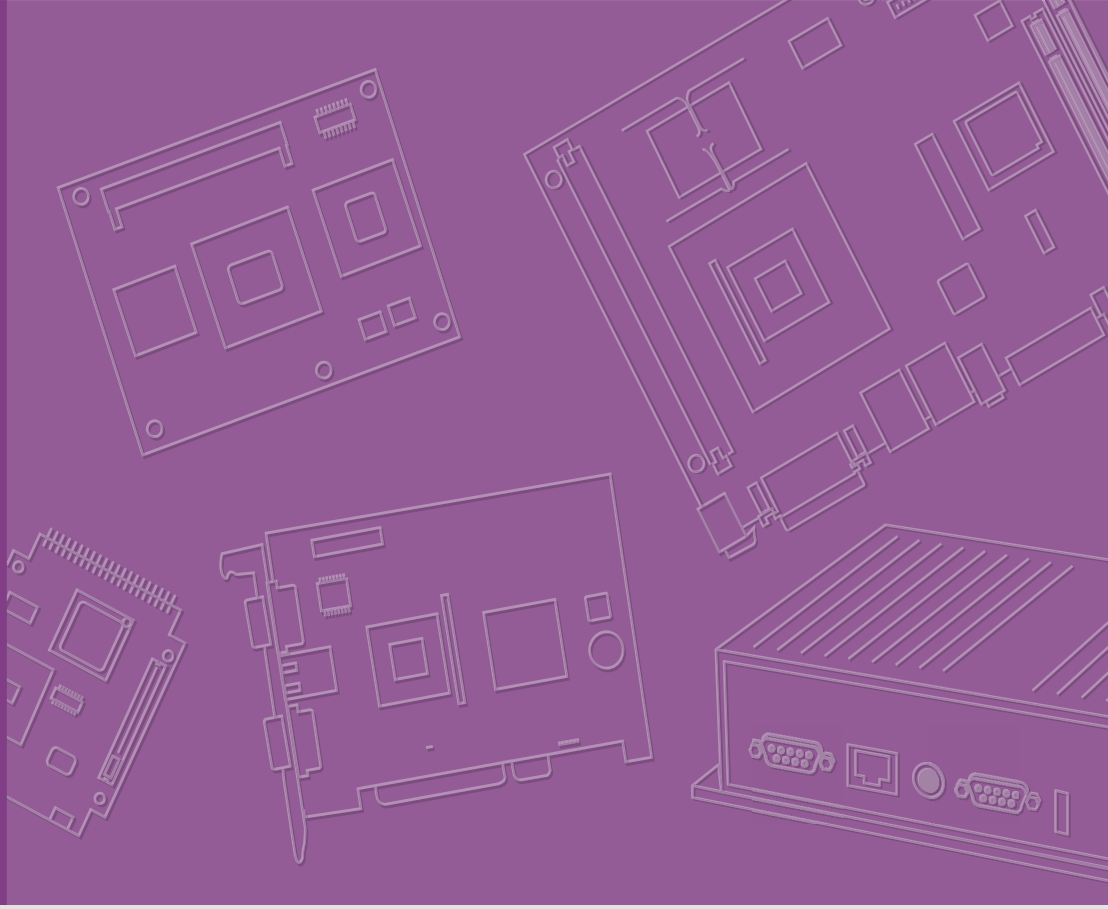
Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!

Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832
Email & Skype: info@chipsmall.com Web: www.chipsmall.com
Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China



User Manual

SOM-5897

COM Express Basic Module

ADVANTECH

Enabling an Intelligent Planet

Copyright

The documentation and the software included with this product are copyrighted 2018 by Advantech Co., Ltd. All rights are reserved. Advantech Co., Ltd. reserves the right to make improvements in the products described in this manual at any time without notice. No part of this manual may be reproduced, copied, translated or transmitted in any form or by any means without the prior written permission of Advantech Co., Ltd. Information provided in this manual is intended to be accurate and reliable. However, Advantech Co., Ltd. assumes no responsibility for its use, nor for any infringements of the rights of third parties, which may result from its use.

Acknowledgements

Intel is a trademark of Intel Corporation.

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.

All other product names or trademarks are properties of their respective owners.

Product Warranty (2 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for two years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For out-of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any onscreen messages you get when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. If your product is diagnosed as defective, obtain an RMA (return merchandize authorization) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Part No. 2006589701 Edition 2

Printed in Taiwan February 2018

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class B

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FM

This equipment has passed the FM certification. According to the National Fire Protection Association, work sites are classified into different classes, divisions and groups, based on hazard considerations. This equipment is compliant with the specifications of Class I, Division 2, Groups A, B, C and D indoor hazards.

Technical Support and Assistance

1. Visit the Advantech website at http://support.advantech.com where you can find the latest information about the product.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
   - Product name and serial number
   - Description of your peripheral attachments
   - Description of your software (operating system, version, application software, etc.)
   - A complete description of the problem
   - The exact wording of any error messages

Warnings, Cautions and Notes

Warning! *Warnings indicate conditions, which if not observed, can cause personal injury!*

Caution! *Cautions are included to help you avoid damaging hardware or losing data. e.g.*

There is a danger of a new battery exploding if it is incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Note! *Notes provide optional additional information.*

Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to: support@advantech.com

Packing List

Before setting up the system, check that the items listed below are included and in good condition. If any item does not accord with the table, please contact your dealer immediately.

- SOM-5897 CPU module
- 1 x Heatspreader (1960073944N001)

Safety Instructions

1. Read these safety instructions carefully.
2. Keep this User Manual for later reference.
3. Disconnect this equipment from any AC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
4. For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
5. Keep this equipment away from humidity.
6. Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
7. The openings on the enclosure are for air convection. Protect the equipment from overheating. DO NOT COVER THE OPENINGS.
8. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
9. Position the power cord so that people cannot step on it. Do not place anything over the power cord.
10. All cautions and warnings on the equipment should be noted.
11. If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.
12. Never pour any liquid into an opening. This may cause fire or electrical shock.
13. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
14. If one of the following situations arises, get the equipment checked by service personnel:
    - The power cord or plug is damaged.
    - Liquid has penetrated into the equipment.
    - The equipment has been exposed to moisture.
    - The equipment does not work well, or you cannot get it to work according to the user's manual.
    - The equipment has been dropped and damaged.
    - The equipment has obvious signs of breakage.
15. DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO BELOW -20° C (-4° F) OR ABOVE 60° C (140° F). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.
16. CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER, DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

The sound pressure level at the operator's position according to IEC 704-1:1982 is no more than 70 dB (A).

DISCLAIMER: This set of instructions is given according to IEC 704-1. Advantech disclaims all responsibility for the accuracy of any statements contained herein.

Safety Precaution - Static Electricity

Follow these simple precautions to protect yourself from harm and the products from damage.

- To avoid electrical shock, always disconnect the power from your PC chassis before you work on it. Don't touch any components on the CPU card or other cards while the PC is on.
- Disconnect power before making any configuration changes. The sudden rush of power as you connect a jumper or install a card may damage sensitive electronic components.

Contents

Chapter 1 General Information 1

1.1 Introduction 2
1.2 Specifications 2
1.2.1 Board Information 2
1.2.2 System Information 2
1.2.3 Display 3
1.2.4 Expansion Interface 3
1.2.5 I/O 4
1.2.6 iManager 2.0 4
1.2.7 Mechanical and Environmental Specification 4
1.3 Functional Block Diagram 5

Chapter 2 Mechanical Information 7

2.1 Board Information 8
Figure 2.1 Board Chips Identify - Front 8
Figure 2.2 Board Chips Identify - Back 8
2.2 Mechanical Drawing 9
Figure 2.3 Board Mechanical Drawing - Front 9
Figure 2.4 Board Mechanical Drawing - Back 9
2.3 Assembly Drawing 10
Figure 2.5 Assembly Drawing (Reference Only) 10

Chapter 3 BIOS Operation 11

3.1 Starting 12
3.1.1 Main Setup 13
3.1.2 Advanced BIOS Features Setup 14
3.1.3 Chipset 37
3.1.4 Security 48
3.1.5 Boot Settings 49
3.1.6 Save & Exit 50

Chapter 4 S/W Introduction & Installation 51

4.1 S/W Introduction 52
4.2 Driver Installation 52
4.2.1 Windows Driver Setup 52
4.2.2 Other OS 52
4.3 Advantech iManager 53

Appendix A Pin Assignment 55

A.1 SOM-5897 Type 6 Pin Assignment 56

Appendix B Watchdog Timer 61

B.1 Programming the Watchdog Timer 62

Appendix C Programming GPIO 63

C.1 GPIO Register 64

Appendix D System Assignments 65

D.1 System I/O Ports 66
Table D.1: System I/O ports 66
D.2 DMA Channel Assignments 67
Table D.2: DMA Channel Assignments 67
D.3 Interrupt Assignments 67
Table D.3: Interrupt Assignments 67
D.4 1st MB Memory Map 68
Table D.4: 1st MB Memory Map 68

Chapter 1

General Information

This chapter gives background information on the SOM-5897 CPU Computer on Module.

Sections include:

- Introduction
- Specification
- Functional Block Diagram

1.1 Introduction

SOM-5897 is equipped with the Intel® 6th Generation Core™/ Celeron/ Xeon product family, which are manufactured on 14nm process technology. SOM-5897 ECC/ non-ECC memory supports DDR4 2133MT/s with 1.2V power design, and up to 32GB of dual channel. SOM-5897 not only supports higher memory bandwidth, but also has 33% better battery life than previous generations. SOM-5897 is able to support 8 x PCIex1 as well as x4, x8 configurations if requested. Most important of all, SOM-5897 adopts a 28mm low profile cooler with a TDP of 45watt at 60°C ambient temperature (optional accessory). SOM-5897 is suitable for rich I/O applications with high performance requirements, such as ultra sound, military, broadcasting, and industrial automation fields.

Compared with previous generations there is 30% improvement in processor performance and up to 50% better 3D graphics. It supports Qual/ Dual core CPU with GT4e/ GT2, DX12, OpenGL 4.4, and OpenCL 2.0 functions. In addition, multiple displays are supported such as dual or triple displays. HDMI/DisplayPort with 4K2K resolution and dual channel LVDS and 16 simultaneous channels at 1920 x1080 full HD resolution are also available.

Advantech iManager was designed to satisfy a lot of embedded application requirements for monitoring and management of voltage and temperatures, thermal protection through processor throttling, LCD backlight on/off and brightness control and more. Combined with Advantech SUSI Access, it can remotely monitor and control devices through the internet for easy maintenance and configuration. All Advantech COM Express modules integrate iManager and SUSI Access.

SOM-5897 is suitable for computing intensive designs, thermally sensitive applications, graphics/media sensitive designs, and I/O demanding applications.

1.2 Specifications

1.2.1 Board Information

- **Pin Definition:** PICMG COM.0 R2.1 Type 6 pin-out definition.
- **Form Factor:** PICMG COM.0 R2.1 basic module 125 x 95 mm.

1.2.2 System Information

- **CPU:** 6th Gen Intel® Core Processors.

CPU	Standard Freq.	Max. Turbo Freq.	Core	Cache (MB)	TDP(W)
i7-6820EQ	2.8GHz	3.5GHz	4	8	45
I7-6822EQ	2.0GHz	2.8GHz	4	8	25
i5-6440EQ	2.7GHz	3.4GHz	4	6	45
i5-6442EQ	1.9GHz	2.7GHz	4	6	25
i3-6100E	2.7GHz	NA	2	3	35
i3-6102E	1.9GHz	NA	2	3	25
G3900E	2.4GHz	NA	2	2	35
E3-1505M V5	2.8GHz	3.7GHz	4	8	45
E3-1505L V5	2.0GHz	2.8GHz	4	8	25
E3-1515M V5	2.8GHz	3.7GHz	4	8	45

- **Memory:** 2 SODIMM socket for DDR4 2133, up to 32GB.
- **BIOS:** AMI UEFI.

- **Power management:** Supports power saving modes including Normal / Standby / Suspend modes. ACPI 2.0 compliant.

1.2.3 Display

- Graphic Core: Intel® Gen9 HD/P530/P580 graphics supports DX12, OGL4.4, OCL2.0, and MPEG2, HEVC/H265, VC1/WMV9 HW decode/encode/transcode acceleration.

CPU	Graphics Core	Base Freq.	Max Freq.
i7-6820EQ	Gen9 HD Graphic	350MHz	1000MHz
I7-6822EQ	Gen9 HD Graphic	350MHz	1000MHz
i5-6440EQ	Gen9 HD Graphic	350MHz	1000MHz
i5-6442EQ	Gen9 HD Graphic	350MHz	1000MHz
i3-6100E	Gen9 HD Graphic	350MHz	950MHz
i3-6102E	Gen9 HD Graphic	350MHz	950MHz
G3900E	Gen9 HD Graphic	350MHz	950MHz
E3-1505M V5	HD Graphic P530	350MHz	1050MHz
E3-1505L V5	HD Graphic P530	350MHz	1000MHz
E3-1515M V5	HD Graphic P580	350MHz	1000MHz

- **VGA:** Resolution up to 1920 x 1200.
- **LVDS:** Supports single/dual channel 18/24-bit, resolution up to 1920 x 1200 @ 60 Hz.
-
- **HDMI/DVI/DP:** Supports 3 ports HDMI (default), DVI, or DP multiplexed.
  Resolution: HDMI up to 4096 x 2160 @24Hz
  DVI up to 1920 x 1080 @ 60 Hz
  DP up to 4096 x 2304@60Hz 24bpp
- **Dual Display:**
  - VGA + LVDS,
  - VGA + HDMI/DVI/DP,
  - LVDS + HDMI/DVI/DP,
  - HDMI/DVI/DP + HDMI/DVI/DP
- **Triple Display:**
  - LVDS + DP + DP/HDMI,
  - LVDS + DP + VGA,
  - LVDS + HDMI + HDMI,
  - DP + DP + DP,
  - DP + HDMI +HDMI,
  - DVI + DP + HDMI,
  - VGA + DP + HDMI

1.2.4 Expansion Interface

- **PCI Express x1:** Supports default 8 PCIe x1 compliant ports to PCIe Gen3 (8.0 GT/s) specification; optionally configurable to PCIe x4 or PCIe x2. Several configurable combinations may need BIOS modification. Please contact Advantech sales or FAE for more details.
- **Audio Interface:** Intel HD Audio interface

- **LPC Bus:** Supports Low Pin Count (LPC) 1.1 specification, without DMA or bus mastering. Allows connection to Super I/O, embedded controller, or TPM. LPC clock is 25MHz.
- **SMBus:** Supports SMBus 2.0 specification with alert pin.
- **I2C Bus:** Up to 400KHz.
- **SPI:** Supports SPI BIOS only.

1.2.5 I/O

- **Ethernet:** Intel I219LM Gigabit LAN supports 10/100/1000 Mbps Speed
- **SATA:** Supports 4 ports SATA Gen3 (600 Gb/s)
- **USB Interface:** Supports 4 ports USB3.0, 8 ports USB 2.0
- **Serial Port:** Supports 2 ports 2-wire serial port
- **Express Card:** 2 ports
- **Panel Control:** Supports panel backlight on/off control, brightness control
- **Thermal Protection:** Supports thermal shutdown or CPU throttling
- **Watchdog Timer:** 65536 level timer interval, from 0~65535 sec, multi-level, multi-option watchdog timer
- **Smart Fan:** 1 port on module, 1 port down to carrier board
- **GPIO:** 8-bit GPIO
- **Hardware Monitor:** Vin, 5VSB, CMOS
- **TPM:** BOM option, default not available

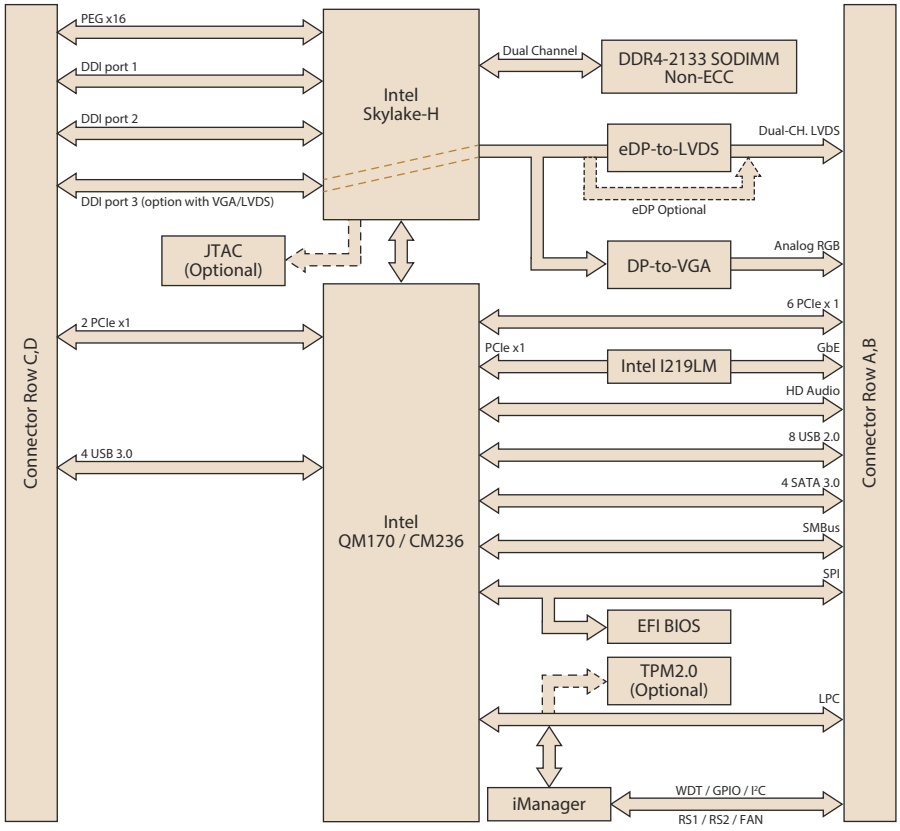
1.2.6 iManager 2.0

Refer to section 4.3.

1.2.7 Mechanical and Environmental Specification

- **Dimensions:** 125 x 95 mm (4.92" x 3.74")
- **Power Type and Supply Voltage:**
  - ATX: +8.5~20V and +4.75~5.25VSB (standby power)
  - AT: +8.5~20V
  - CMOS Battery: +3.3V
- **Power Requirements:**
  - Test condition: SOM-5897C3-U3A1E (i3-6100U), DDR3L-1600 16GB, WIN8.1 64-bit, under 12V and 5VSB input power supply.
  - Idle: 8.5W
  - Max: 41.8W (Burn-in V6.0 Pro)
- **Temperature Specification:**
  - Operating: 0 ~ 60° C (32 ~ 140° F)
  - Storage: -40 ~ 85° C (-40 ~ 185° F)
- **Humidity Specification:**
  - Operating: 40° C @ 95% relative humidity, non-condensing
  - Storage: 60° C @ 95% relative humidity, non-condensing

1.3 Functional Block Diagram



Chapter 2

Mechanical Information

This chapter gives mechanical information on the SOM-5897 CPU Computer on Module.

Sections include:

- Board Information
- Mechanical Drawing
- Assembly Drawing

2.1 Board Information

The figures below indicate the main chips on SOM-5897 Computer-on-Module. Please be aware of these positions while designing your own carrier board to avoid mechanical issues, as well as designing thermal solution contact points for best thermal dissipation performance.

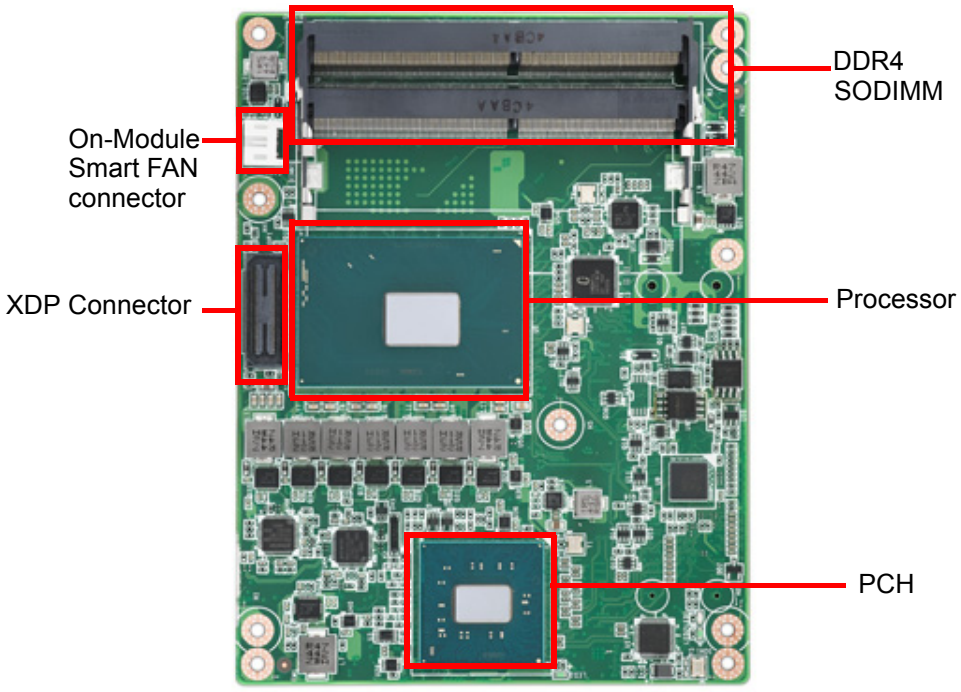


Figure 2.1 Board Chips Identify - Front

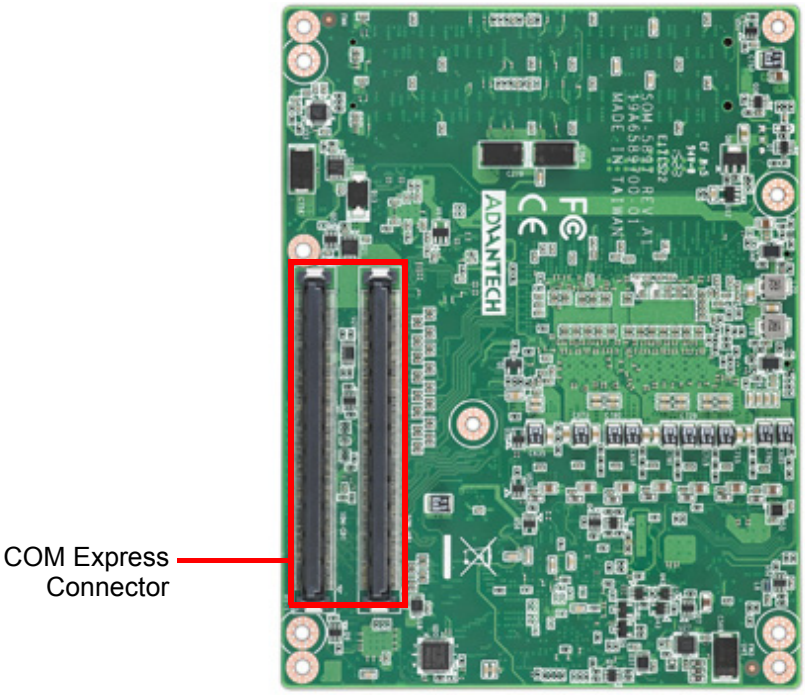


Figure 2.2 Board Chips Identify - Back

2.2 Mechanical Drawing

For more details about 2D/3D models, please look on the Advantech COM support service website http://com.advantech.com.

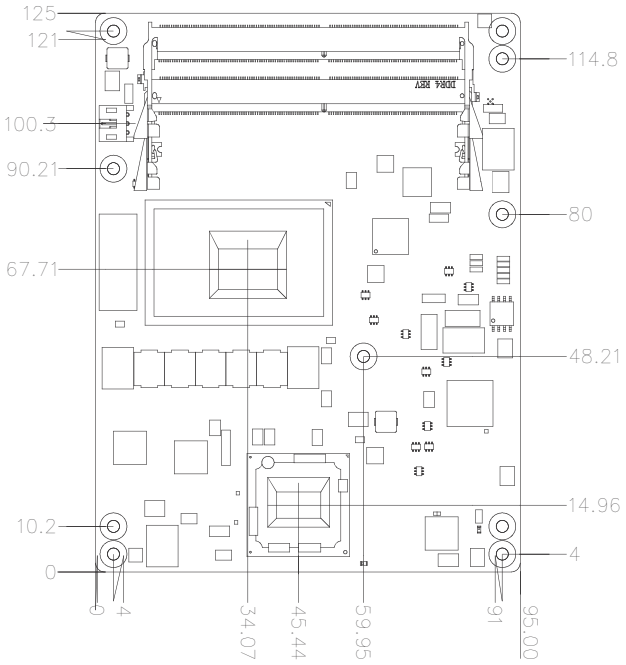


Figure 2.3 Board Mechanical Drawing - Front

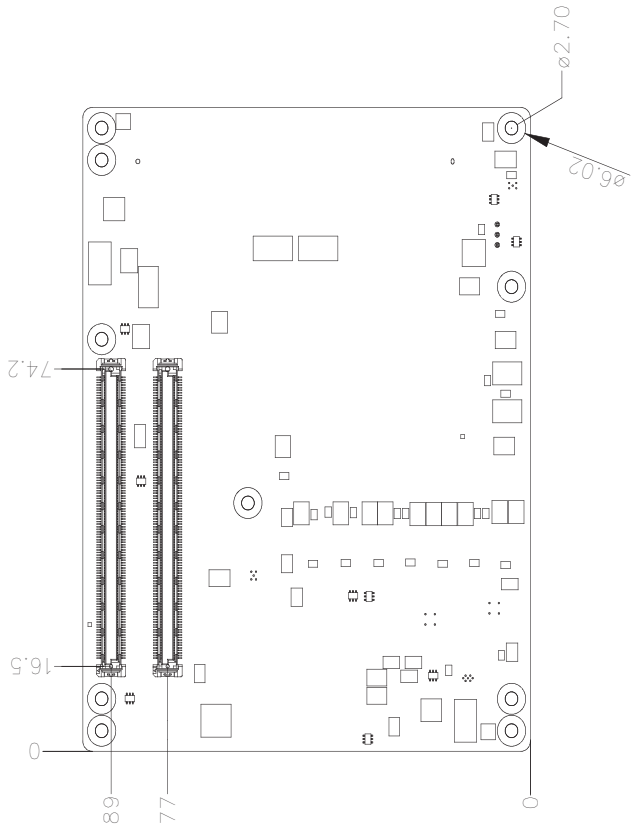


Figure 2.4 Board Mechanical Drawing - Back

2.3 Assembly Drawing

Assembly order for the thermal module and COM module onto the carrier board.

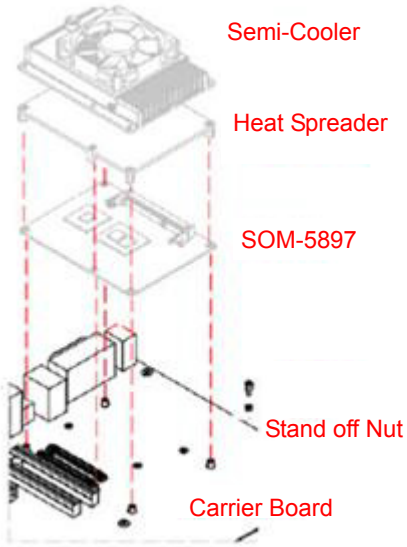


Figure 2.5 Assembly Drawing (Reference Only)

There are 3 reserved screw holes for SOM-5897 to be pre-assembled with the heat spreader.

Chapter 3

BIOS Operation

This chapter gives BIOS setup information for the SOM-5897 CPU Computer on Module.

Sections include:

- Introduction
- Entering Setup
- Hot / Operation Key
- Exit BIOS Setup Utility

3.1 Starting

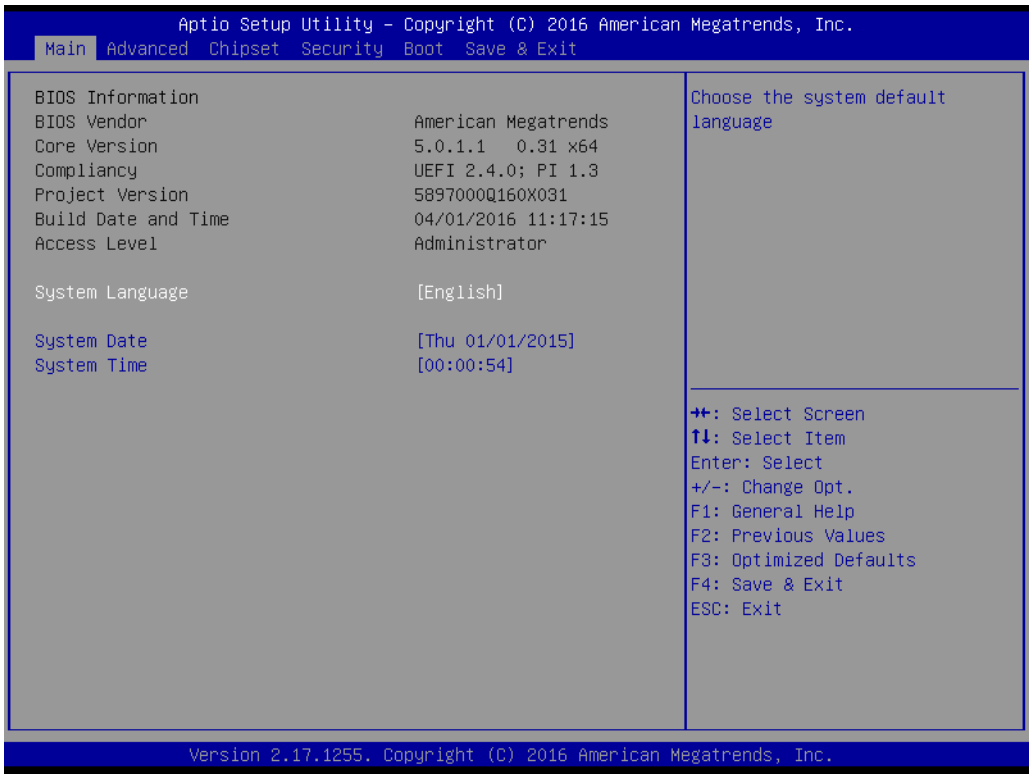
SOM-5897 BIOS has been stored into a flash ROM which is inserted into a BIOS socket on the board. With the BIOS Setup program, users can modify BIOS settings and control various system features. This chapter describes the basic navigation of the **SOM-5897** BIOS setup screens.

Advantech will have revisions for product optimization so customers can re-flash the latest BIOS through the AFU utility. Please contact Advantech sales or FAE for more details.

Entering the BIOS

To enter the BIOS setup screens, follow the steps below:

1. Power on the motherboard.
2. Press the **Delete** or **Esc** key on your keyboard when you see the following text prompt: Press **Delete** or **Esc** to enter setup.
3. After you press the **Delete** key, the main BIOS setup menu displays. You can access the other BIOS function settings.



The BIOS setup screen has three main frames. The left frame displays all information and configurable items. Grayed-out text is information only. Blue items are options that can be configured. White one is the current focus item to be selected.

The right-upper frame is an area reserved for a text message. When an option is selected from the left frame, a help text message will show at this area.

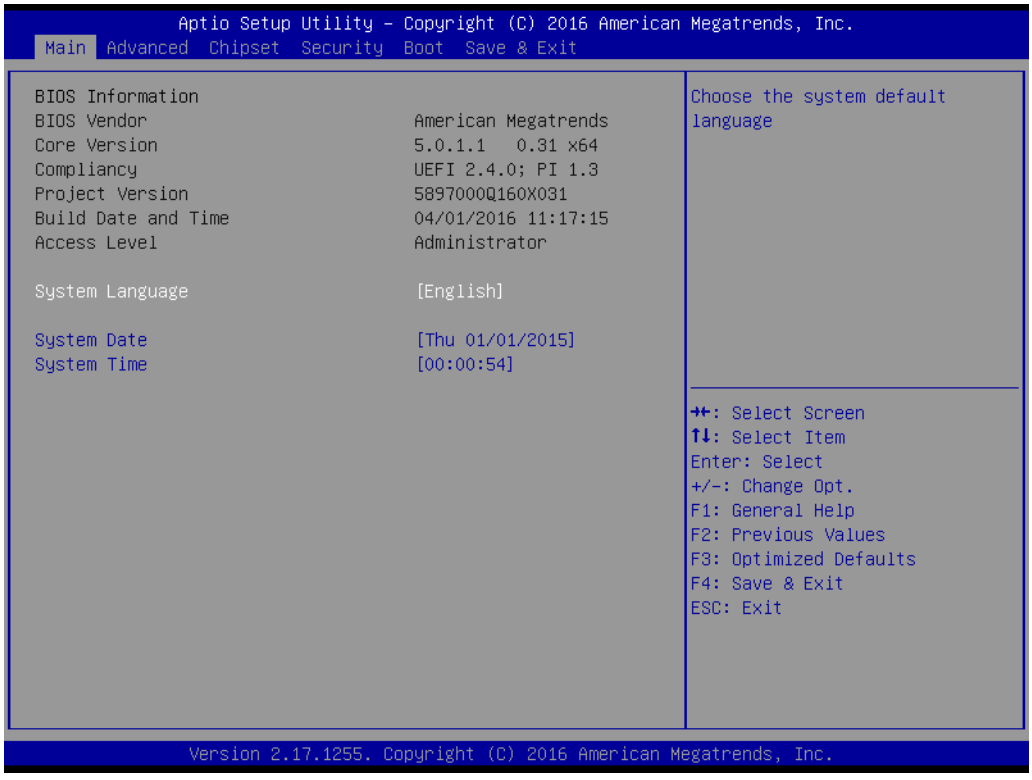
The following table shows the hot keys operation guide.

Hot Key	Description
→ Right ← Left	The Left and Right < > keys allow you to select a BIOS setup page. For example: Main page, Advanced page, Chipset page, and so on.
↑ Up ↓ Down	The Up and Down < > keys allow you to select a BIOS setup item or sub-screen.
+ - Plus/Minus	The Plus and Minus keys allow you to change the field value of a particular setup item. For example: Date and Time.
F1	The <F1> key allows you to display the General Help screen. Press the <F1> key to open the General Help screen.
F2	Load Previous Values. Ignore modified configures.
F3	Load Optimized Defaults.
F4	Save configuration and exit.
ESC	The <Esc> key allows you to go back to upper menu item. At root page, <Esc> key is used for Quit without saving.
Enter	Entering submenu or display option items.

SOM-5897 BIOS has a built-in Setup program that allows users to modify the basic system configuration. This information is stored in flash ROM so it retains the Setup information when the power is turned off.

3.1.1 Main Setup

When users first enter the BIOS Setup Utility, they will enter the **Main** setup screen. You can always return to the Main setup screen by selecting the **Main** tab. The Main BIOS Setup screen is shown below.

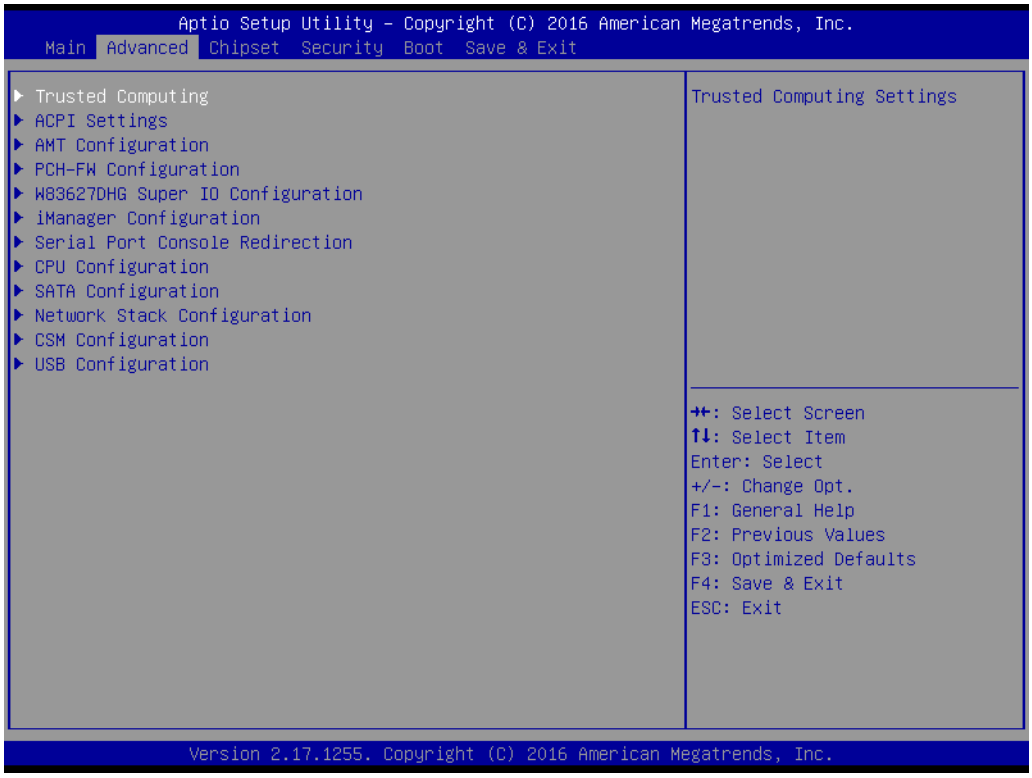


The Main page shows BIOS Information

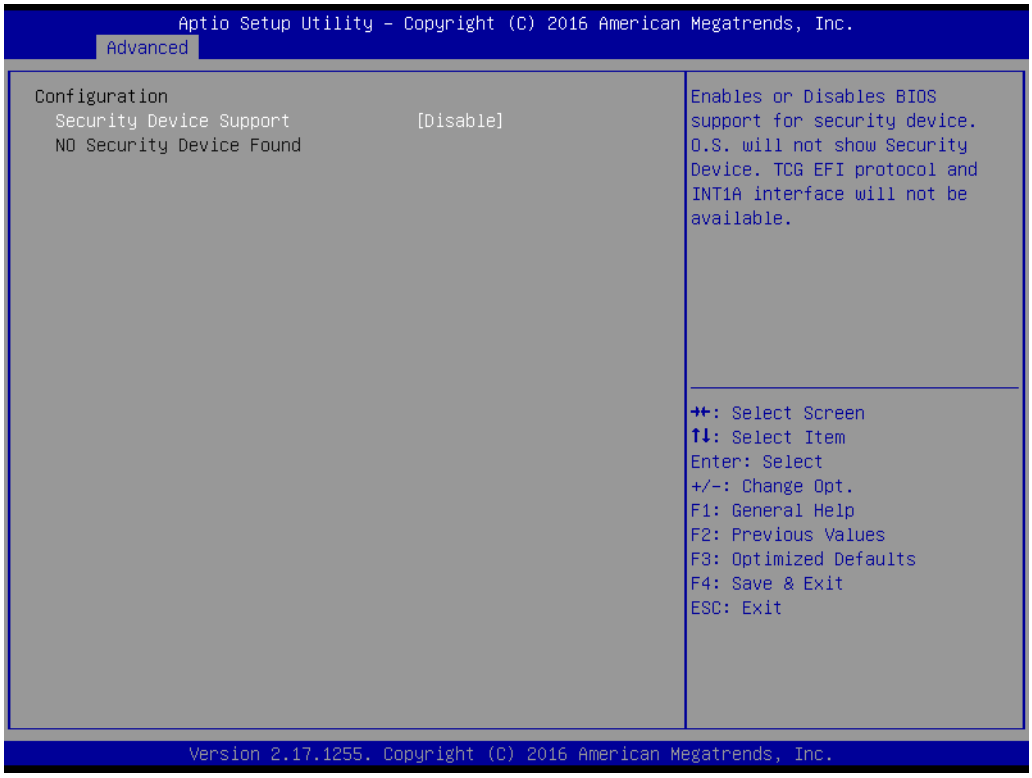
Feature	Options	Description
BIOS Information	No option	Subtitle
BIOS Vender	No option	Displays the BIOS vendor, where we suppliers license from.
Core Version	No option	Displays the BIOS vendor's kernel core version.
Compliancy	No option	Displays this BIOS supporting industry standards compliance.
Project Version	No option	Displays the project version of Advantech projects.
Build Date and Time	No option	Displays this BIOS build date and time.
Access Level	No option	Please refers to session "3.1.4 Security".
System Language	English	Choose the BIOS language
System Date	mm/dd/yyyy	Set the system date. Use Tab to switch between Date elements. Use + / - or numbers to change the value.
System Time	hh:mm:ss	Set the system time. Use Tab to switch between Date elements. Use + / - or numbers to change the value.

3.1.2 Advanced BIOS Features Setup

Select the Advanced tab from the **SOM-5897** setup screen to enter the Advanced BIOS Setup screen. Users can select any item in the left frame of the screen, such as CPU Configuration, to go to the sub menu for that item. Users can display an Advanced BIOS Setup option by highlighting it using the <Arrow> keys. All Advanced BIOS Setup options are described in this section. The Advanced BIOS Setup screens are shown below. The sub menus are described on the following pages.



3.1.2.1 Trusted Computing



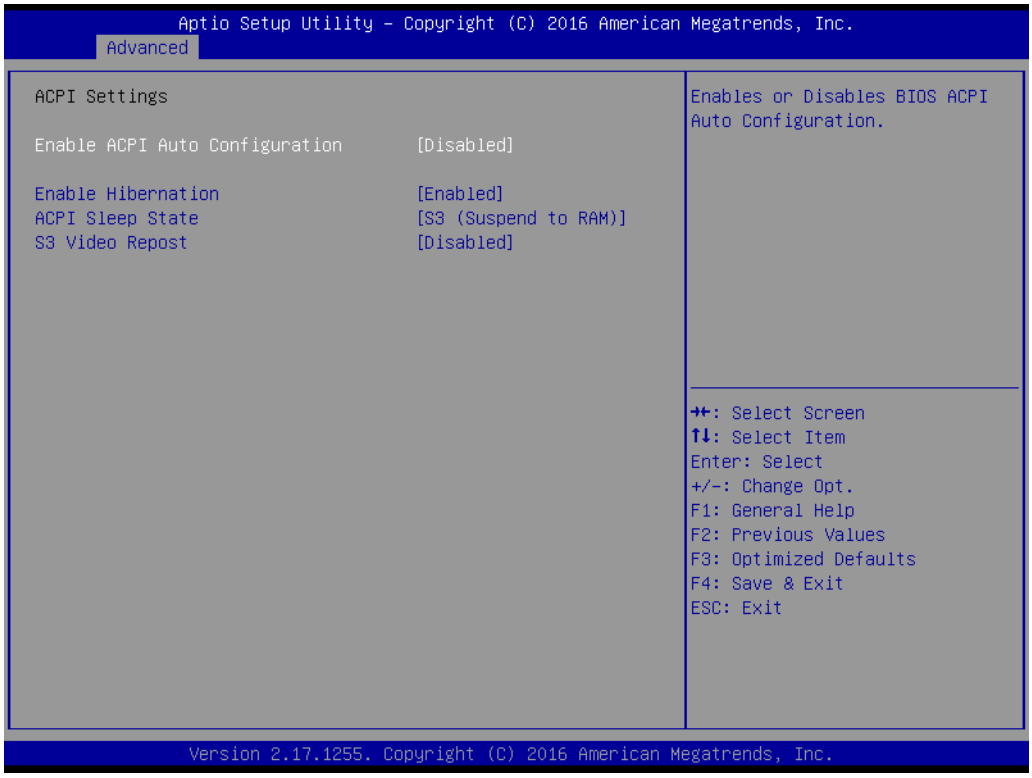
Trusted Computing is a technology developed and promoted by the Trusted Computing Group. With Trusted Computing, the computer will consistently behave in expected ways, and those behaviors will be enforced by computer hardware and software. Enforcing this behavior is achieved by loading the hardware with a unique encryption key inaccessible to the rest of the system.

Security Device Support

This sub-menu will allow you to enable/disable TPMTrusted Platform Module (TPM) support, and to configure the TPM state. Select Trusted Computing and press **Enter** to access the sub-menu. Press **Enter** to access the TPM support menu and select **Enable** to display the full TPM configuration menu.

Feature	Options	Description
Security Device Support	Disable Enable	Enables or disables the BIOS support for TPM (Trusted Platform Module) function.
TPM State	Disable Enable	Enable or Disable security device. Note: Your computer will reboot during restart in order to change State of the Device.
Pending Operation	None TPM Clear	Schedule an operation for the security device. Note: Your computer will reboot during restart in order to change the state of the device.
Device Select	TPM1.2 TPM2.0 Auto	TPM 1.2 will restrict support to TPM 1.2 devices. TPM 2.0 will restrict support to TPM2.0. Auto will support both with the default set to TPM2.0 devices if not found, TPM 1.2 devices will be enumerated.

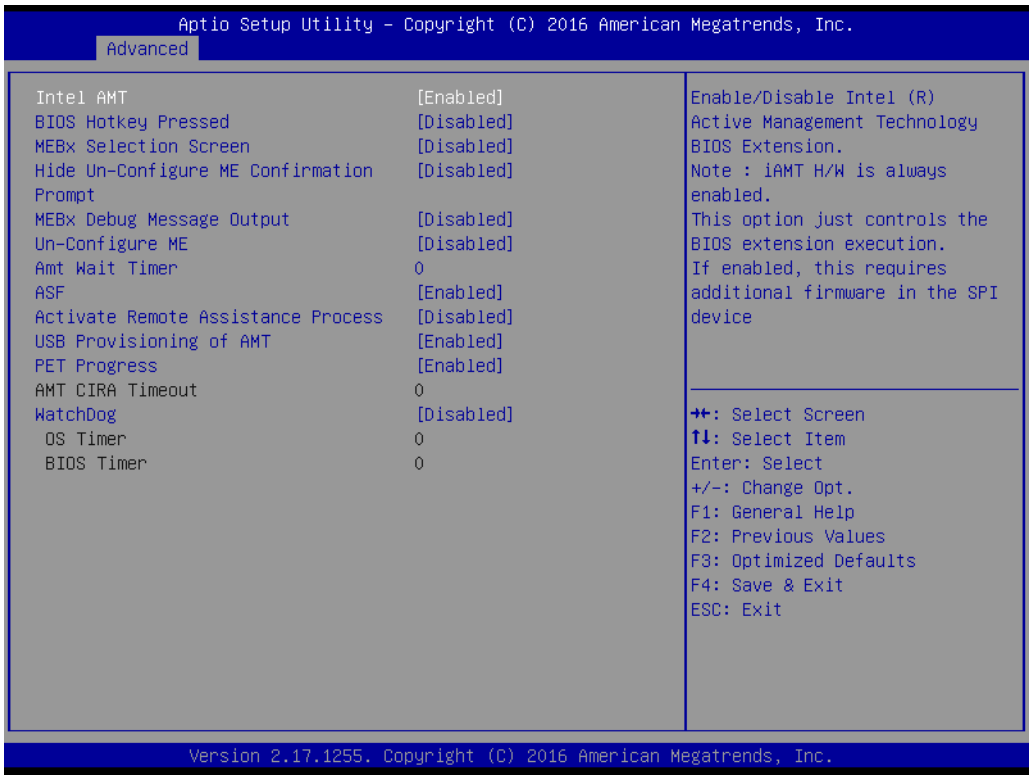
3.1.2.2 ACPI Settings



Feature	Options	Description
Enable ACPI Auto Configuration	Disable Enable	Enables or disables BIOS ACPI auto configuration. If this feature is enabled as auto, no more options can be configured.
Enable Hibernation	Disable Enable	Enable or disable system's ability to hibernate (operating system S4 sleep state). Needs OS support for this feature.
ACPI Sleep State	Suspend Disabled S3 (Suspend to RAM)	Select the state used for ACPI system sleep/ suspend.
S3 Video Repost	Disable Enable	Enables or disables video BIOS screen when resume from S3 state.

Note! *ACPI (Advanced Configuration and Power Interface) is a Power Management and configuration standard for the PC. ACPI allows the operating system to control the amount of power each device is given (allowing it to put certain devices on standby or power-off for example). It is also used to control and/or check thermal zones (temperature sensors, fan speeds, etc), battery levels, PCI IRQ routing, CPUs, NUMA domains and many other things.*

3.1.2.3 AMT Configuration



Feature	Options	Description
Intel AMT	Disable Enable	Enable/Disable Intel ® Active Management Technology BIOS Extension. Note: iAMT H/W is always enabled. This option just controls the BIOS extension execution. If enabled, this requires additional firmware in the SPI device.
BIOS Hotkey Pressed	Disable Enable	Enable/Disable BIOS hotkey press. Enable this feature will show hotkey prompt at booting up screen.
MEBx Selection Screen	Disable Enable	Enable/Disable MEBx selection screen at booting up. This feature allows to enter ME configuration screens OR initiate a remote connection.
Hide Un-Configure ME Confirmation Prompt	Disable Enable	Hide Un-Configure ME without password Confirmation Prompt
MEBx Debug Message Output	Disable Enable	Enable MEBx debug message output. This feature is for debug purpose only.
Un-Configure ME	Disable Enable	Use this item to enable/disable un-configure ME without password.
AMT Wait Timer	0 ~ 65535	Set timer to wait before sending ASF_GET_BOOT_OPTOINS.
ASF	Disable Enable	Use this item to enable/disable Alert Specification Format.
Activate Remote Assistance Process	Disable Enable	Use this item to enable/disable trigger CIRA (Client Initiated Remote Access) boot.
USB Provisioning of AMT	Disable Enable	Enable/Disable of AMT USB Provisioning
PET Progress	Disable Enable	User can Enable/Disable PET Events progress to receive PET events or not