encoded according to PKCS #1. The signature uses RSA-2048 encryption and SHA-256 hashing. This provides automated detection of invalid EC code that may be a result of malicious or accidental corruption. It occurs before each boot of the host processor, thereby ensuring a HW based root of trust not easily thwarted via physical replacement attack.

The MEC1322 is directly powered by two separate suspend supply planes (VBAT and VCC1) and senses the runtime power plane (VCC) to provide "Instant On" and system power management functions. It also contains an integrated VCC1 Reset Interface and a system Power Management Interface that supports low-power states and can drive state changes as a result of hardware wake events.

# TO OUR VALUED CUSTOMERS

It is our intention to provide our valued customers with the best documentation possible to ensure successful use of your Microchip products. To this end, we will continue to improve our publications to better suit your needs. Our publications will be refined and enhanced as new volumes and updates are introduced.

If you have any questions or comments regarding this publication, please contact the Marketing Communications Department via E-mail at docerrors@microchip.com. We welcome your feedback.

#### Most Current Data Sheet

To obtain the most up-to-date version of this data sheet, please register at our Worldwide Web site at:

#### http://www.microchip.com

You can determine the version of a data sheet by examining its literature number found on the bottom outside corner of any page. The last character of the literature number is the version number, (e.g., DS30000000A is version A of document DS30000000).

#### Errata

An errata sheet, describing minor operational differences from the data sheet and recommended workarounds, may exist for current devices. As device/documentation issues become known to us, we will publish an errata sheet. The errata will specify the revision of silicon and revision of document to which it applies.

To determine if an errata sheet exists for a particular device, please check with one of the following:

- Microchip's Worldwide Web site; http://www.microchip.com
- Your local Microchip sales office (see last page)

When contacting a sales office, please specify which device, revision of silicon and data sheet (include -literature number) you are using.

#### **Customer Notification System**

Register on our web site at www.microchip.com to receive the most current information on all of our products.

# **BLOCK DIAGRAM**



# PACKAGE OUTLINE

םבעופוטאו חופידססע	REV         DESCRIPTION         DATE         RELEASED           C         DESCRIPTION OF CHANGES - IN FRONT PAGE         122804         SKLLEV           D         ADDED PART MARKING ORIENTATION         9192014         SKLLEV	COMMON DIMENSIONS	NOM MAX NOTE REMARK	- 1.20 - OVERALL PACKAGE HEIGHT	- 0.15 - STANDOFF - 1.05 - BODY THICKNESS	– 16.20 – "X"/"Y" SPAN	14.00 14.20 3 "X"/"Y" BODY SIZE	0.60 0.75 4 LEAD FOOT LENGTH	1.00 REF – LEAD LENGTH	0.18 0.23 2 LEAD WIDTH	– 0.20 LEAD FOOT THICKNESS	0.40 BSC – LEAD PITCH	LEAD SHOULDER RADIUS	- 0.20 LEAD FOOT RADIUS	- 0.08 - COPLANARITY	RE IN MILLIMETER. NUD "EF" DO NOT TICLUEE MOLE ND 3± 0.035mm MAXIMUM. NUD "Ef" DO NOT INCLUEE MOLE PROTRUSIONS. MAXIMUM ALLOWED 26 mm PER SIDE. BEAURED AT THE GAUGE PLANE. 0.25mm ABOVE THE SEATING PLANE. DEATINER ARE OPTIONAL BUT MUST BE LOCATED WITHIN THE ZONE		wwe bate PACKAGE OUTLINE	Reaver S.K.ILIEV 128 VTQFP-14x14x1.0mm BODY, 0.4mm PITCH	Outcode         Devolvaments         Rev           S.K.ULEV         12/17/04         MO-128-VTQFP-14x14x1-0         D           APPROVED         saute         stroometrum         setter
	25 - 0°-7°		r win	'	0.05	15.80	1 13.80	0.45		0.13	0.09		0.08	0.08	ı	B DIMENSIONS / E POSITION SF ENSIONS "D1", ENSION ST ENSION "L" IS 1 ALS ON PIN 1 CATED.	8 OTHERWISE SPECIFIE ONS ARE IN MILLIMETER ONS ARE IN MILLIMETER TOLERANCES ARE: ANGUL ANGUL	1 025 PRET DM AND TOL PER SME Y14 5M 1994	N/A	N/A T WITH SCALE TO FIT
			SYMBO	۲	A2	D/E	D1/E	-	5	م	υ	Ð	Ł	R2	2 C C C	NOTE: 1. ALL C 2. TRUE 3. DIME PRO 5. DETA INDIO	UNLES: DIMENSI AND CECIMAL XX ±0	X_XXX ±0 INTERU AS	MATERIAL	PRINT
						TOP VIEW			SEE DETAIL "A"			SEATING PLANE			SIDE VIEW				3-D VIEW	

## FIGURE 1: 128-PIN VTQFP PACKAGE OUTLINE

### FIGURE 2: 132-PIN DQFN PACKAGE OUTLINE (1 OF 2)



### FIGURE 3: 132-PIN DQFN PACKAGE OUTLINE (2 OF 2)



## FIGURE 4: 144-PIN PACKAGE OUTLINE



# APPENDIX A: PRODUCT BRIEF REVISION HISTORY

#### TABLE A-1: REVISION HISTORY

Revision	Section/Figure/Entry	Correction
DS00001733B (06-19-15)	Document Features, Prod- uct Identification System page, Package Outlines	144-pin WFBGA package added
DS00001733A (05-05-14)	Document Release	

# THE MICROCHIP WEB SITE

Microchip provides online support via our WWW site at www.microchip.com. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- General Technical Support Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- Business of Microchip Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

# CUSTOMER CHANGE NOTIFICATION SERVICE

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at www.microchip.com. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

# **CUSTOMER SUPPORT**

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or field application engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

#### Technical support is available through the web site at: http://www.microchip.com/support

## **PRODUCT IDENTIFICATION SYSTEM**

To order or obtain information, e.g., on pricing or delivery, refer to the factory or the listed sales office.

PART NO. <sup>(1)</sup> Device	- <u>XXX<sup>(2)</sup> - XX</u> - <u>[X]<sup>(3)</sup></u> Package ROM Tape and Reel Version Option	Examples:           a)         MEC1322-NU-C0 = 128-pin VTQFP           b)         MEC1322-LZY-C0 = 132-pin DQFN           c)         MEC1322-SZ = 144-pin WFBGA
Device:	MEC1322 <sup>(1)</sup>	
Package:	NU = 128 pin VTQFP <sup>(2)</sup> LZY = 132 pin DQFN <sup>(2)</sup> SZ = 144 pin WFBGA <sup>(2)</sup>	Note 1:         These products meet the halogen maximum concentration values per IEC61249-2-21.           Note 2:         All package options are RoHS compliant. For RoHS compliance and environmental information, please visit <a href="http://www.micro-chip.com/pagehandler/en-us/aboutus/ehs.html">http://www.micro-chip.com/pagehandler/en-us/aboutus/ehs.html</a> .
Tape and Reel Option:	Blank = Tray packaging TR = Tape and Reel <sup>(3)</sup>	<b>Note 3:</b> Tape and Reel identifier only appears in the catalog part number description. This identifier is used for ordering purposes and is not printed on the device package. Check with your Microchip Sales Office for package availability with the Tape and Reel option.

#### Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights unless otherwise stated.

#### Trademarks

The Microchip name and logo, the Microchip logo, dsPIC, FlashFlex, flexPWR, JukeBlox, KEELOQ, KEELOQ logo, Kleer, LANCheck, MediaLB, MOST, MOST logo, MPLAB, OptoLyzer, PIC, PICSTART, PIC<sup>32</sup> logo, RightTouch, SpyNIC, SST, SST Logo, SuperFlash and UNI/O are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

The Embedded Control Solutions Company and mTouch are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Analog-for-the-Digital Age, BodyCom, chipKIT, chipKIT logo, CodeGuard, dsPICDEM, dsPICDEM.net, ECAN, In-Circuit Serial Programming, ICSP, Inter-Chip Connectivity, KleerNet, KleerNet logo, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICkit, PICtail, RightTouch logo, REAL ICE, SQI, Serial Quad I/O, Total Endurance, TSHARC, USBCheck, VariSense, ViewSpan, WiperLock, Wireless DNA, and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

Silicon Storage Technology is a registered trademark of Microchip Technology Inc. in other countries.

GestIC is a registered trademarks of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

All other trademarks mentioned herein are property of their respective companies.

© 2014 - 2015, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

ISBN: 9781632775078

# QUALITY MANAGEMENT SYSTEM CERTIFIED BY DNV = ISO/TS 16949=

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELoQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and mulfacture of development systems is ISO 9001:2000 certified.



# **Worldwide Sales and Service**

#### AMERICAS

Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: http://www.microchip.com/ support

Web Address: www.microchip.com

Atlanta Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455

Austin, TX Tel: 512-257-3370

Boston Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088

**Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075

**Cleveland** Independence, OH Tel: 216-447-0464 Fax: 216-447-0643

**Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924

**Detroit** Novi, MI Tel: 248-848-4000

Houston, TX Tel: 281-894-5983

Indianapolis Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453

Los Angeles Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608

New York, NY Tel: 631-435-6000

San Jose, CA Tel: 408-735-9110

**Canada - Toronto** Tel: 905-673-0699 Fax: 905-673-6509

#### ASIA/PACIFIC

Asia Pacific Office Suites 3707-14, 37th Floor Tower 6, The Gateway Harbour City, Kowloon Hong Kong Tel: 852-2943-5100 Fax: 852-2401-3431 Australia - Sydney

Tel: 61-2-9868-6733 Fax: 61-2-9868-6755

**China - Beijing** Tel: 86-10-8569-7000 Fax: 86-10-8528-2104

**China - Chengdu** Tel: 86-28-8665-5511 Fax: 86-28-8665-7889

**China - Chongqing** Tel: 86-23-8980-9588 Fax: 86-23-8980-9500

China - Dongguan Tel: 86-769-8702-9880

**China - Hangzhou** Tel: 86-571-8792-8115 Fax: 86-571-8792-8116

**China - Hong Kong SAR** Tel: 852-2943-5100 Fax: 852-2401-3431

**China - Nanjing** Tel: 86-25-8473-2460 Fax: 86-25-8473-2470

**China - Qingdao** Tel: 86-532-8502-7355 Fax: 86-532-8502-7205

**China - Shanghai** Tel: 86-21-5407-5533 Fax: 86-21-5407-5066

China - Shenyang Tel: 86-24-2334-2829 Fax: 86-24-2334-2393

**China - Shenzhen** Tel: 86-755-8864-2200 Fax: 86-755-8203-1760

**China - Wuhan** Tel: 86-27-5980-5300 Fax: 86-27-5980-5118

**China - Xian** Tel: 86-29-8833-7252 Fax: 86-29-8833-7256

#### ASIA/PACIFIC

**China - Xiamen** Tel: 86-592-2388138 Fax: 86-592-2388130

**China - Zhuhai** Tel: 86-756-3210040 Fax: 86-756-3210049

India - Bangalore Tel: 91-80-3090-4444 Fax: 91-80-3090-4123

**India - New Delhi** Tel: 91-11-4160-8631 Fax: 91-11-4160-8632

India - Pune Tel: 91-20-3019-1500

Japan - Osaka Tel: 81-6-6152-7160 Fax: 81-6-6152-9310

**Japan - Tokyo** Tel: 81-3-6880- 3770 Fax: 81-3-6880-3771

Korea - Daegu Tel: 82-53-744-4301 Fax: 82-53-744-4302

Korea - Seoul Tel: 82-2-554-7200 Fax: 82-2-558-5932 or 82-2-558-5934

Malaysia - Kuala Lumpur Tel: 60-3-6201-9857 Fax: 60-3-6201-9859

Malaysia - Penang Tel: 60-4-227-8870 Fax: 60-4-227-4068

Philippines - Manila Tel: 63-2-634-9065 Fax: 63-2-634-9069

**Singapore** Tel: 65-6334-8870 Fax: 65-6334-8850

**Taiwan - Hsin Chu** Tel: 886-3-5778-366 Fax: 886-3-5770-955

**Taiwan - Kaohsiung** Tel: 886-7-213-7828

**Taiwan - Taipei** Tel: 886-2-2508-8600 Fax: 886-2-2508-0102

**Thailand - Bangkok** Tel: 66-2-694-1351 Fax: 66-2-694-1350

#### EUROPE

Austria - Wels Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 Denmark - Copenhagen Tel: 45-4450-2828 Fax: 45-4485-2829

France - Paris Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79

Germany - Dusseldorf Tel: 49-2129-3766400

**Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44

**Germany - Pforzheim** Tel: 49-7231-424750

**Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781

Italy - Venice Tel: 39-049-7625286

Netherlands - Drunen Tel: 31-416-690399 Fax: 31-416-690340

Poland - Warsaw Tel: 48-22-3325737

**Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91

Sweden - Stockholm Tel: 46-8-5090-4654

**UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820