Alderamin Mk5

Version:
v1.1.0

Date:
25.11.2025

Contents

1 Copyright

2 Regulatory Compliances

2.1 CE and UKCA Notice

This device complies with the requirements of the CE directive and UKCA regulations.

Low Voltage Directive 2014/35/EU + Electrical Equipment Safety Regulations 2016 (SI 2016 No 1101)

- IEC 62368-1:2018
- EN IEC 62368-1:2020+A11:2020
- BS EN IEC 62368-1:2020+A11:2020

EMC Directive 2014/30/EU + Electromagnetic Compatibility Regulations 2016

- EN 55032:2015/A1:2020; CISPR 32:2015/AMD1:2019; BS EN 55032:2015+A1:2020
- EN 55035:2015/A1:2020; CISPR 35:2015/AMD1:2019; BS EN 55035:2015+A1:2020
- IEC 61000-3-2:2018/AMD1:2020/ISH1:2021; EN IEC 61000-3-2:2019+A1:2021; BS EN IEC 61000-3-2:2019+A1:2021
- IEC 61000-3-3:2013/AMD1:2017+A2:2021+COR1:2022; EN 61000-3-3:2013+A1:2019+A2:2021+AC:2022-01; BS EN 61000-3-3:2013+A1:2019+A2:2021
- EN 55035:2017+A11:2020; CISPR 35:2016; BS EN 55035:2017+A11:2020
- IEC 61000-4-2:2008; EN 61000-4-2:2009; BS EN 61000-4-2:2009
- IEC 61000-4-3:2020; EN IEC 61000-4-3:2020; BS EN IEC 61000-4-3-TC:2020
- IEC 61000-4-4:2012; EN 61000-4-4:2012; BS EN 61000-4-4:2012
- IEC 61000-4-5:2014/AMD1:2017; EN 61000-4-5:2014+A1:2017; BS EN 61000-4-5:2014+A1:2017
- IEC 61000-4-6:2023; EN IEC 61000-4-6:2023; BS EN IEC 61000-4-6-TC:2023
- IEC 61000-4-8:2009; EN 61000-4-8:2010; BS EN 61000-4-8:2010
- IEC 61000-4-11:2020/COR1:2020/COR2:2022; EN IEC 61000-4-11:2020/AC:2020-10; BS EN IEC 61000-4-11:2020

RoHS 2 Directive 2011/65/EU & 2015/863/EU + RoHS 2 Directive 2020 No. 1647

- Exemption(s) used:
- 6c,7a,7c,9a

UK CA CE

2.2 FCC PART 15 VERIFICATION STATEMENT

WARNING

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Notice: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

2.3 ICED-003 ISSUE 7 VERIFICATION STATEMENT

CAN ICES3(A)/NMB3(A)

This device complies with CAN ICES-003 Issue 7 Class A. Operation is subject to the following two conditions: (1) This devicemay not cause harmful interference, and (2) this devicemust accept any interference received, including interference that may cause undesired operation.

3 Intended Use and IT Security Instructions

This section provides crucial safety and security information and recommendations to help you configure your Welotec Industrial Computer (IPC) for optimal security in your deployment.

3.1 Intended Use

This section specifies the intended use and essential operating conditions for your Welotec Industrial Computer (hereinafter referred to as “IPC”).

The IPC is designed for use as a dedicated control, monitoring, and data acquisition unit within the enclosed control cabinet of a machine. Its primary function is to execute specific machine-control software, process operational data, provide human-machine interface (HMI) functionalities, and/or facilitate communication within the industrial automation environment. The IPC is exclusively intended for continuous operation within a controlled industrial setting.

The intended use of the IPC is strictly defined by the following conditions and requirements:

3.1.1 Physical Security and Installation Environment

- Enclosure: The IPC must be permanently installed within a secure, locked control cabinet (e.g., meeting IP54 or higher protection class) that provides adequate protection against dust, moisture, mechanical impact and unauthorized access.
- Controlled Access: Access to the control cabinet and its wiring must be restricted to authorized personnel only. Physical security measures (e.g., key locks, access control systems) are mandatory.
- Environmental Conditions:
  - Temperature: The IPC must operate within the specified ambient temperature and humidity range as outlined in the technical specifications. Adequate ventilation or active cooling within the cabinet must ensure these limits are not exceeded. This includes accounting for the unit’s own thermal dissipation and that of all other components in the cabinet.
  - Vibration and Shock: The IPC must be mounted securely within the cabinet to minimize exposure to excessive vibrations and mechanical shock, adhering to the manufacturer’s specifications.
  - Cleanliness: The inside of the cabinet must be kept free of dust, debris, and contaminants that could impair cooling or lead to electrical shorts.

3.1.2 EMC compliant electrical Installation and Power Supply

This product is designed to meet EMC standards when installed according to the following instructions. Failure to adhere to these instructions may result in the equipment failing to meet compliance standards and can cause interference with other devices. The installer is responsible for ensuring the EMC conformity of the final system.

- Power Supply: The IPC must be connected to a dedicated stable and filtered power supply within the specified voltage range. To ensure operational reliability and meet EMC requirements, the power source must provide adequate filtering against surges, transients, electrical fast transients (EFTs), and conducted RF noise common in industrial environments. An Uninterruptible Power Supply (UPS) is highly recommended to protect further against power fluctuations and outages.

- Wiring: All wiring connecting to the IPC must comply with applicable industrial wiring standards, be properly insulated, strain-relieved, and protected against mechanical damage.
- Grounding: The unit must be properly grounded according to the installation manual, typically via a low-impedance connection to the control cabinet's central grounding point.

3.1.3 Functional Safety

This unit is not certified as a standalone component for functional safety applications (e.g., SIL, PL).

Intended Use: The unit is intended for standard control and monitoring. It must not be used as the sole or primary controller for safety-critical functions (e.g., emergency stops, safety interlocks, light curtains, burner controls).

System Integration: Safety-related control logic must be executed by dedicated, certified safety controllers (e.g., Safety PLC, safety relays). This unit may be used to supervise or monitor a safety system (e.g., for HMI visualization or data logging) via a non-safety-rated communication channel, but it must not be part of the safety-critical control loop. The failure of this unit must not lead to a loss of the primary safety function.

3.1.4 Qualified and Trained Personnel

- Installation, Configuration, and Maintenance: All installation, configuration, maintenance, troubleshooting, and repair activities on the IPC and its connections within the control cabinet must be performed exclusively by qualified, trained, and authorized technical personnel. This personnel must possess proven expertise in electrical systems, IT hardware, and cybersecurity best practices.
- Security Awareness: All personnel interacting with the IPC or the network it is connected to must receive regular training on IT security awareness including password policies and reporting suspicious activities.

3.1.5 Software and Configuration

- Operating System: Only the pre-installed or manufacturer-approved operating system (OS) version may be used. The OS must be regularly updated with security patches provided by the manufacturer or OS vendor, after thorough testing in a non-production environment.
- Secure Configuration: The IPC's operating system, firmware, and installed applications must be configured according to secure hardening guidelines, including disabling unused services, ports, and protocols, and enforcing strong password policies.
- Secure Boot: Where supported Secure Boot must be enabled to prevent the loading of unsigned or malicious bootloaders.

Please refer to the section "Cyber Security" for further details.

3.1.6 Network Segmentation and "Defense in Depth" IT Security Principles

- Network Segmentation: The unit and its control network must be isolated from all other networks (e.g., corporate, guest, public internet) using industrial firewalls and network segmentation. Direct connection to the internet is considered misuse unless done via a secure, managed gateway.
- Defense in Depth: A multi-layered security approach ("Defense in Depth") must be implemented for the entire machine. This includes:
  - Network Security: Industrial Firewalls (e.g., Next-Generation Firewalls) at network boundaries, strict firewall rules (whitelist approach – only allow explicitly required traffic), VLANs for segmentation.
  - System Security: Operating system hardening (minimum services, disabled unnecessary ports), regular security updates, robust antivirus/anti-malware solutions specifically designed for industrial environments, and strong password policies.

  - Application Security: Secure configuration of all industrial applications, disabling default credentials, and ensuring application-level security features are enabled.
  - Data Integrity: Measures to ensure data integrity and availability (e.g., backups, redundant systems where appropriate).
  - Physical Security: see above

- Access Control: Remote access to the IPC (if required) must be strictly controlled, using secure connections, multi-factor authentication, and granular user permissions. Unnecessary remote access functionalities must be disabled.
- Logging and Monitoring: The IPC and connected network devices should implement logging of security-relevant events. Centralized monitoring and alerting systems are recommended for timely detection of anomalies.

3.2 Non-Intended Use

Any use of the IPC that deviates from the conditions described including but not limited to:

- Operation outside the specified environmental limits.
- Operation without a secure, enclosed control cabinet.
- Operation in hazardous locations (e.g., explosive atmospheres) for which the unit is not explicitly certified.
- Installation or maintenance by unqualified personnel.
- Connection to an unfiltered, unstable, or non-grounded power source.
- Direct connection to unsecured corporate networks or the internet without adequate protective measures.
- Installation of unauthorized software or operating systems.
- Bypassing or disabling of security features (e.g., firewall, antivirus, Secure Boot).
- Failure to implement a cyber security management plan (patching, hardening, access control).

is considered non-intended use and may result in:

- Damage to the IPC or the machine.
- Compromised data security and integrity.
- Serious personal injury or death.
- Failure to comply with regulatory requirements.

3.3 Exposed Interfaces and Services

The following interfaces are exposed:

Interface	Comment
LAN 1 … 4	
COM 1 … 3	
USB 1 … 8	
HDMI	
DP	
GPIO	
VGA	
Mic-In	
Line-Out	
Reset	External Reset
SW	Power Switch

Available services highly depend on Operating System type and version.

3.4 Cyber Security

The flexibility to run common operating systems like Windows and Linux places the full responsibility of cyber security implementation on the system integrator and end-user. The unit is a component that must be integrated into a comprehensive, defense-in-depth security architecture.

The intended use requires the integrator/user to implement, at a minimum, the following:

3.4.1 Use Secure Boot

Secure Boot is a crucial security feature that helps protect your system from malware and unauthorized operating systems during the boot process. It's a component of the Unified Extensible Firmware Interface (UEFI) that ensures only trustworthy software, signed with a digital certificate, loads when your system starts. Without Secure Boot, malicious programs or unsigned operating systems could load unnoticed before the actual operating system, compromising your system's integrity and security.

We highly recommend enabling Secure Boot - please refer to "BIOS" section for further details

3.4.2 Enable Storage Encryption

Storage encryption is a critical security measure that protects your sensitive data by rendering it unreadable to unauthorized parties, even if they gain physical access to your storage device. In today's interconnected world, where devices can be lost, stolen, or compromised, ensuring the confidentiality of your information is paramount.

Windows (using BitLocker with TPM)

Windows' built-in BitLocker encryption leverages the TPM to securely store the encryption key, making the process largely automatic and secure.

- Check TPM Status: Ensure that the TPM chip is enabled in the UEFI/BIOS settings
- Open BitLocker Drive Encryption: Search for "BitLocker" in the Windows search bar and select "Manage BitLocker."
- Turn on BitLocker: Select the drive you wish to encrypt (typically your C: drive) and click "Turn on BitLocker."
- Follow the Wizard: Windows will guide you through the process. Since a TPM is present, it will typically automatically use the TPM to store the encryption key. You will be prompted to save a recovery key (e.g., to a Microsoft account, a USB drive, or print it) – this is crucial in case you ever need to access your data if the TPM is reset or unavailable.
- Start Encryption: The encryption process will begin in the background. You can continue using your computer during this time.

Linux (using LUKS with TPM consideration):

Linux uses LUKS (Linux Unified Key Setup) for full disk encryption. Integrating it with a TPM for automatic unlocking at boot can be more involved than BitLocker but offers similar benefits. This typically involves tools like clevis or systemd-cryptenroll.

- Install Necessary Tools: You'll need cryptsetup for LUKS and potentially tpm2-tools and clevis (or similar TPM integration tools) if you want to bind your LUKS key to the TPM for automatic decryption.
- Encrypt the Drive (during OS Installation or manually):
  - During Installation: Most Linux distributions (e.g., Ubuntu, Fedora) offer an option to "Encrypt the disk" during the installation process. This is the simplest way to set up LUKS.
  - Manually (Post-Installation): If encrypting an existing drive or a secondary drive, you would use cryptsetup luksFormat /dev/sdXy to format the partition for LUKS, followed by cryptsetup luksOpen /dev/sdXy my_encrypted_drive and then creating a filesystem on the opened device.
- Bind LUKS Key to TPM (Optional, for automatic unlock):
  - This is the step that utilizes the TPM. Tools like clevis can be used to "bind" a LUKS passphrase (or a key slot) to the TPM. This allows the system to automatically unlock the encrypted volume at boot if the TPM verifies the system's integrity.
  - The exact commands vary, but it generally involves generating a new LUKS key slot and then using a TPM-binding tool to store the key in the TPM and configure the system to use it for unlocking.
- Update Boot Configuration: Ensure your bootloader (e.g., GRUB) is configured correctly to handle the encrypted root partition and, if used, to leverage the TPM for unlocking.

For both operating systems, it's essential to:

- Backup your recovery keys/passphrases: Without them, your data can be permanently lost if there's a hardware failure or you forget your primary password.
- Understand the implications: While encryption provides strong security, proper handling of keys and adherence to security best practices are still crucial.

3.4.3 Use Strong Passwords

Strong passwords are the first line of defense against unauthorized access. If you want to use password based access it is recommended to:

- Change the factory default password on first login
- Use passwords with a minimum length of 12 characters or more
- Use a combination of uppercase and lowercase letters, numbers, and special characters (e.g., !@#$%^&*)
- Do not use easily guessable patterns, such as sequences (e.g., “123456”, “abcdef”), repeated characters (e.g., “aaaaaa”), or dictionary words

3.4.4 System Hardening:

The operating system (Windows or Linux) must be hardened. This includes:

- Disabling all unused services, applications, and network ports.
- Enforcing strong, unique passwords for all accounts.
- Implementing a least-privilege access model for users and applications.
- Configuring OS-level firewalls (e.g., ufw, Windows Defender Firewall).

3.4.5 Patch Management

A robust process must be in place for testing and deploying security patches for the operating system and all installed third-party applications. This process must be compatible with the operational constraints of the industrial environment.

3.4.6 Endpoint Protection

Where appropriate for the application, industrial-compatible endpoint protection (e.g., anti-malware, application whitelisting, host-based intrusion detection) must be installed, maintained, and kept up-to-date.

3.4.7 Physical Security

Use of the locked control cabinet (see Section 3) to prevent unauthorized physical access and tampering (e.g., via USB ports) is a critical part of the security model.

3.5 Vulnerability Handling

Welotec has implemented a Coordinated Vulnerability Disclosure Policy - please visit the following site for further details: https://welotec.com/pages/coordinated-vulnerability-disclosure-policy

4 Safety Instructions

Please read these instructions carefully and retain them for future reference.

1. Disconnect this equipment from the power outlet before cleaning. Do not use liquid or sprayed detergent for cleaning. Use a moist cloth or sheet.
2. Keep this equipment away from humidity.
3. Ensure the power cord is positioned to prevent tripping hazards and do not place anything on top of it.
4. Pay attention to all cautions and warnings on the equipment.
5. If the equipment is not used for an extended period, disconnect it from the main power to avoid damage from transient over-voltage.
6. **Prolonged usage with less than 12V may damage the PSU or destroy the mainboard.**
7. Never pour any liquid into openings as this could cause fire or electrical shock.
8. Have the equipment checked by service personnel if:
    - The power cord or plug is damaged.
    - Liquid has penetrated the equipment.
    - The equipment has been exposed to moisture in a condensation environment.
    - The equipment does not function properly, or you cannot get it to work by following the user manual.
    - The equipment has been dropped and damaged.
9. Do not leave this equipment in an unconditioned environment, with storage temperatures below -20 degrees or above 60 degrees Celsius for extended periods, as this may damage the equipment.
10. Unplug the power cord when performing any service or adding optional kits.
11. Lithium Battery Caution:
    - Risk of explosion if the battery is replaced incorrectly. Replace only with the original or an equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.
    - Do not remove the cover, and ensure no user-serviceable components are inside. Take the unit to a service center for service and repair.

⚠ Warning!
Always completely disconnect the power cord from your chassis whenever you work with the hardware. Do not make connections while the power is on. Sensitive electronic components can be damaged by sudden power surges. Only experienced electronics personnel should open the PC chassis.

⚠ Caution!
Always ground yourself to remove any static charge before touching the CPU card. Modern electronic devices are very sensitive to static electric charges. As a safety precaution, use a grounding wrist strap at all times. Place all electronic components in a static-dissipative surface or static-shielded bag when they are not in the chassis.

5 Product Specifications

5.1 Features

The **Alderamin MK5 Embedded System** delivers high performance and versatility with the following key features:

- **Powerful Processing**: Supports **14th Generation Intel® Core™ i9 / i7 / i5 / i3** processors.
- **Triple Display Support**: Connect via **HDMI, DisplayPort, and VGA** for enhanced multi-screen capabilities.
- **Fan-less & Expandable Design**: Ensures silent operation with modular expansion options.
- **Versatile Connectivity**: Expand via **COM, DIO, LAN, and PoE modules** for diverse applications.
- **Vehicle-Ready Power Ignition**: Supports **Xpansion Module** for in-vehicle applications.
- **Wide Power Range**: Operates on a **9-48V power supply** for industrial adaptability.
- **Extreme Temperature Tolerance**:
  - **-40°C to 70°C** with a **35W CPU**
  - **-40°C to 50°C** with a **51-65W CPU**
  - **-40°C to 40°C** with a **71-80W CPU**

5.2 Alderamin MK5 & Alderamin MK5-D CPU Options

Processor Name	Cores	Threads	TDP
Intel® Raptor Lake Refresh 14th Generation			
Intel® Core™ i9-14900T – 36M Cache, up to 5.50 GHz	24	32	35W
Intel® Core™ i7-14700T – 33M Cache, up to 5.20 GHz	20	28	35W
Intel® Core™ i5-14500T – 20M Cache, up to 4.50 GHz	10	16	35W
Intel® Core™ i3-14100T – 20M Cache, up to 4.50 GHz	4	8	35W

5.3 Technical Details

Feature	Specification	Details
Processor	CPU	14th Gen Intel® Raptor Lake Refresh Core-i FC-LGA16A Socket Processor, TDP Max. 65W
Chipset	Chipset	Intel® R680E
Memory	System Memory	DDR5 4800MHz, 2 x 262-pin SO-DIMM, Max. 96GB (i7 / i9: ECC; i3 / i5: Non-ECC)
Graphics	GPU	Intel® UHD Graphics 730 (i3 / i5), 770 (i7 / i9)
Storage	Storage Slots	2 x 2.5” HDD / SSD (1 w/ Removable HDD Bay; 2 w/ Internal HDD Bracket) 1 x mSATA
Networking	Ethernet	4x Intel® I226-LM 2.5 Gigabit LAN
Audio	Audio	Realtek® ALC888
Security	I/O Chipset	Nuvoton NCT6126D
	TPM	Nuvoton NPCT760AABYX
I/O Ports	Front I/O	1 x HDMI 1.4 2 x USB 3.2 Gen2 2 x SIM Card Slot w/ Cover 1 x 2.5” SATAIII HDD / SSD Bay
	Rear I/O	4 x RJ-45 6 x USB 3.2 Gen 2 (10 Gbps) 3 x RS232 / 422 / 485 (Support Power 5V / 12V) 6 x SMA Antenna (Optional for WiFi/LTE function) 1 x 8-bit GPIO (in DB9 Connector) 1 x DisplayPort 1.2 1 x VGA 1 x Mic-in 1 x Line-out 1 x PCIe x16 slot 1 x 2-pin Terminal Block Remote Power Reset 1 x 3-pin Terminal Block Power Input 1 x 2-pin Terminal Block Remote Power On/Off
Power	Power Input	9~48V Wide Range DC Input w/ Terminal Block Connectivity
Cooling	Thermal Design	Fanless (MK5) / Optional Internal System Fans (MK5-D)
Mechanical	Mounting	Wall mount
	Dimensions	MK5: 10.6” x 9.7” x 4.3” (268 mm x 246 mm x 108 mm) MK5-D: 10.6” x 9.7” x 5” (268 mm x 246 mm x 128 mm)
	Material	Top cover: Aluminum Alloy Bezel and chassis: Steel
Environmental	Operating Temperature	**Fanless Design (MK5 & MK5-D):** 35W TDP: -40°C to 70°C 51~65W TDP: -40°C to 50°C 71~80W TDP: -40°C to 40°C **MK5-D with Internal Fans:** 35W TDP: -20°C to 50°C 51~65W TDP: -20°C to 45°C 71~80W TDP: -20°C to 40°C
	Operating	10%~90% R/H (Non-condensing)

5.4 ⊠ Important Notes

Restricted Access Location (RAL) A Restricted Access Location is an area with extreme temperatures where only authorized personnel can enter for specific purposes.

1. Access is limited to trained personnel aware of location restrictions and necessary precautions.
2. Entry requires security measures such as tools, lock-and-key, or controlled access by the responsible authority.

Power Consumption Considerations Ensure power consumption is within the power supply's specifications.

- Recommended AC Adapters:
  - **AC/DC 24V/12.5A, 300W** (3PIN Terminal Block Power Adaptor)
  - **AC/DC 24V/9.16A, 220W** (3PIN Terminal Block Power Adaptor)

Ambient Temperature Precaution

- The maximum safe operating temperature is **40°C** if the external AC adapter model **EA12501J** or **EA13001N** is placed in the same high-temperature area as the embedded system.

PXE Application Requirement

- Before OS installation via PXE server, pre-install the **i219-LM driver** in the OS image.

Lithium Battery Safety Warning

- **Caution:** This system contains a **Lithium battery**.
- Do **NOT** puncture, mutilate, or dispose of it in fire.
- Risk of **explosion** if replaced incorrectly—use only manufacturer-recommended replacements.
- Dispose of batteries as per manufacturer instructions and local regulations.

System Shutdown Risks The following configurations may cause unexpected shutdowns:

- **12 x LANs** or **10 x PoE LANs** with certain **NVMe SSD models** (Check compatibility with sales support).
- **12 x LANs** or **10 x PoE LANs** with **mPCIe or M.2 Wi-Fi Cards** (Excludes CNVi Wi-Fi Cards; check compatibility with sales support).

BIOS Flashing Precautions

- **Read BIOS release notes before re-flashing BIOS.**
- If BIOS resets to default settings post-flash, verify configuration before booting.
- **Incorrect RAID settings** may cause system boot failure.

PCIe GFX Card Installation Considerations

- With a **PCIe GFX card** installed in **Alderamin MK5-D**, BIOS setup will only support display output via the **external graphics card**.

Storage Limitations for Dual-Layer PCIe GFX Cards

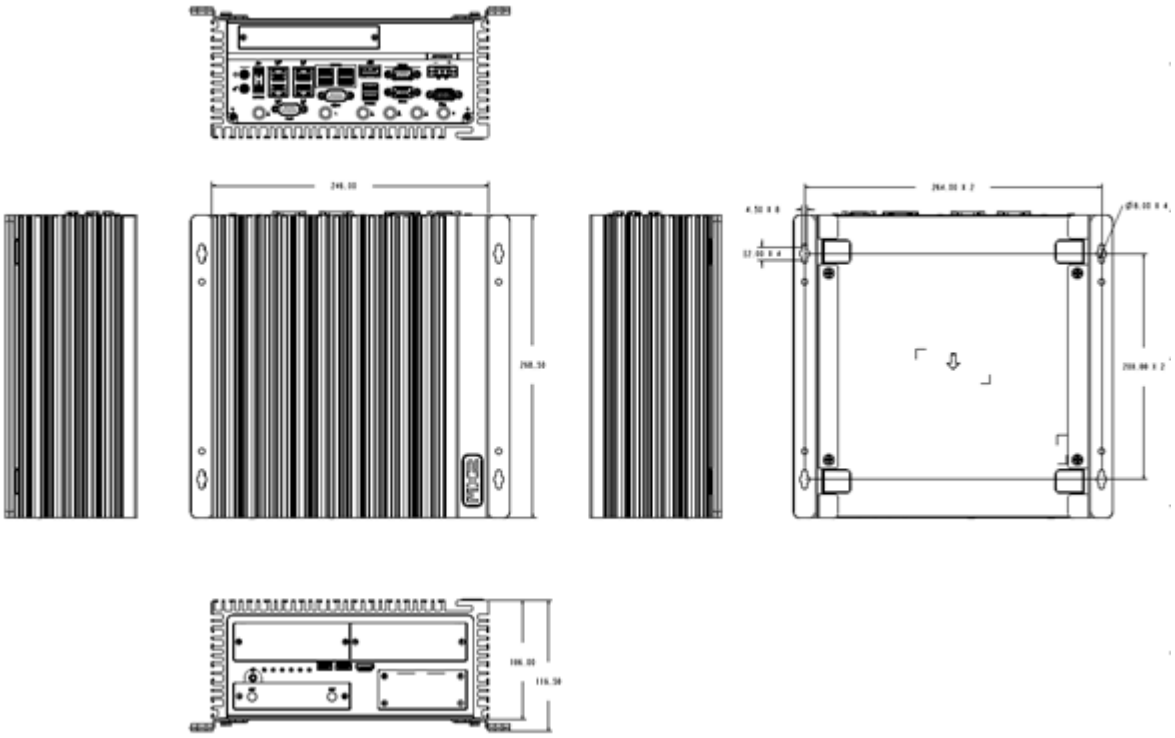
- Installing a **dual-layer PCIe GFX card** allows only **one** internal HDD/SSD (excluding removable HDD/SSD) instead of **two** due to mechanical constraints.
- **SATA cable connector** must be inserted into the **SATA port next to the 2 × 40x40x20mm internal system fan**.
- **Cable clip removal may be required** for clearance with the graphics card.

Storage Limitations for NVIDIA T4/P4 AI Card

- Installing an **NVIDIA T4 or P4 AI card** with **2 × 40x40x28mm internal fans and a fan duct** allows only **one** internal HDD/SSD (excluding removable HDD/SSD) instead of **two** to prevent interference.
- **SATA cable connector** must be inserted into the **internal SATA connector**.

5.5 Alderamin MK5

- **Mechanical Dimensions:** 268 mm x 246 mm x 108 mm
- **PCI Express x16 Slot Maximum Card Dimensions:**
  - **111.15 x 200 x 18.7 mm** (with mPCIe PoE Module)
  - **111.15 x 230 x 18.7 mm** (without mPCIe PoE Module)



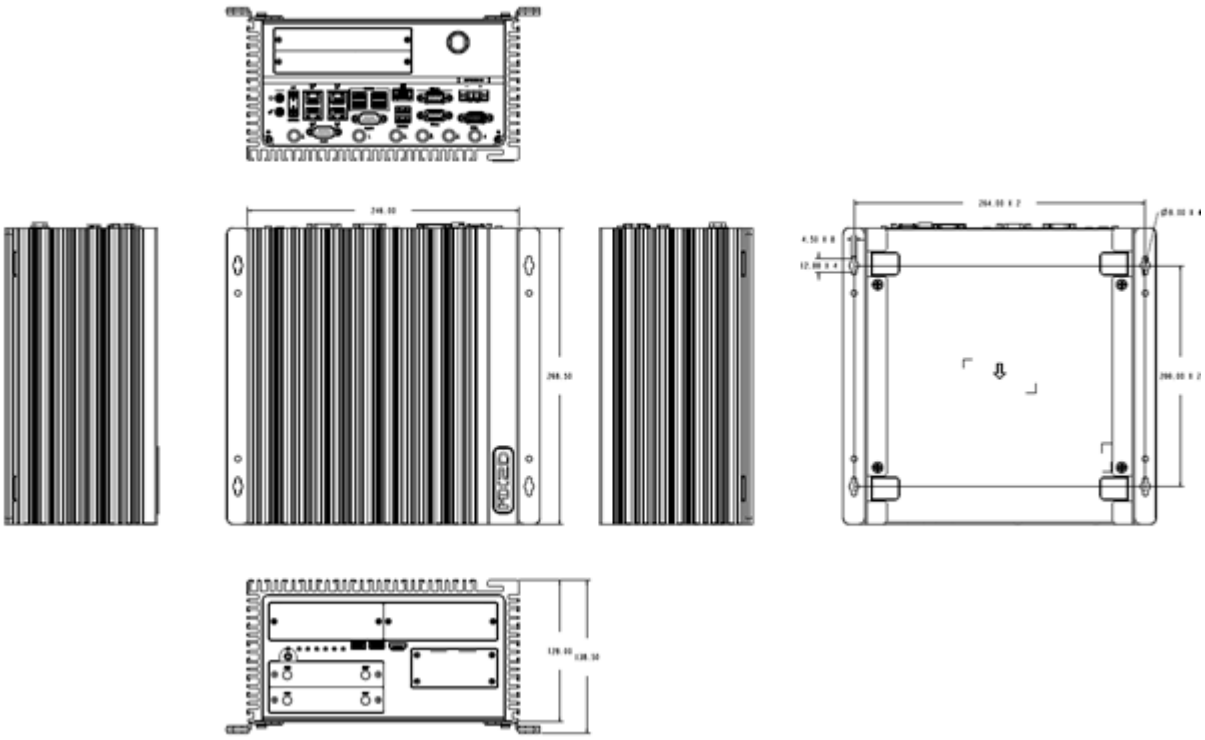
5.6 Alderamin MK5-D

- **Mechanical Dimensions:** 268 mm x 246 mm x 128 mm
- **PCI Express x16 Slot Maximum Card Dimensions:**
  - **145 x 221 x 43 mm** (without mPCIe PoE Module)
- **PCI Express Slot Configurations:**
  - **PCI Express X16 + X1 Dual Slot** (Default)
  - **PCI Express X8 + X8 Dual Slot** (Optional)

5.6.1 AI & Graphics Card Support List:

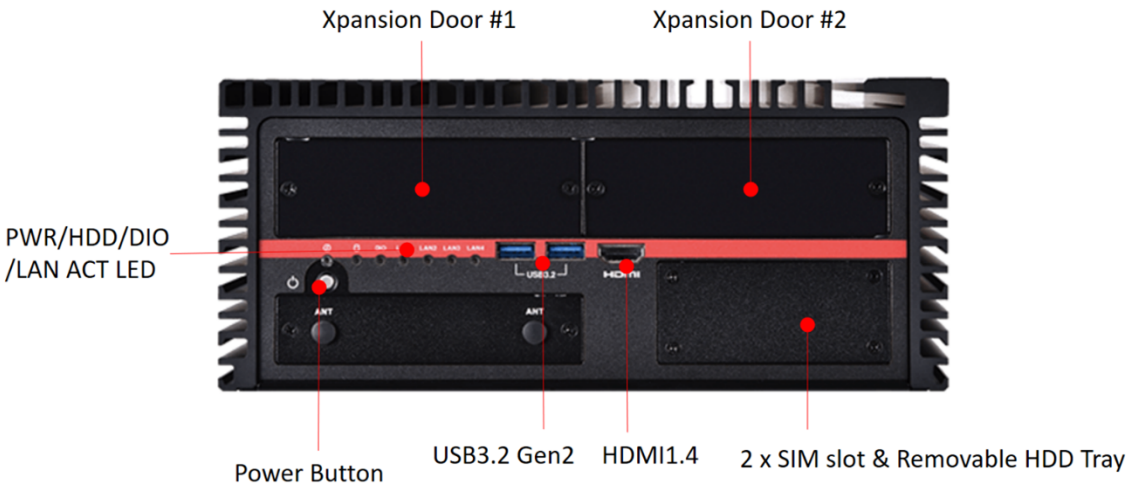
- **NVIDIA Quadro P400** (30W)
- **NVIDIA Quadro P620** (40W)
- **NVIDIA Quadro P2000** (75W)
- **NVIDIA Tesla T4 / P4** (75W)
- **Aetina GTX1050 N1050-J9FX** (2GB, 75W)
- **Leadtek WinFast GTX1650** (4GB, 75W)

- **Leadtek WinFast GTX1660 HURRICANE** (6GB, 120W) *Requires secondary 12V, 180W AC Adapter*
- **Leadtek WinFast GTX1660 Ti HURRICANE** (6GB, 120W) *Requires secondary 12V, 180W AC Adapter*



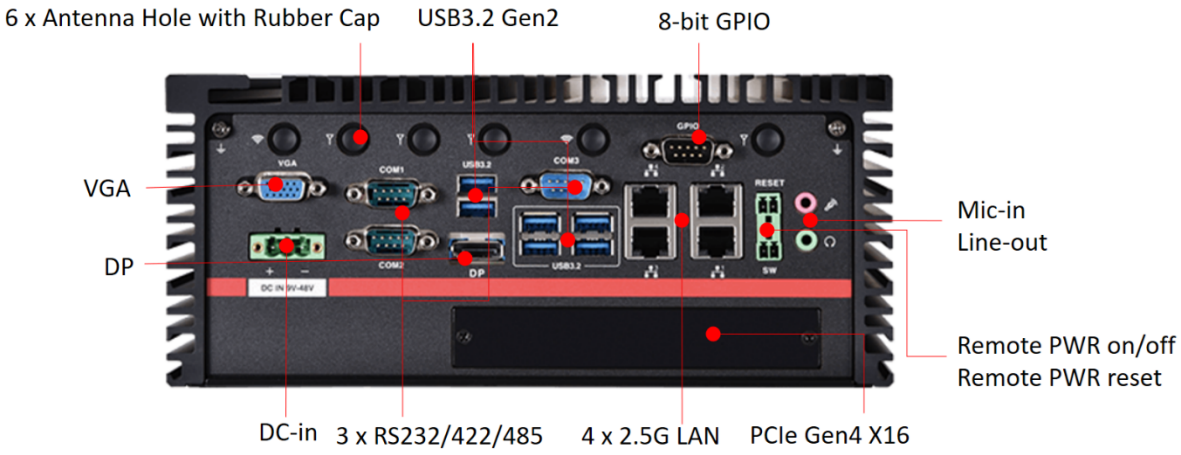
6 Interfaces and Connections

6.1 Front I/O

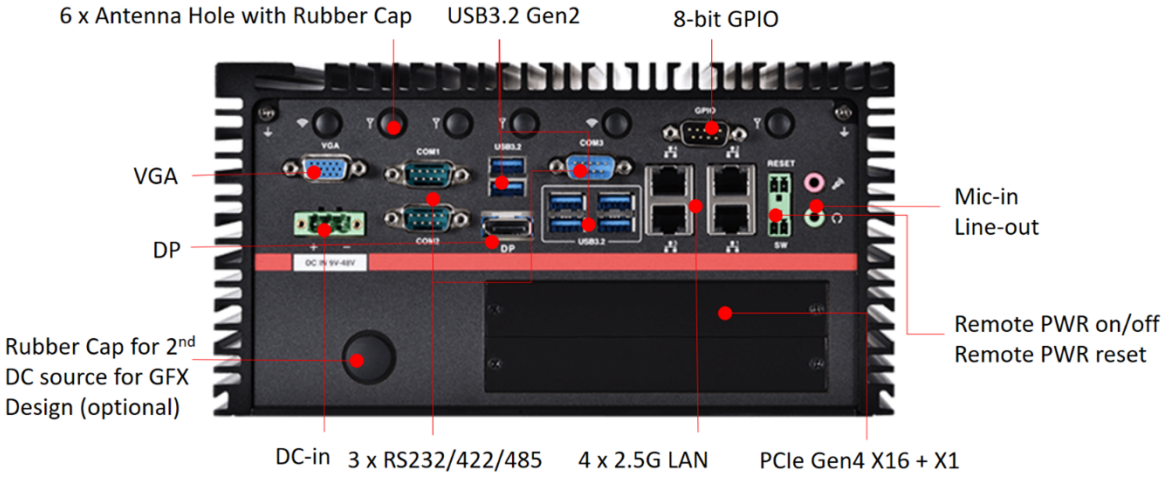


6.2 Rear I/O

6.2.1 Alderamin MK5



6.2.2 Alderamin MK5-D



Note: The recommended dimensions for a USB cable connector or device for USB 2.0 ports are **9mm height x 19mm width** when all other I/O ports are occupied. However, compatibility also depends on the dimensions of the DisplayPort connector and other devices to avoid interference.

6.3 Expansion Module (Optional) Configuration Table

Expansion	Function	1	2	3
COM/DIO	4x COM, 8x DIO	X	X	
PoE RJ45	4x Gigabit PoE RJ45	X	X	
PoE M12	4x Gigabit PoE M12	X	X	
DualLAN	2x Gigabit LAN RJ45			X

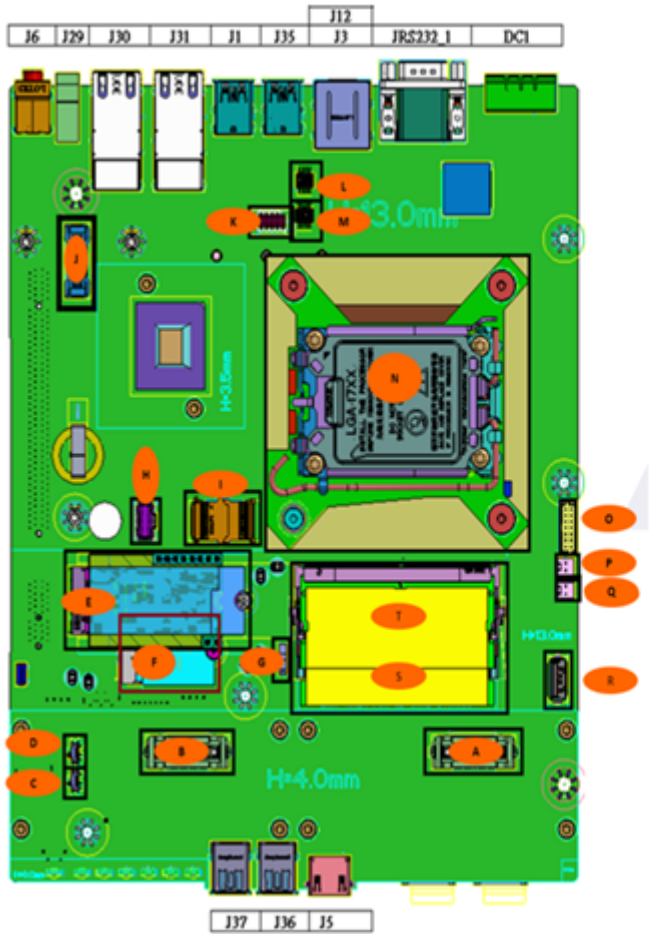
6.4 Recommended PoE Configuration and Environmental Spec Matrix

CPU TDP	PoE Configuration	Max. Ambient (°C)	CPU Utility	Memory Loading	HDD/SSD Loading	PoE Power %
35W	None	70	100%	40%	10%	-
35W	x2 PoE ports (Max. 30W)	65	70%	40%	10%	70%
35W	x4 PoE ports (Max. 50W)	60	70%	40%	10%	70%
35W	x6 PoE ports (Max. 80W)	55	70%	40%	10%	70%
35W	x8 PoE ports (Max. 100W)	50	70%	40%	10%	70%
35W	x12 PoE ports (Max. 130W)	40	70%	40%	10%	70%

7 DIP Switch Settings and Pin Definitions

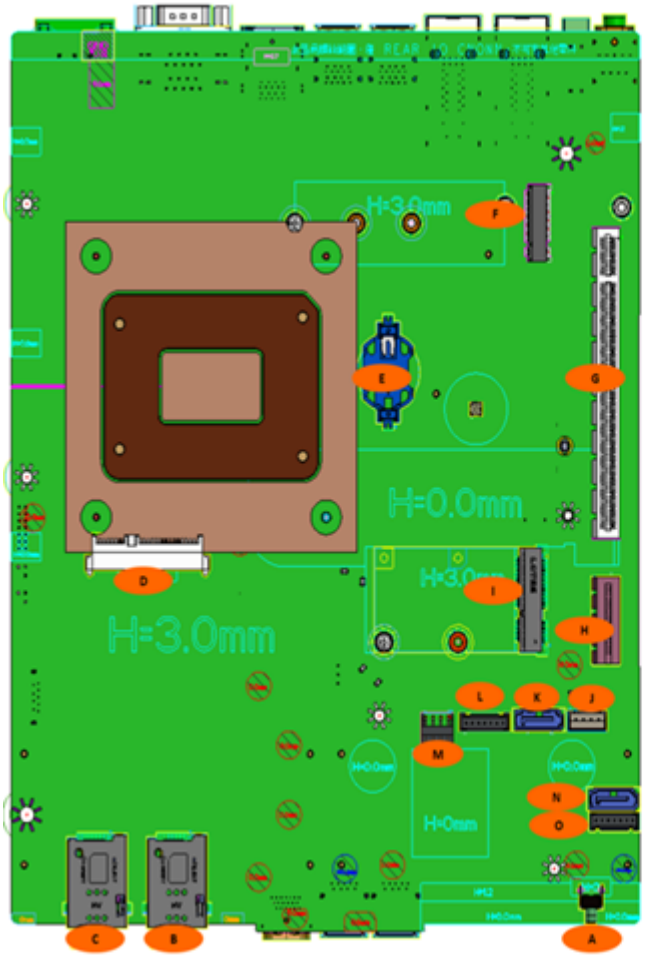
7.1 Jumper and Internal Connector Placement

7.1.1 Overall Layout



Side IO	
J6	AUDIO: MIC/ LINE OUT
J29	Power ON/OFF(Low)/ Reset(High)
J30	DUAL LAN CONN
J31	DUAL LAN CONN
J1	DUAL USB3.2 CONN
J35	DUAL USB3.2 CONN
J12	DUAL USB3.2 (stack-high)
J3	Display port ((stack-low)
JRS232_1	JRS232 CONN
DC1	DC Power CONN
J5	HDMI port
J36	USB3.2 CONN
J37	USB3.2 CONN

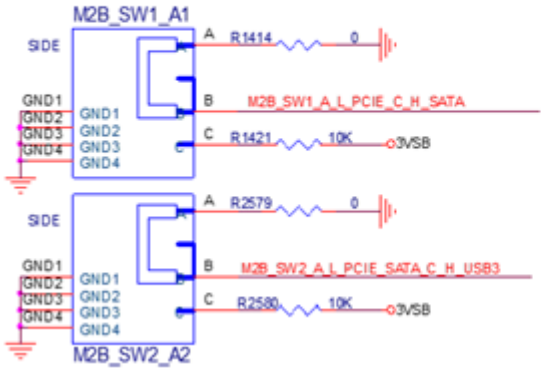
TOP side internal		
A	J16	Board to board 1
B	J17	Board to board 2
C	M2B_SW2_A1	M2B-PCIe/sata/USB3 switch
D	M2B_SW1_A1	M2B-PCIe/sata/USB3 switch
E	M2B1	M.2 key B
F	M2E1	M.2 key E
G	SW1	AT/ATX mode
H	J24	DIO header
I	E1	BIOS socket
J	J11	POE module header
K	J_RS232_P1	RS232 header
L	SW2	COM port RI power selector
M	SW3	COM port RI power selector
N	CPU SOCKET	CPU socket
O	J2	VGA header
P	J27	VCC output header
Q	J28	VCC output header
R	J15	USB3.1 header
S	DIMM2	DIMM2-DDR5
T	DIMM1	DIMM1-DDR5



BTN side internal		
A	PWR_BTN1	Power ON/OFF Button
B	SIM2_J1	SIM card header
C	SIM2_J2	SIM card header
D	J18	SATA header
E	XBT1	RTC battery header
F	M2M1	M.2 -m key Slot
G	PCIE_X16_SLOT1	PCIe X16 slot
H	PCIE_X1_SLOT1	PCIe X1 slot
I	MPCIE1	Mini PCIe slot
J	J26	Power Header(12V-5A)
K	J22	SATA header
L	J19	SATA Power header (12V/ 5V /3V)
M	J25	System FAN header
N	J21	SATA header
O	J20	SATA Power header (12V/ 5V /3V)

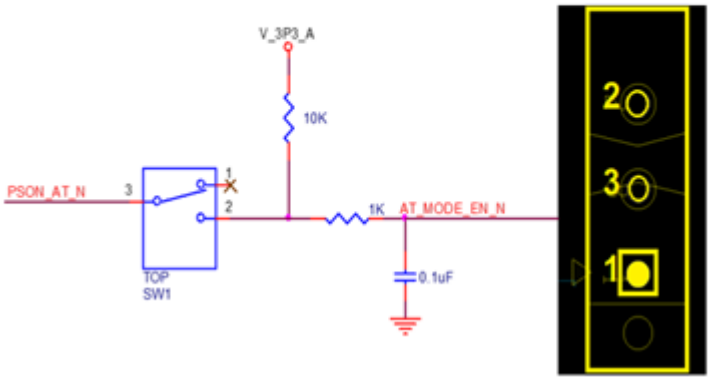
7.2 DIP Switch Settings

D	M2B_SW1_A1	M2B-PCIe/SATA/USB3 switch-1
C	M2B_SW2_A1	M2B-PCIe/SATA/USB3 switch-2

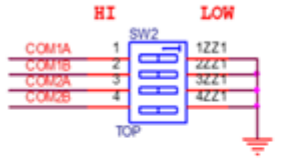


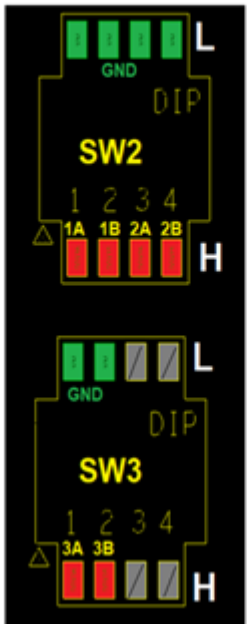
Function	M2B_SW1	M2B_SW2
PCIe	A	A
SATA	C	A
USB3.0	X (A or C)	C

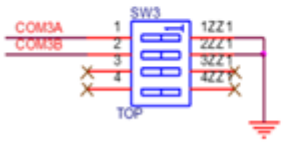
G	SW1	AT/ATX mode
	Pin1- Pin3	Normal mode
	Pin2- Pin3	AT mode



L	SW2	COM port RI power selector
M	SW3	COM port RI power selector







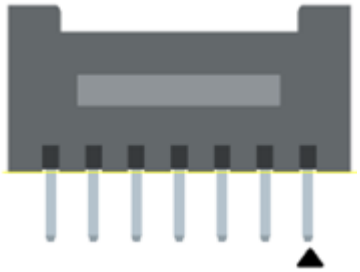
	COM1A	COM1B	COM1 MULTI_NRI1
SW2	Low	Low	Ring
	Low	High	5V
	High	Low	12V
	COM2A	COM2B	COM2 MULTI_NRI2
	Low	Low	Ring
	Low	High	5V
	High	Low	12V
SW3	COM3A	COM3B	COM3 J_RS232_P1
	Low	Low	Ring
	Low	High	5V
	High	Low	12V

7.3 Internal Connector Pin Definition

7.3.1 1st SATA Connector (Location J18)

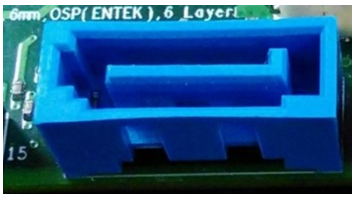
Pin	Signal Name
P1-P3	VCC3
P4-P6	GND
P7-P9	VCC
P10	GND
P11	RES
P12	GND
P13-P15	+12V
S1	GND
S2	SATAHDR_TXP0_C
S3	SATAHDR_TXN0_C
S4	GND
S5	SATAHDR_RXN0_C
S6	SATAHDR_RXP0_C
S7	GND

7.3.2 SATA Power Headers (Location J19/J20 - 2nd & 3rd SATA Power Headers)



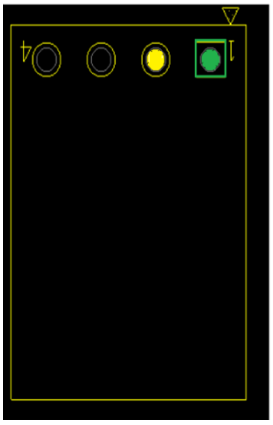
Pin	Signal Name
1	VCC3
2	GND
3-4	VCC
5	GND
6-7	+12V

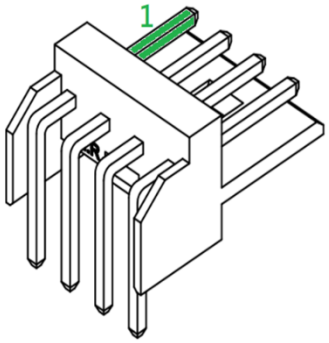
7.3.3 SATA Signal Headers (Location J19/J20 - 2nd & 3rd SATA Signal Headers)



Pin	Signal Name	Description
1	GND	Ground
2	SATAHDR_TXP_C	SATA Data Transmit (Positive)
3	SATAHDR_TXN_C	SATA Data Transmit (Negative)
4	GND	Ground
5	SATAHDR_RXN_C	SATA Data Receive (Negative)
6	SATAHDR_RXP_C	SATA Data Receive (Positive)
7	GND	Ground
8	G1	GND
9	G2	GND

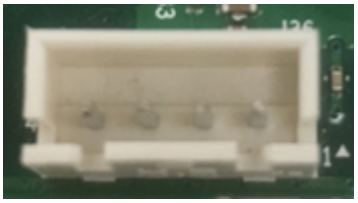
7.3.4 Fan Header (Location J25)





Pin	Signal
1	Ground
2	+12V
3	CPU_FAN_TACH
4	CPU_FAN_CTRL

7.3.5 12V/5A Power Headers for PoE Expansion (Location J26)



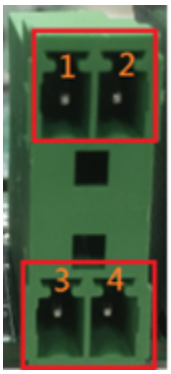
Pin	Signal
1	Ground
2-3	+12V
4	GND

7.4 External Connector Pin Definitions

7.4.1 3-Pin Terminal Block for DC Input

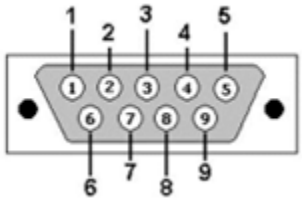
Pin	Signal
1	DC IN +9~48VIN
2	N/A
3	GND

7.4.2 2-Pin Terminal Block for Remote Power ON/OFF and Reset



Pin	Signal
1	Ground
2	EXT Reset
3	Ground
4	EXT_PWRBT_ON/OFF

7.4.3 COM#1 / COM#2 / COM#3



Pin No	RS-232	RS-422	RS-485
1	DCD	TX-	DATA-
2	RX	TX+	DATA+
3	RTX	RX+	NC
4	DTR	RX-	NC
5	GND	GND	GND
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC

7.5 Expansion Module DIO/COM

The DIO/COM module consists of two parts: **Serial COM** and **Digital IO** functions.
Please refer to the guideline for instructions on how to correctly set up this module.

7.5.1 COM Port Setting

Location

The **DIO/COM** module has a total of **4 COM ports**. These ports can be configured as:

- RS232
- RS422
- RS485
- Powered RS232

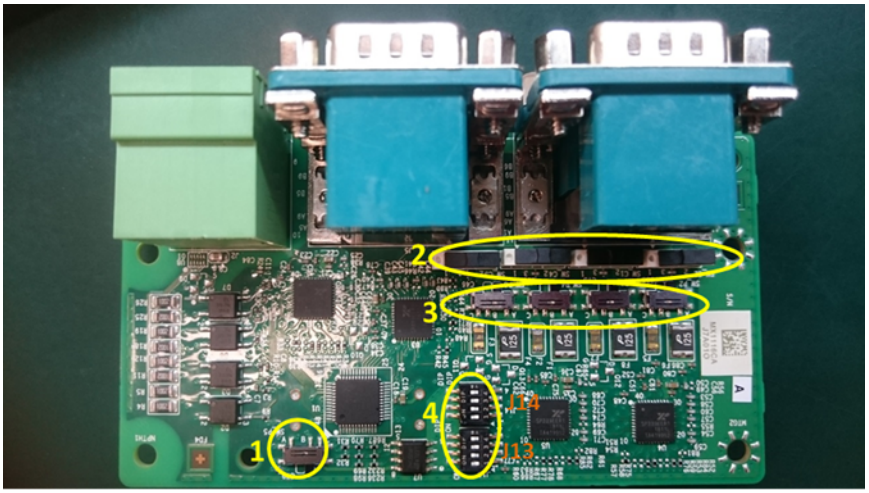
There are two types of **Expansion COM drivers**:

1. **Standard non-fixed COM port order driver**
2. **Fixed COM order driver**

If the **fixed COM port order driver** is installed, the positions will be as follows:

- 1st DIO/COM (Left Expansion Door)
- 2nd DIO/COM (Right Expansion Door)

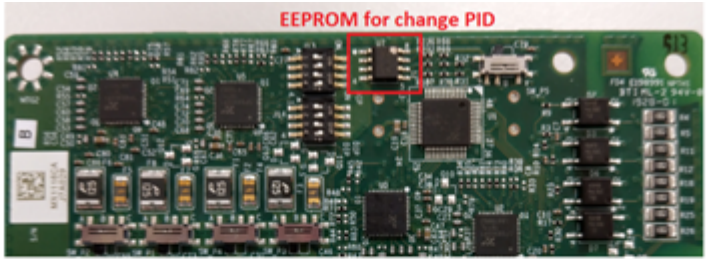
7.5.2 DIP Switch Function



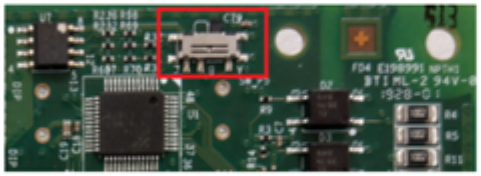
COM PID Selection Switch

- **Set A-B**: COM PID 0x1414 is determined by the UART controller (default).
- **Set B-C**: COM PID 0x1415 is determined by EEPROM (for 2nd MS-48CDN-DT10).

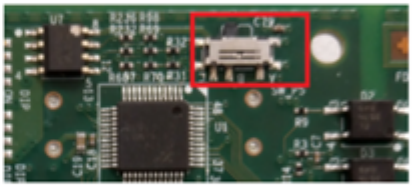
PID and Driver Version Matrix Table



PID 0x1414 from COM chip



PID 0x1415 from EERPOM



Fix COM driver (2.5.0.5) "SW Control table V0.21"	PID 0x1414	PID 0x1415
COM sequence	COM 12 ~ COM 15	COM 16 ~ 19

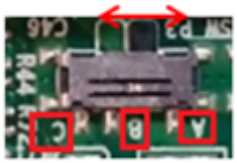
Standard driver (2.5.0.3) "SW Control table V0.21"	PID 0x1414	PID 0x1415
COM sequence	OS detect	OS detect

Powered COM Enable Switch

Set to the right(default)
Normal COM port (Pin9 = signal)

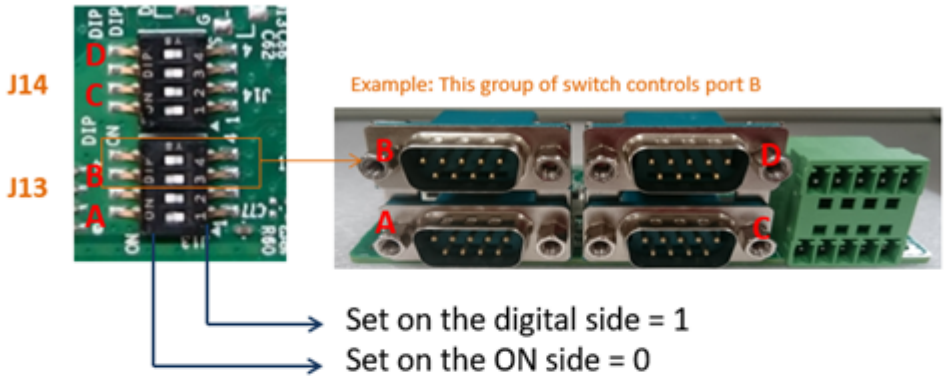
Set to the left
Powered COM port (Pin9 = VDD)

Powered COM Power Source Selection Switch



Set A-B; VDD = 12V (Default)
Set B-C; VDD = 5V

COM Mode Setting Switch

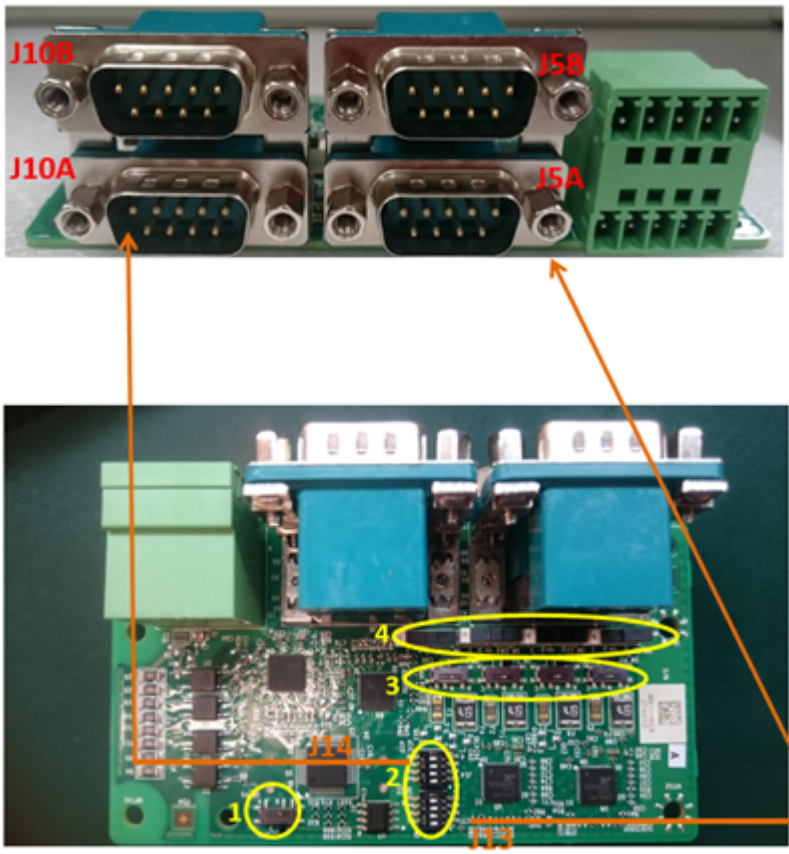


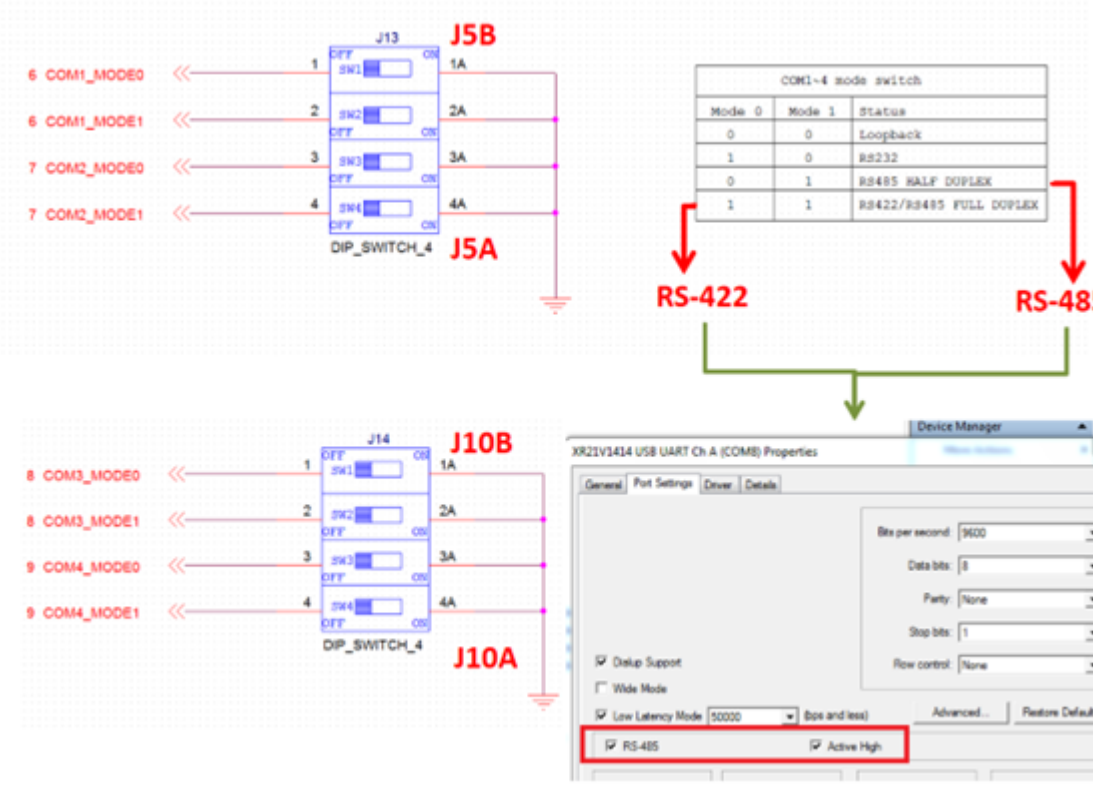
Set on the digital side = 1
Set on the ON side = 0

Switch	Bit	COM Port	Test Mode	RS485	RS232 (Default)	RS422
J14	4	Port D	0	1	0	1
	3		0	0	1	1
	2	Port C	0	1	0	1
	1		0	0	1	1

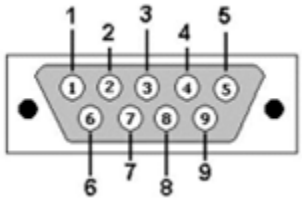
Switch	Bit	COM Port	Test Mode	RS485	RS232 (Default)	RS422
J13	4	Port B	0	1	0	1
	3		0	0	1	1
	2	Port A	0	1	0	1
	1		0	0	1	1

Driver Configuration Setting for RS485





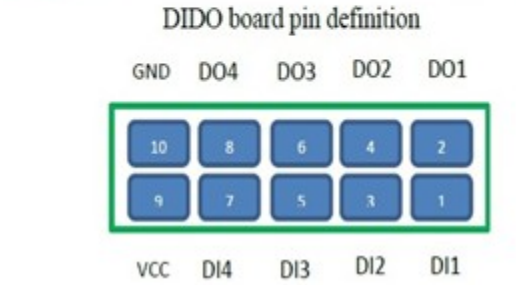
COM Port Pinout



Pin No	RS-232	RS-422	RS-485
1	DCD	TX-	DATA-
2	RX	TX+	DATA+
3	RTX	RX+	NC
4	DTR	RX-	NC
5	GND	GND	GND
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC

7.5.3 Digital IO Port

The **DIO/COM module** has a total **8-bit GPIO**, with the following positions:



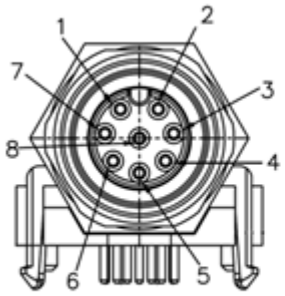
Left DIO Expansion / Right DIO Expansion

PIN	HW	Left DIO Order	Right DIO Order	Description
1	DI_1	21	11	Digital Input 1
2	DO_1	22	12	Digital Output 1
3	DI_2	23	13	Digital Input 2
4	DO_2	24	14	Digital Output 2
5	DI_3	25	15	Digital Input 3
6	DO_3	26	16	Digital Output 3
7	DI_4	27	17	Digital Input 4
8	DO_4	28	18	Digital Output 4
9	VCC	-	-	VCC
10	GND	-	-	Ground

7.5.4 Expansion Module PoE-LAN M12

This module is a Giga LAN module supporting **four M12-type interfaces**.
Combined with a power module, it supports **PoE (Type A)**.

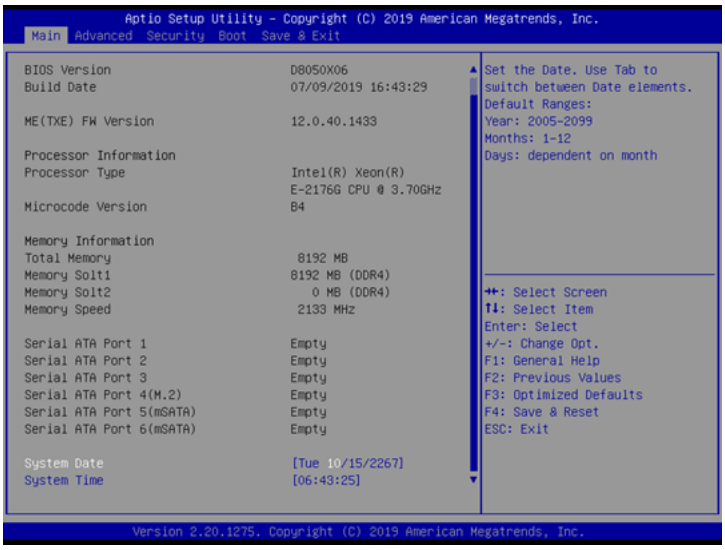
M12 Code A LAN Module Pin Definitions



PIN	Signal	POE typeA
1	LAN_MDI1+	DC+
2	LAN_MDI1-	DC+
3	LAN_MD20+	DC-
4	LAN_MDI2-	
5	LAN_MDI3+	
6	LAN_MDI3-	DC-
7	LAN_MDI4+	
8	LAN_MDI4-	

8 BIOS

8.1 Main Page



8.1.1 System Information

The **Main Page** displays essential system information, including BIOS version, build date, and hardware details. None of these fields are user-configurable.

- **BIOS Vendor:** AMI Megatrends
- **BIOS Version:** Displays the current BIOS version.
- **Build Date:** Shows the BIOS build date.
- **ME (TXE) Firmware Version:** Displays the Management Engine firmware version.
- **Processor Information:** Provides details about the installed CPU.
- **Total Memory:** Displays the installed RAM size.
- **Memory Frequency:** Shows the memory clock speed.
- **SATA Devices:** Lists installed storage devices connected via SATA, M.2, or mSATA.

8.1.2 System Date & Time Settings

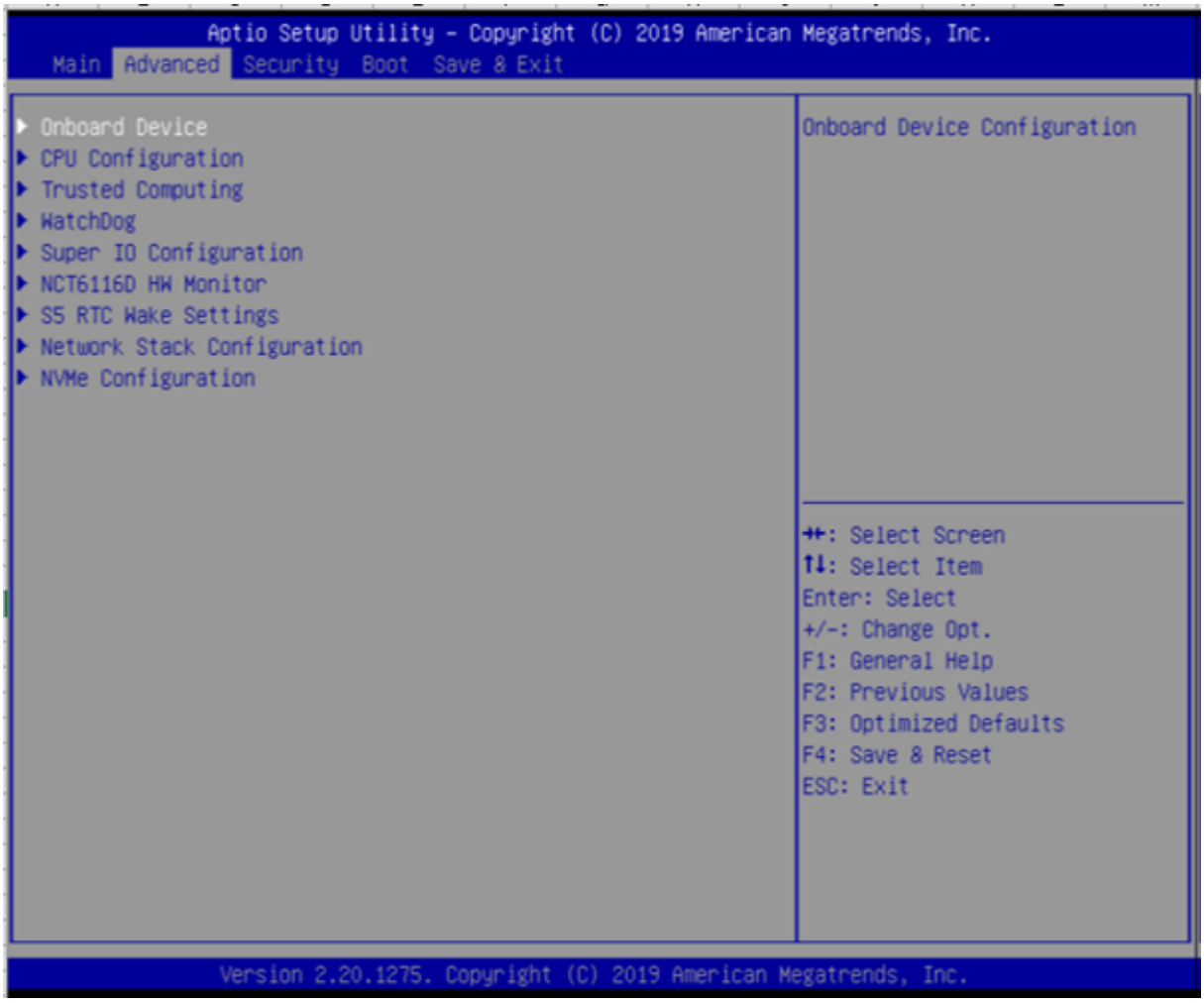
The **System Date & Time** settings allow you to configure the system's real-time clock.

- **System Date:** Set using the format `[Www mm/dd/yyyy]` where:
  - `Www`: Day of the week (Mon-Sun)
  - `mm`: Month (1-12)
  - `dd`: Day (1-31)
  - `yyyy`: Year (1998-9999)
- **System Time:** Set using the format `[hh:mm:ss]`, where:

- `hh`: Hours (0-23)
- `mm`: Minutes (0-59)
- `ss`: Seconds (0-59)

Use the **Tab** key to switch between date and time fields.

8.2 Advanced Page



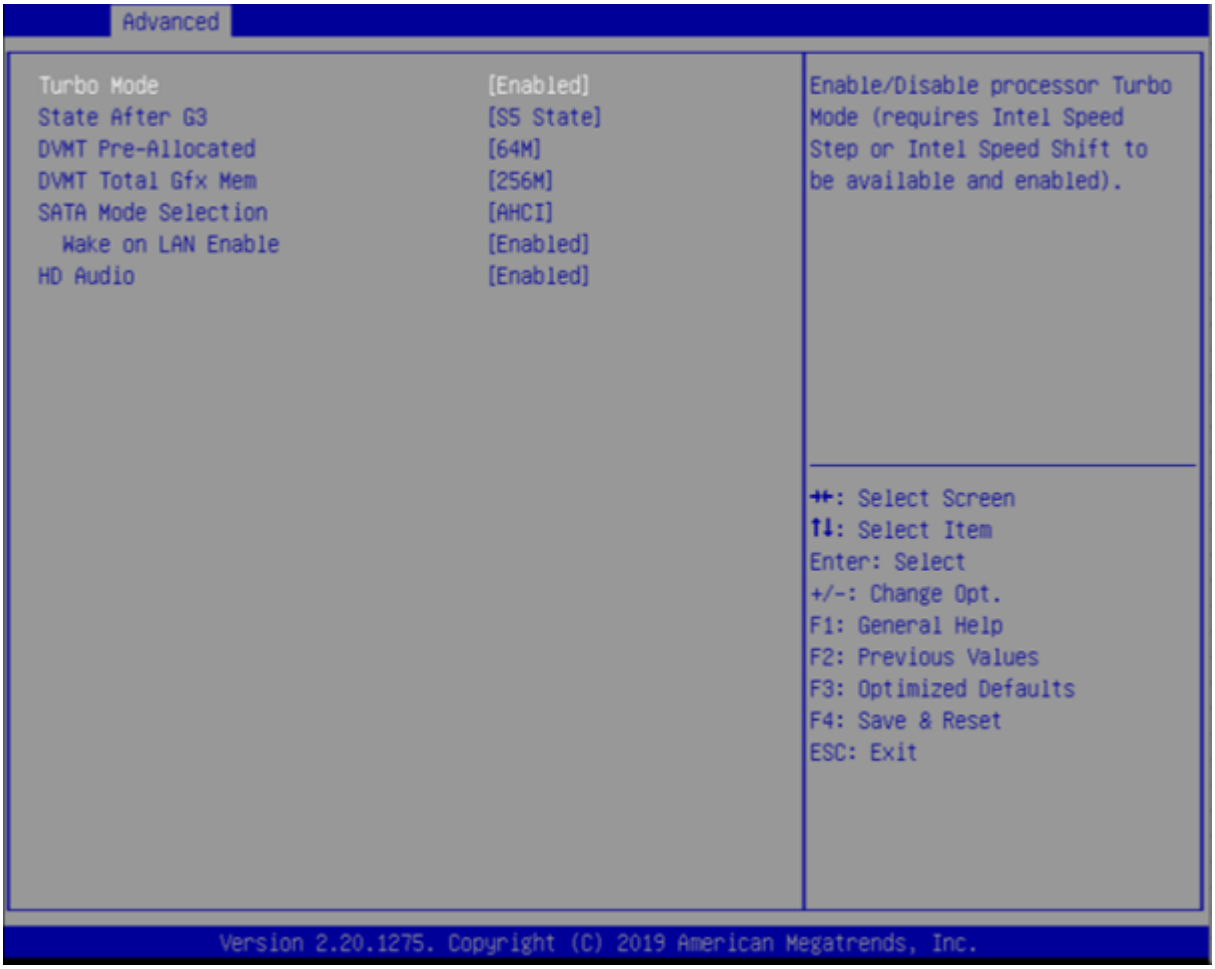
The **Advanced Page** contains various configuration options that allow users to fine-tune system behavior.

8.2.1 Advanced Configuration Options

- **Onboard Devices:** Configure integrated device settings.
- **CPU Configuration:** View and adjust processor settings.
- **Trusted Computing:** Manage TPM and security features.
- **WatchDog:** Enable or disable the WatchDog timer.
- **Super IO Configuration:** Configure settings for system I/O controllers.
- **NCT6116D HW Monitor:** Monitor system temperature, voltage, and fan speeds.
- **S5 RTC Wake Setting:** Enable system wake-up from S5 using an RTC alarm.

- **Network Stack Configuration:** Enable or disable UEFI network boot.
- **NVMe Configuration:** Configure settings for NVMe storage devices.

8.2.2 Onboard Devices Configuration



- **Turbo Mode:** Enable or disable the processor's Turbo Boost feature. Requires Intel Speed Step or Intel Speed Shift.
- **State After G3:** Determines system behavior after power loss (options include S0 and S5 states).
- **DVMT Pre-Allocated:** Set the amount of pre-allocated graphics memory for internal graphics.
- **DVMT Total Graphics Memory:** Choose the total memory allocation for integrated graphics.
- **SATA Mode Selection:** Defines how the SATA controller operates (AHCI or Intel RST Premium).
- **Wake on LAN:** Enable or disable system wake-up on network activity.
- **HD Audio:** Enable or disable high-definition audio detection.

8.3 CPU Configuration

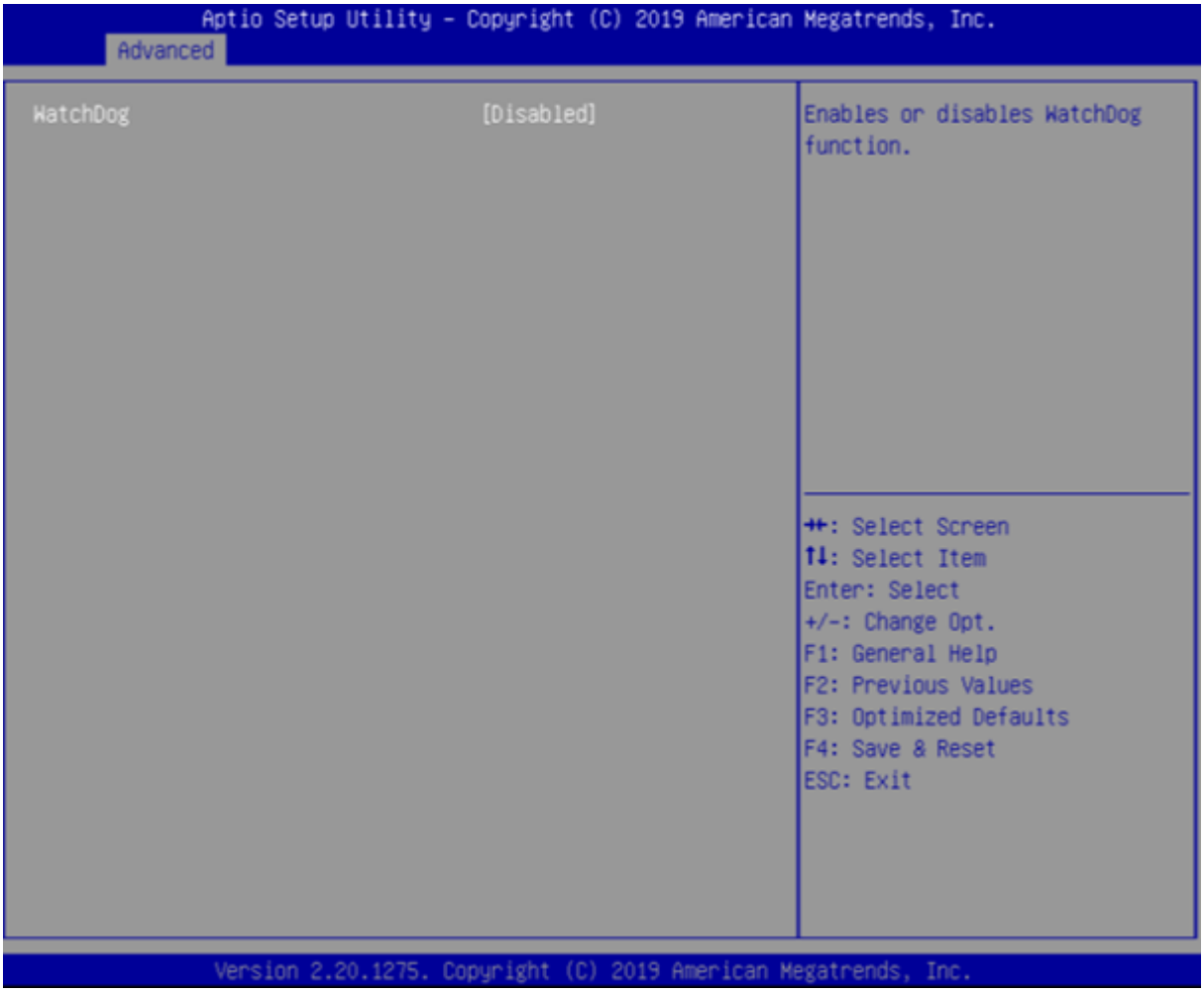
This section displays processor details and allows certain configurations:

- **Processor Type:** Displays the installed CPU model.
- **Processor ID:** Shows the CPU identification number.
- **Clock Speed:** Indicates the processor's base frequency.
- **Cache Levels:** Displays information about L1, L2, and L3 caches.
- **VMX Support:** Indicates whether Virtual Machine Extensions (VMX) are supported.
- **Intel Trusted Execution Technology:** Allows enabling or disabling of Intel's security extensions.

8.4 Trusted Computing

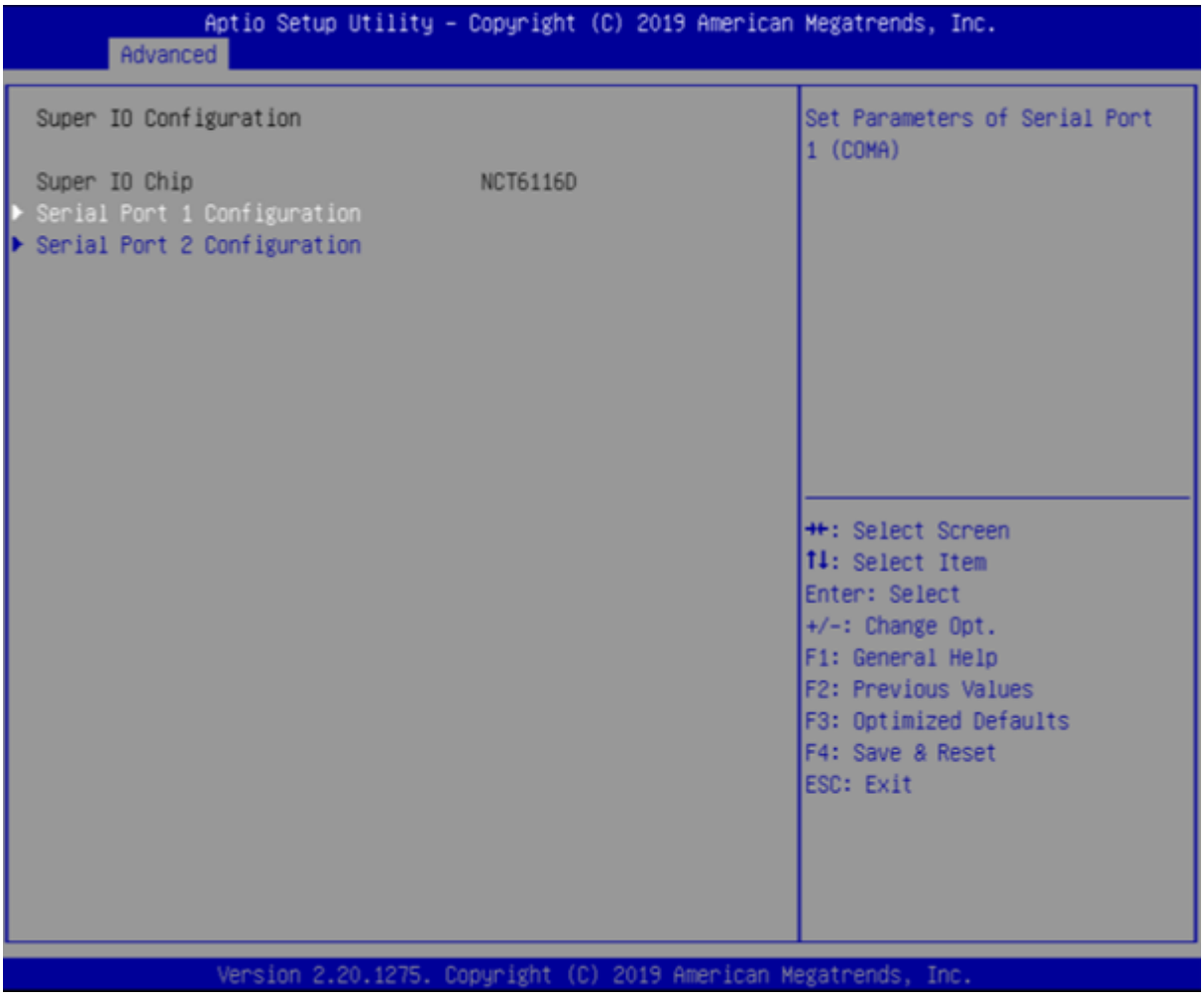
- **TPM 2.0 Device:** Displays the presence of a TPM security module.
- **Firmware Version:** Shows the TPM firmware version.
- **Vendor Information:** Displays the TPM manufacturer.
- **Security Device Support:** Enable or disable TPM functionality within the BIOS.

8.5 WatchDog Configuration



- **WatchDog Timer:** Enable or disable the WatchDog timer to automatically reset the system if it becomes unresponsive.

8.6 Super IO Configuration



- **Serial Port Configuration:** Configure RS232, RS485, and RS422 settings.
- **GPIO Settings:** Manage digital I/O configurations.

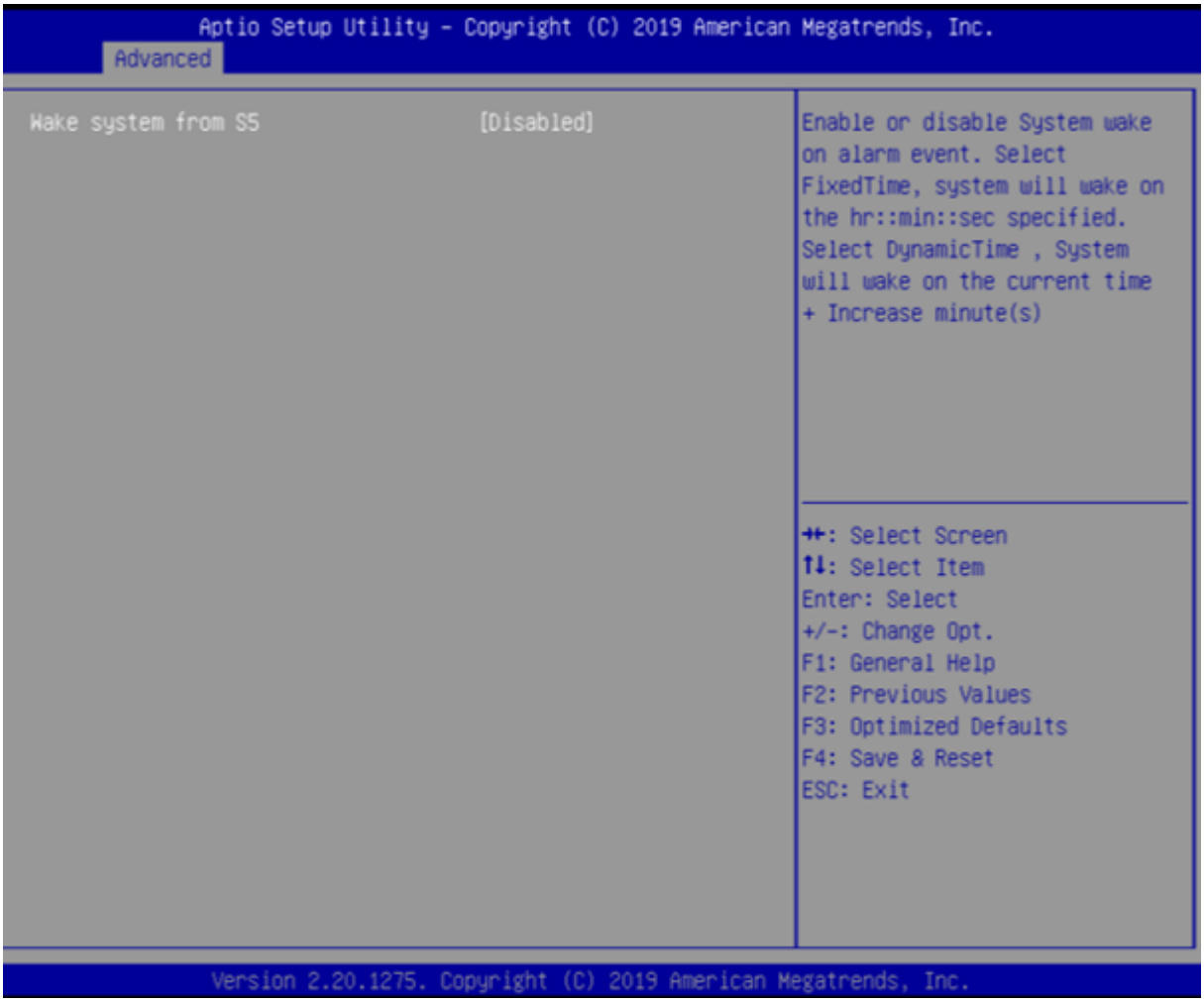
8.7 Hardware Monitoring

- **CPU Temperature:** Displays the current CPU temperature.
- **System Fan Speeds:** Monitors internal and external fan RPMs.
- **Voltage Readings:** Shows system voltage levels for various components.

8.8 RTC Wake Setting

- **Enable System Wake-Up from S5 Using RTC Alarm:** Allows setting a scheduled power-on time.

8.9 Network Stack Configuration

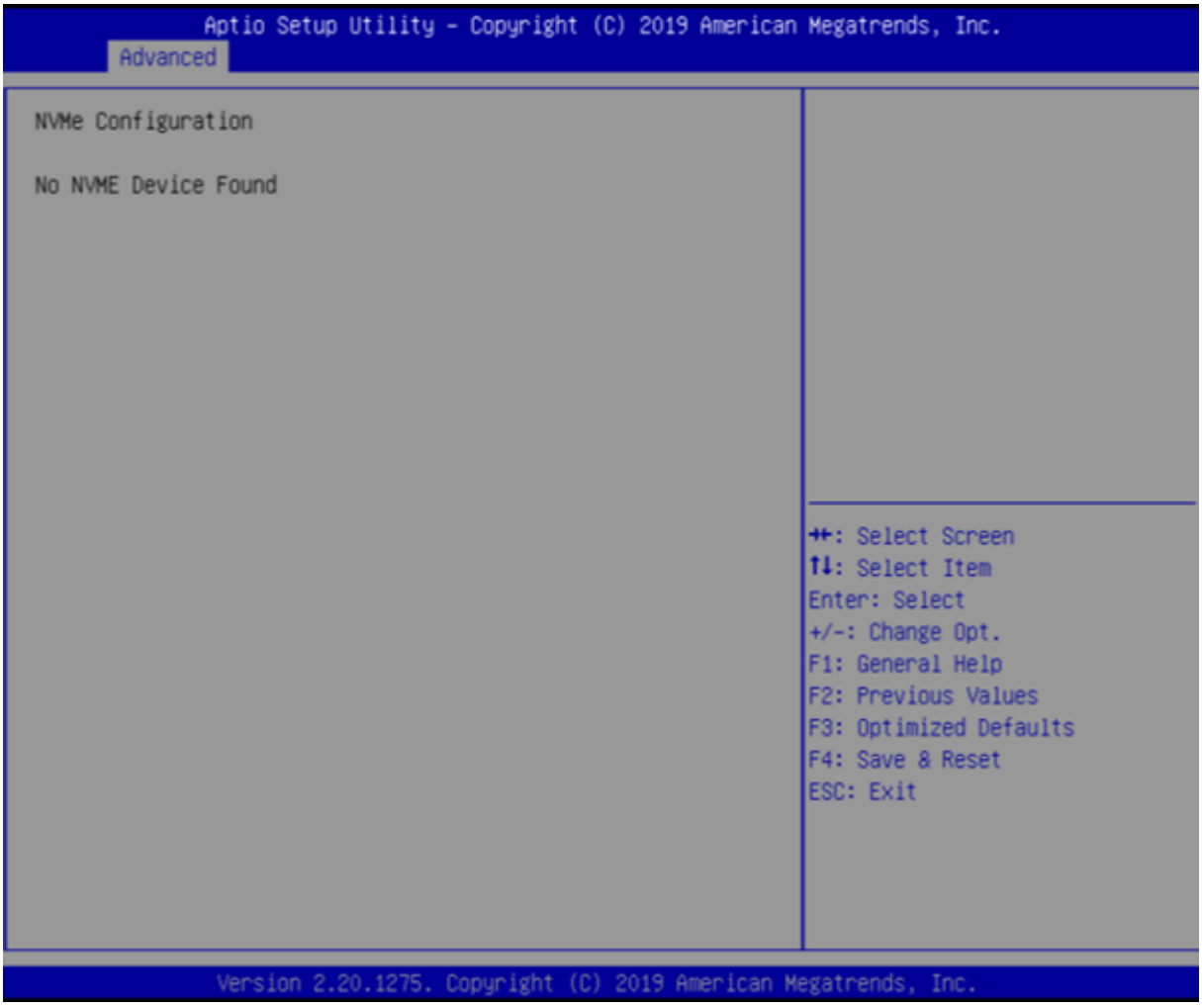


- **Enable UEFI Network Boot:** Toggle network boot functionality.

8.10 NVMe Configuration

- **Configure NVMe Storage Devices:** View and manage NVMe drives.

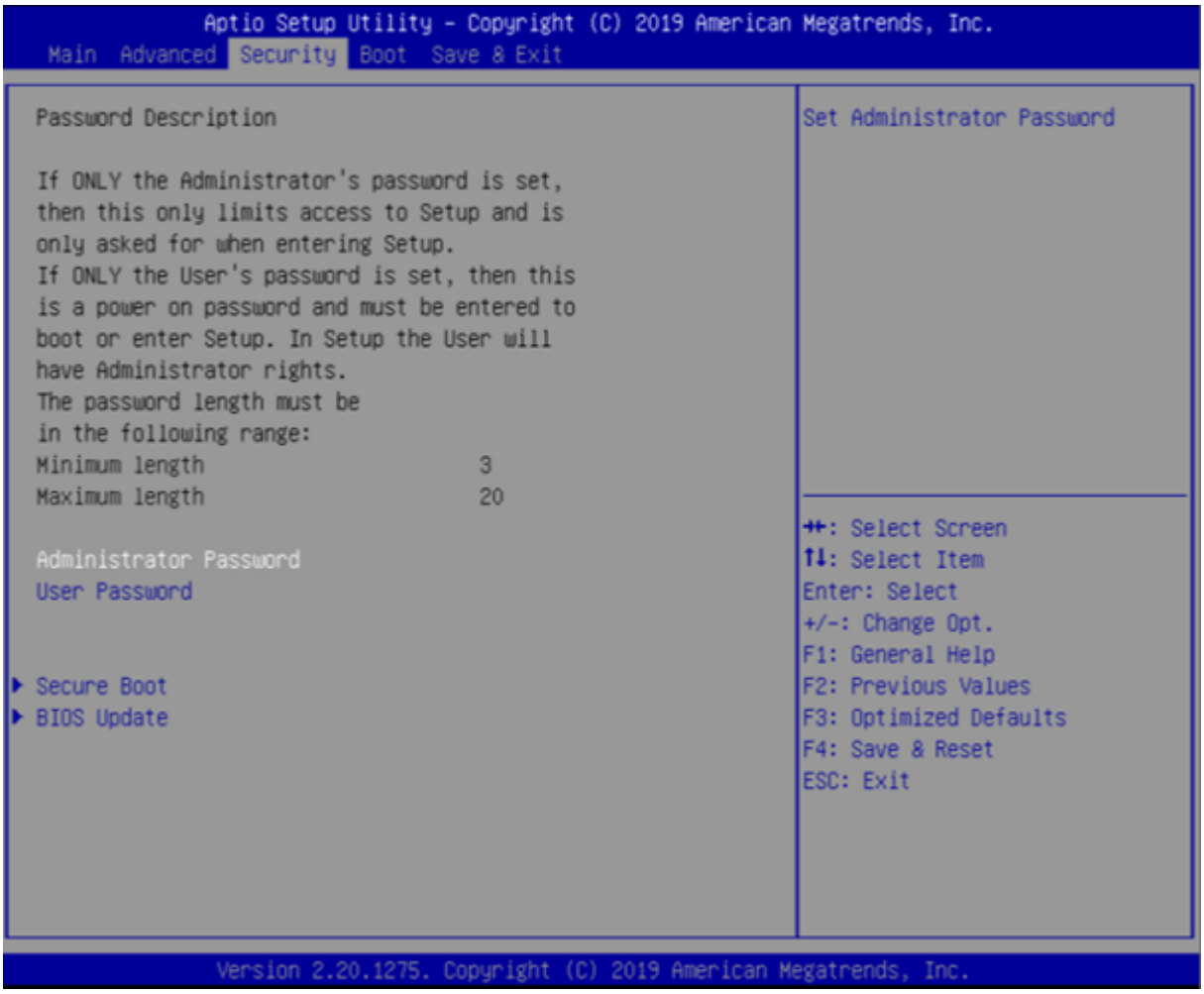
8.11 Security Page



The **Security Page** allows configuration of password protection and security features:

- **Administrator Password:** Set or modify the administrator password.
- **User Password:** Set or modify the user password.
- **Secure Boot:** Enable or disable Secure Boot to enforce signed OS loaders.

8.11.1 Secure Boot Configuration

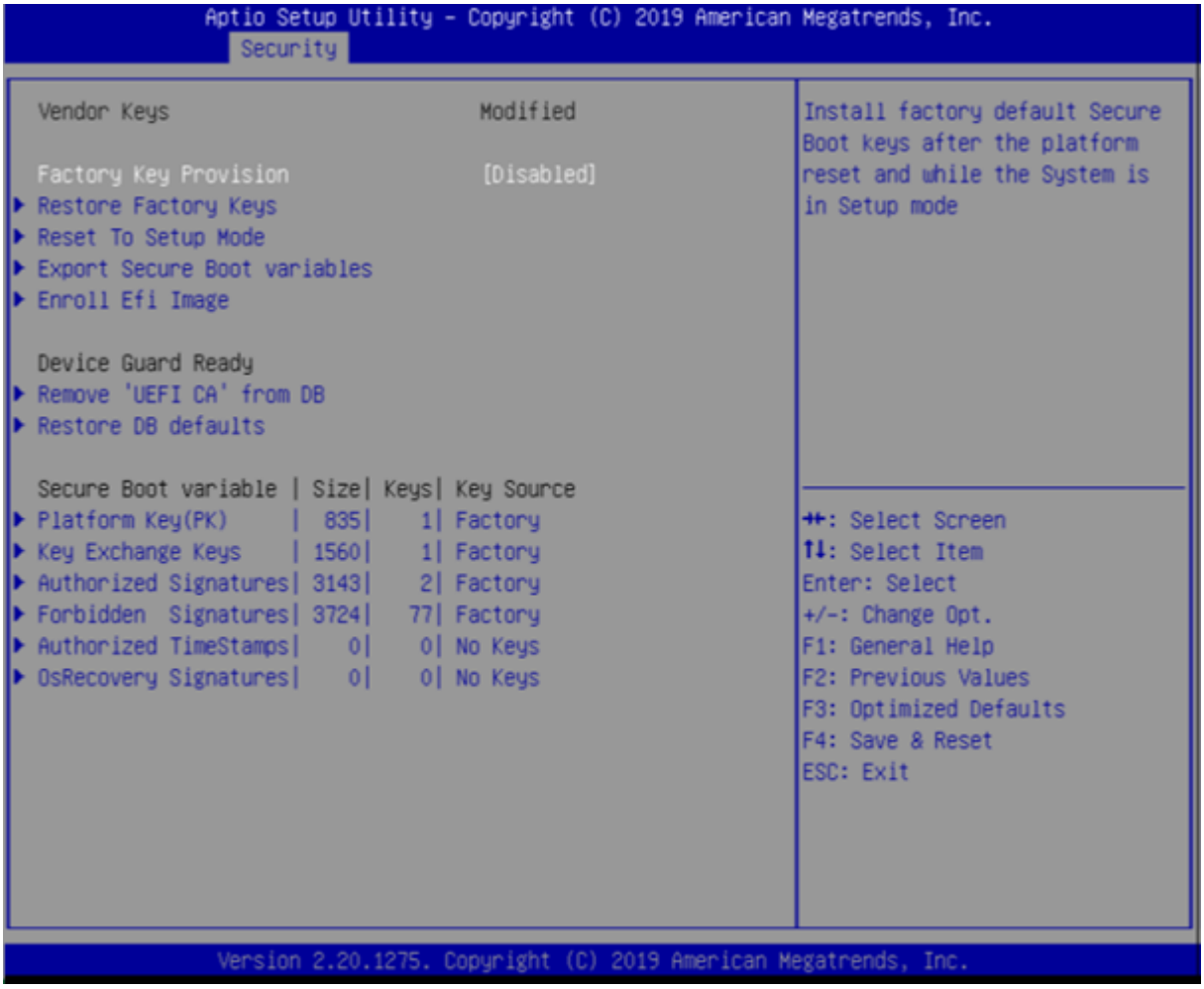


- **Secure Boot Mode:** Choose between Standard and Custom configurations.
- **Restore Factory Keys:** Reset Secure Boot keys to default factory settings.

8.12 Boot Page

- **Setup Prompt Timeout:** Set the time (in seconds) for the BIOS prompt to appear before boot.
- **Boot Order Configuration:** Define the sequence of boot devices.

8.13 Save & Exit



- **Save Changes and Reset:** Apply changes and restart the system.
- **Discard Changes and Reset:** Restart without saving any modifications.
- **Load Optimized Defaults:** Restore factory default settings for all BIOS configurations.

9 System Setup

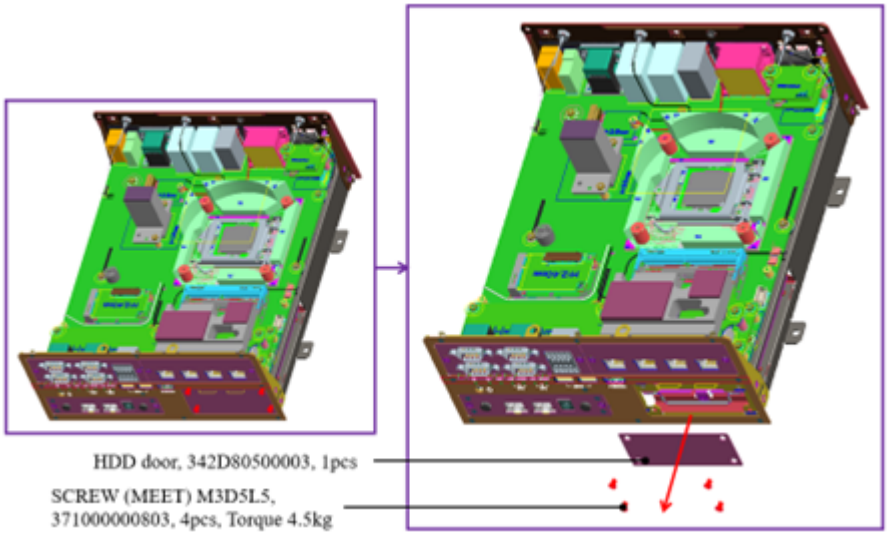
This chapter provides guidance on setting up the **Alderamin MK5 Embedded System** hardware.

Warning: The edges of the ALDERAMIN MK5 aluminum extrusion fins are sharp. Handle the unit carefully during installation, movement, and operation.

9.1 1st 2.5” SATA HDD/SSD Installation

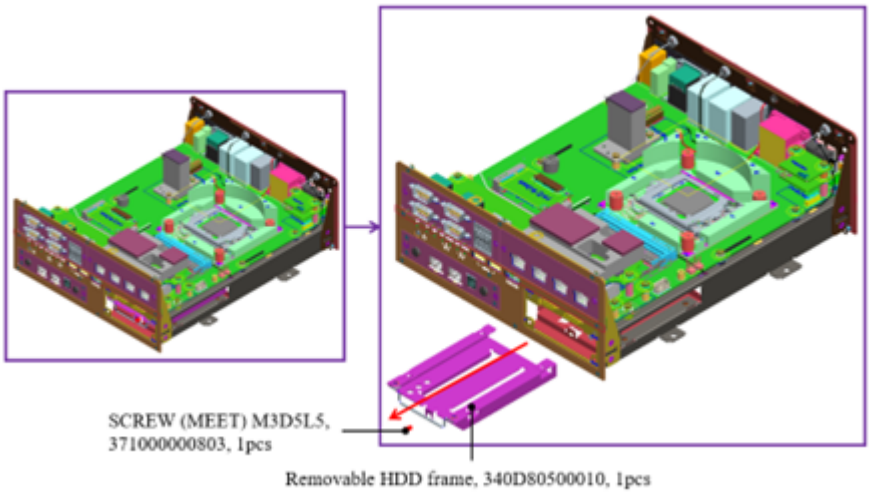
Follow these steps to install a SATA HDD:

- Remove the door from the front bezel.

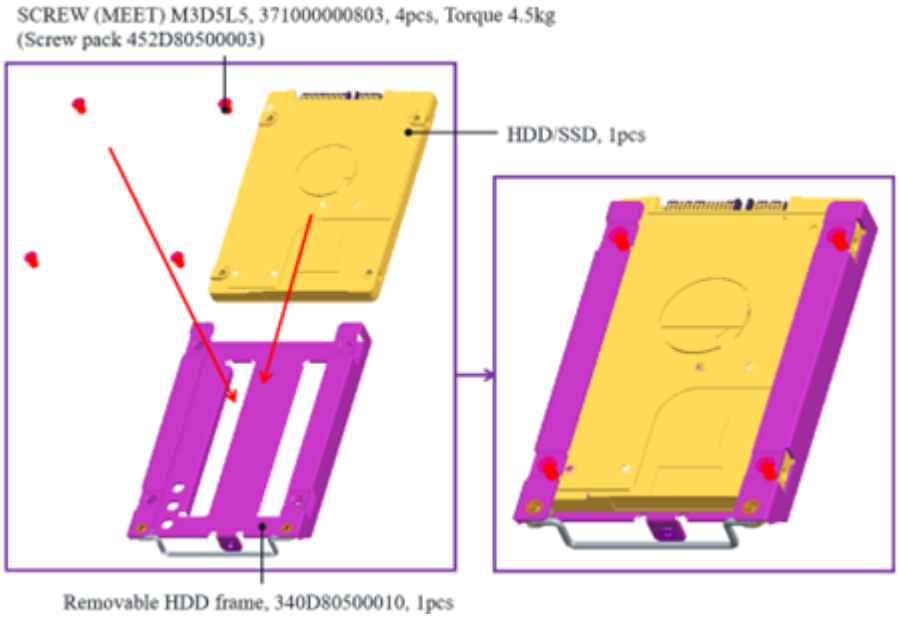


Note: Loosen the four screws from the expansion door, then gently lift the cover with your fingernail to carefully remove it.

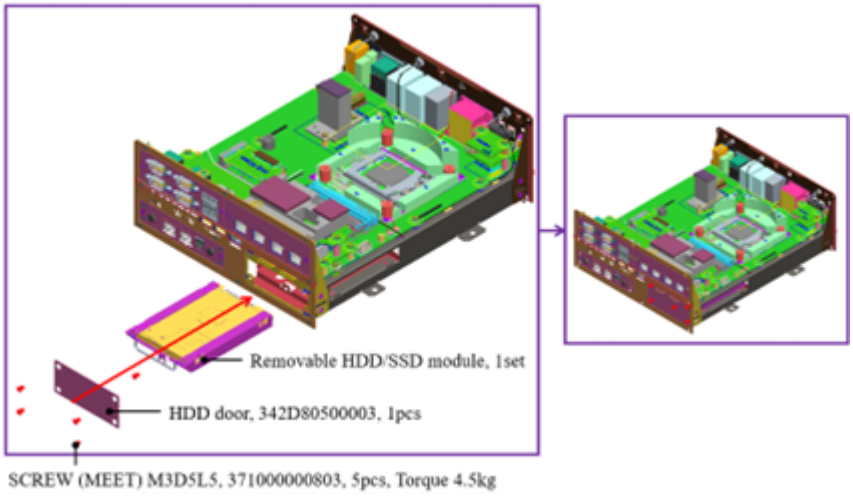
- Pull the HDD tray out from the main chassis.



- Secure the HDD/SSD to the bracket using screws.



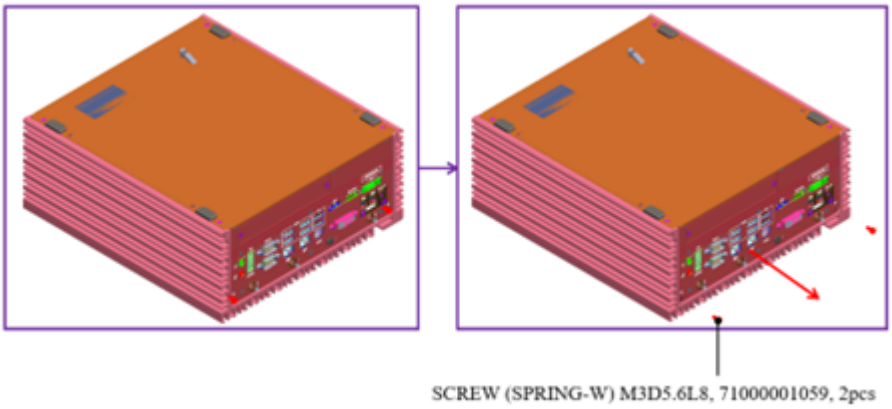
- Insert the HDD/SSD tray back into the main chassis and fasten the screws on the door.



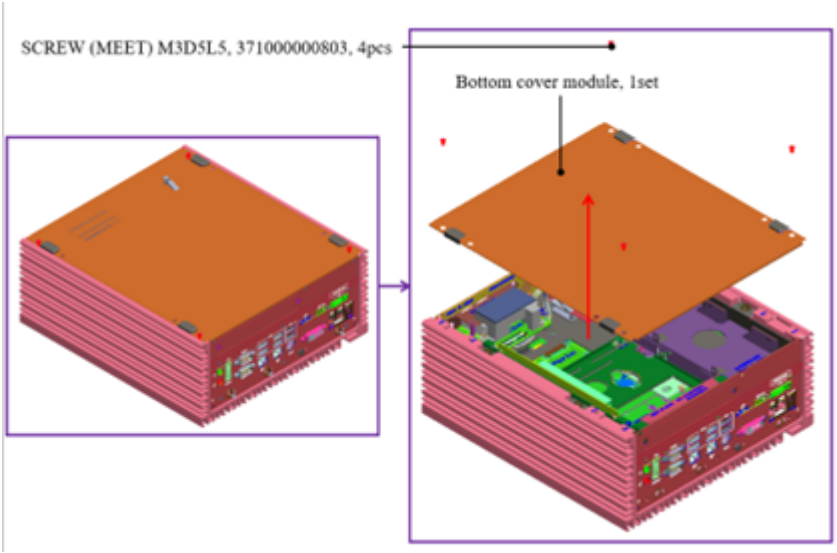
Note: Keep the unit horizontal to facilitate smooth reinsertion of the HDD tray.

9.2 2nd and 3rd 2.5” SATA HDD/SSD Installation

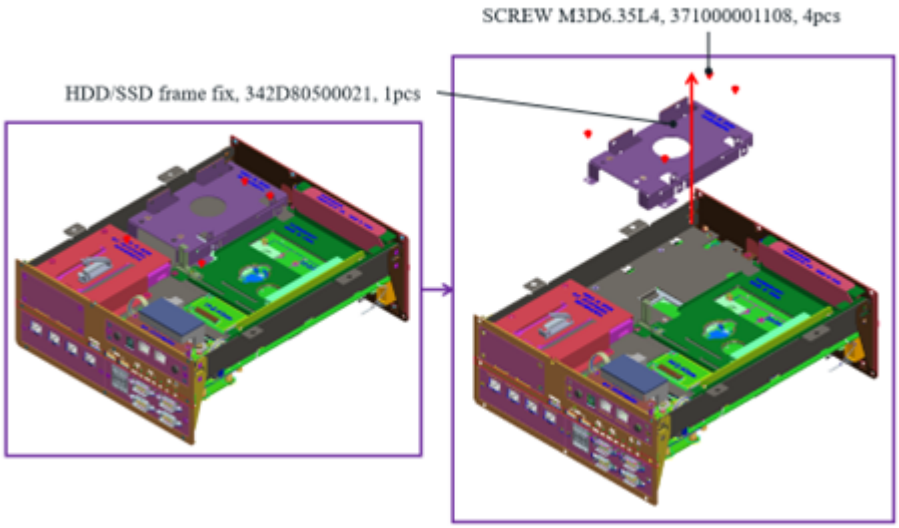
- Remove the **GND screws** from the rear bezel.



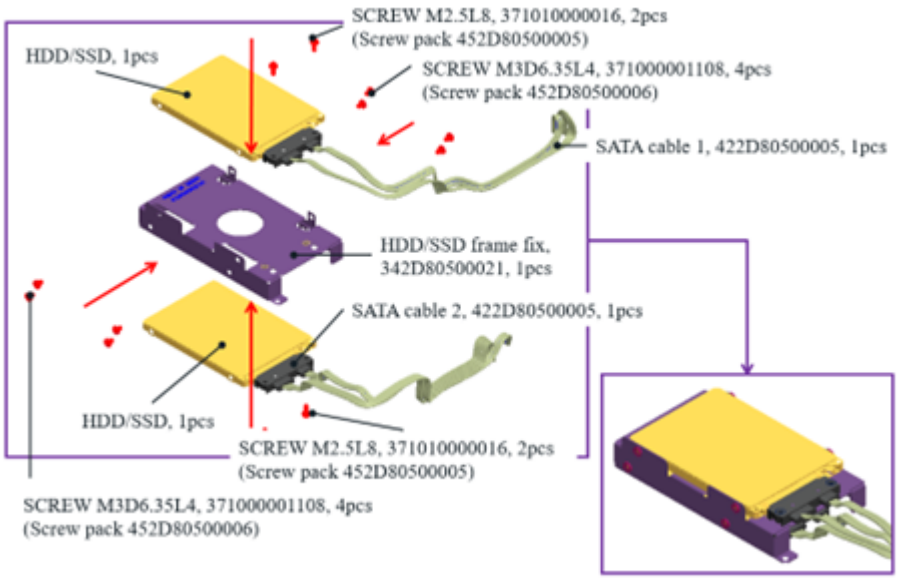
- Remove the **bottom cover**.



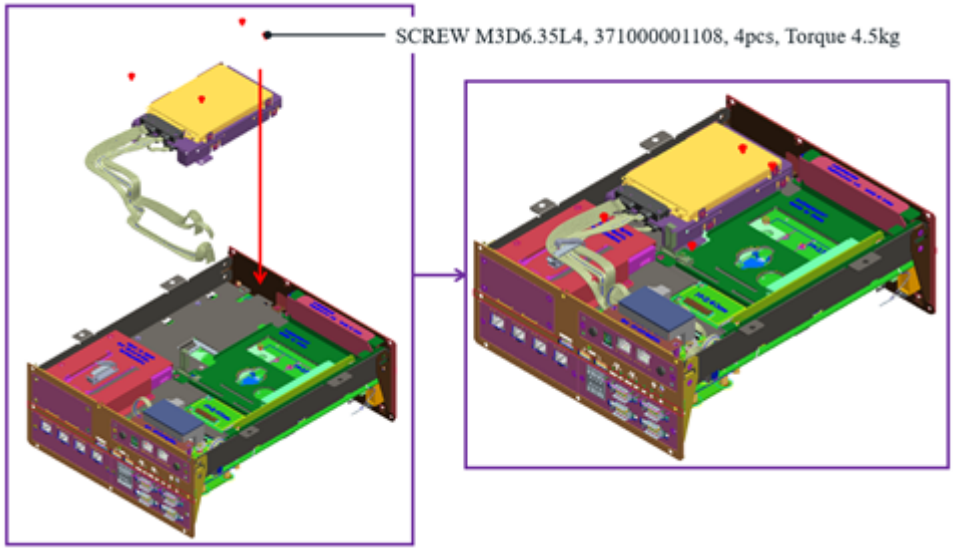
- Loosen the four **HDD bracket screws** and pull the bracket out of the unit.



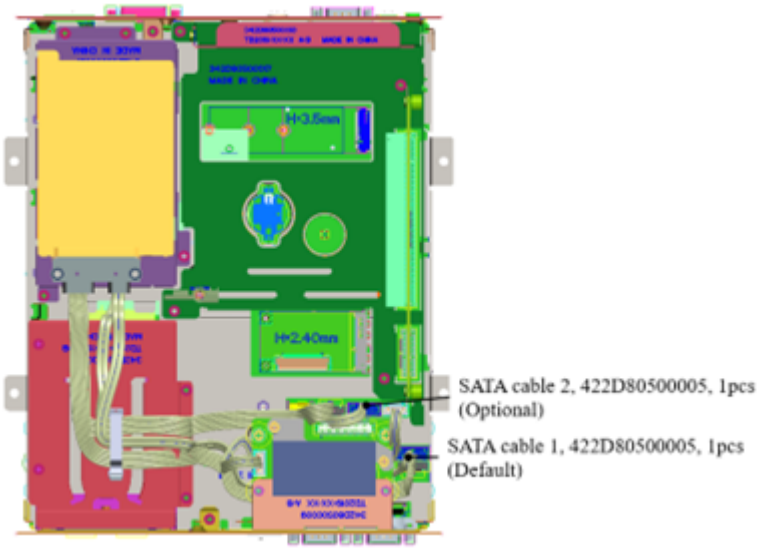
- Secure the **2nd and 3rd HDD/SSD** to the bracket as illustrated in the concept drawing.



- Fasten the **four bracket screws** to the main unit.

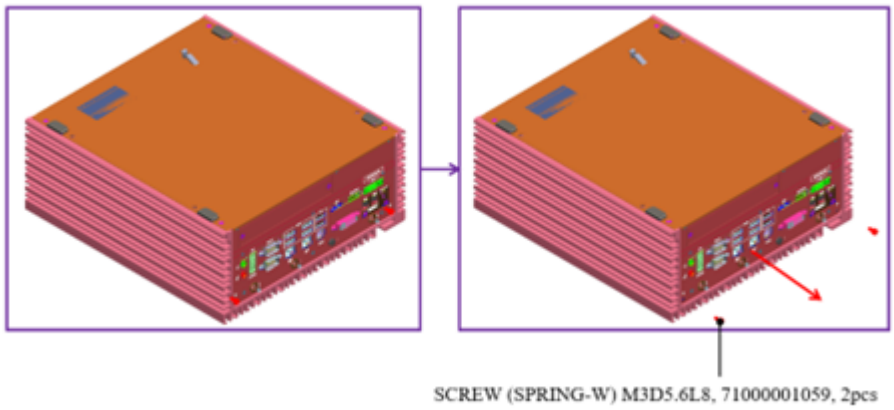


- Follow the guide for proper **SATA cable routing**.

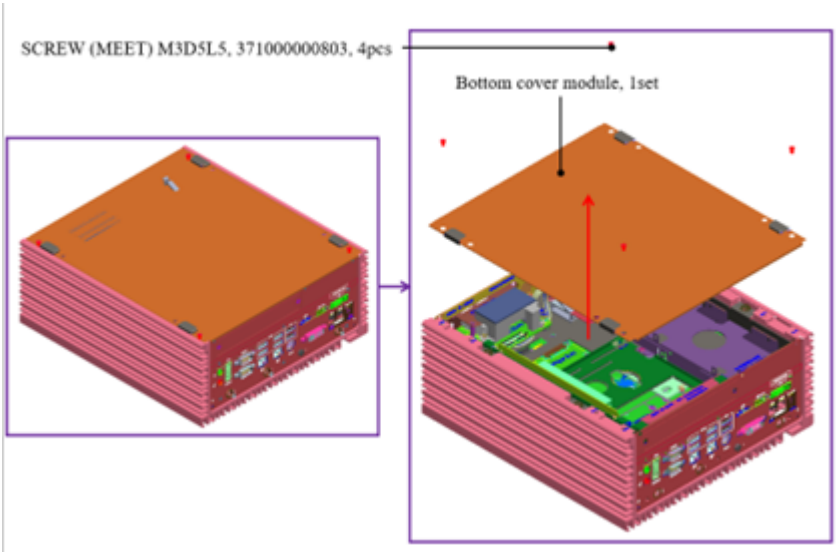


9.3 CPU, CPU Heatsink, and DRAM Installation

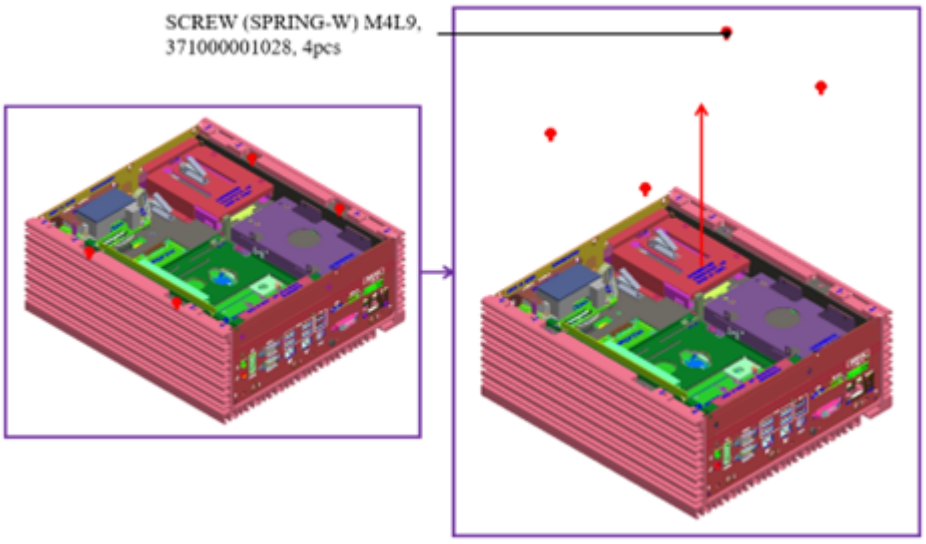
- Remove the **GND screws** from the rear bezel.



- Remove the **bottom cover**.

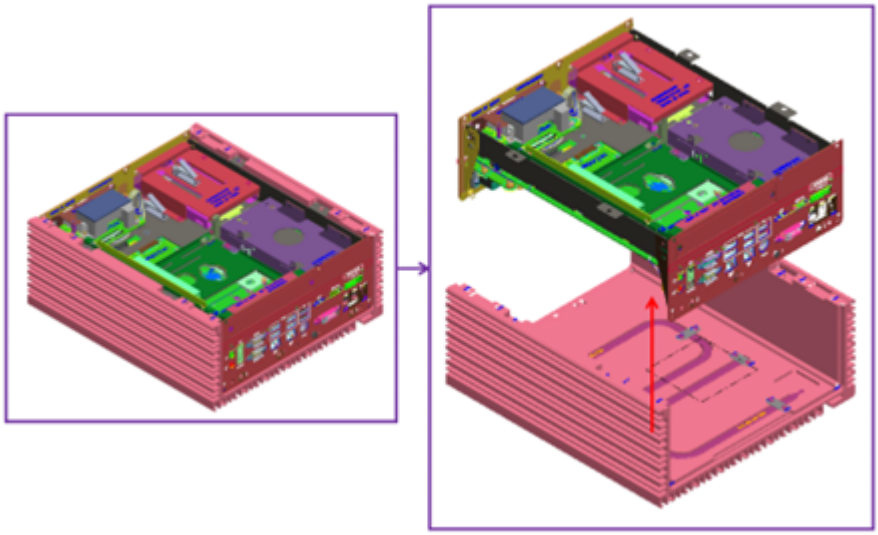


- Loosen the **four M4 screws** from the main chassis.

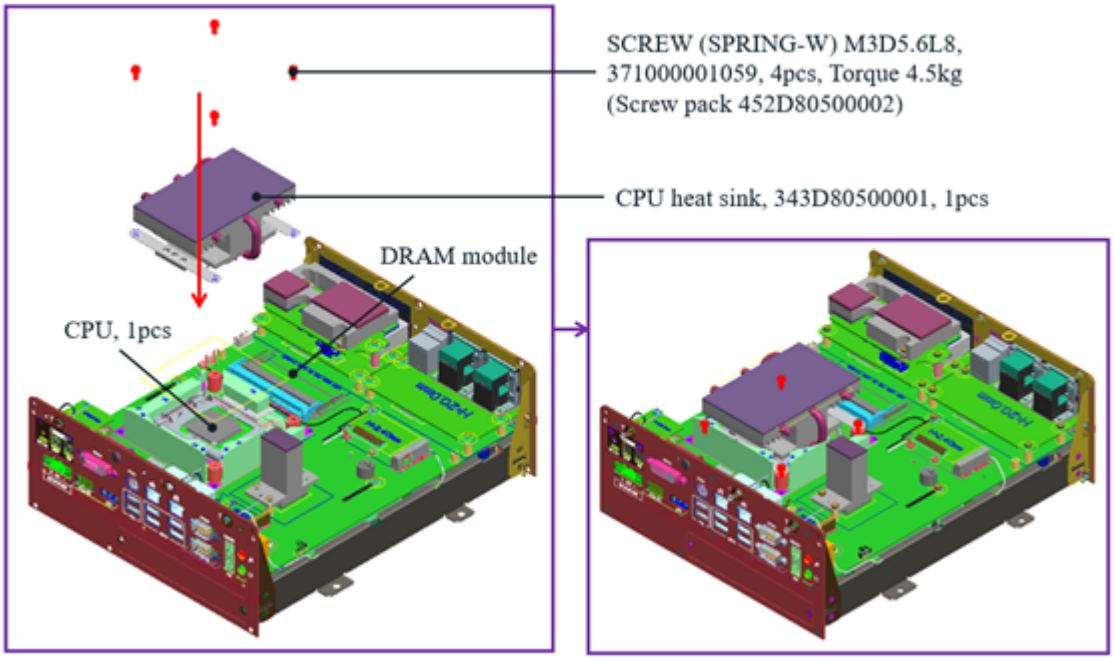


- Ensure the **two GND screws** are loosened, then carefully pull the **main chassis** from the aluminum extrusion.
  - The aluminum extrusion has **chipset thermal pads (L6)** and **two guide pins**, so some force may be required.

  Warning: The aluminum and metal edges are sharp—handle with extreme caution when pulling the main chassis out.

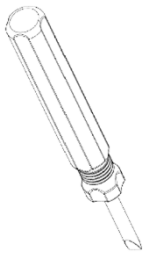


- Take the **CPU passive cooler** from the accessories and install the **CPU, CPU heatsink, and DRAM modules** as shown.



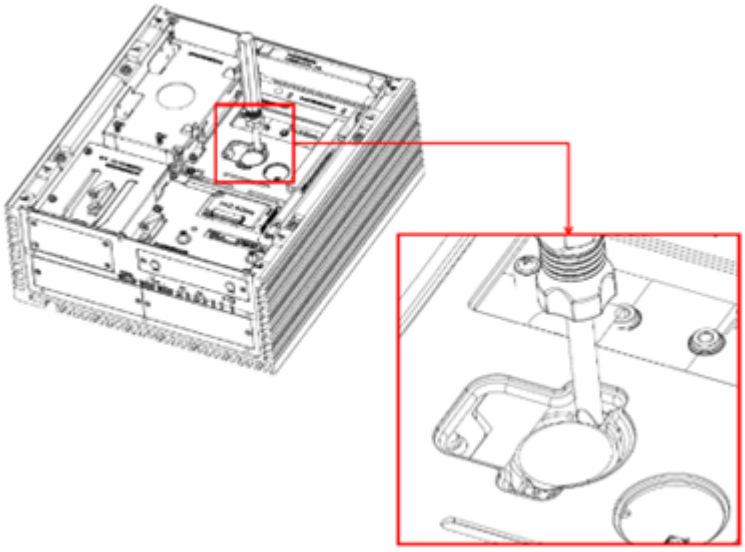
9.4 RTC Battery Maintenance

9.4.1 Preparation for Disassembly



Flathead Screwdriver *(Required for battery removal due to high vibration resistance design)*

- Insert the **flathead screwdriver** into the gap on one side of the **RTC battery** vertically.



- Rotate the screwdriver about **45 degrees** to loosen and remove the coin battery.