WINSYSTEMS®

COMeT10-3900

COM Express® Type 10 mini Module with Intel® Atom™ E3900 processor, Ethernet, Multi-Display, and MIPI-CSI

Product Manual

WinSystems, Inc. | 2890 112th Street, Grand Prairie, TX 75050 | 817-274-7553 | info@winsystems.com | www.winsystems.com

Revision History

Document Version	Last Updated Date	Brief Description of Change
v1.0	10/2020	Initial release
v1.1	7/29/2025	Updated Conformal Coating, added Warranty link, updated all links

Copyright and Trademarks

Trademark Acknowledgments

Table of Contents

1. Before You Begin

Review the warnings in this section and the best practice recommendations (see “Best Practices” on page 29) when using and handling the WINSYSTEMS COMeT10-3900 module. Following these recommendations provides an optimal user experience and prevents damage. Read through this document and become familiar with the COMeT10-3900 before proceeding.

APPLYING CONFORMAL COATING AFTER PURCHASE WILL VOID YOUR WARRANTY. FAILING TO COMPLY WITH THESE BEST PRACTICES MAY DAMAGE THE PRODUCT AND VOID YOUR WARRANTY.

1.1 Warnings

Only qualified personnel should configure and install the COMeT10-3900. While observing best practices, pay particular attention to the following:.

Avoid Electrostatic Discharge (ESD)
Only handle the circuit board and other bare electronics when electrostatic discharge (ESD) protection is in place. Having a wrist strap and a fully grounded workstation is the minimum ESD protection required before the ESD seal on the product bag is broken.

2. Introduction

This manual provides configuration and usage information for the COMeT10-3900. If you still have questions, contact Technical Support at +1-817-274-7553, Monday through Friday, between 8 AM and 5 PM Central Standard Time (CST).

Refer to the WINSYSTEMS website at https://www.winsystems.com/product/comet10-3900/ for other accessories (including cable drawings and pinouts) that can be used with your COMeT10-3900.

3. Functionality

The COMeT10-3900 is an industrial COM Express®, Type 10 mini module with an Intel® Atom™ E3900 processor. This low power, industrial module is designed and manufactured in the USA. The small form factor module is designed as a processor mezzanine that can be plugged onto a carrier board that contains user specific I/O requirements.

COM Express modules allow users to retain the same carrier board design across scalable CPU series and over multiple generations of COM Express modules providing a long project lifetime. Updating a COM Express module to improve performance or replace an end of life processor

drastically improves time to market when revising existing projects. Users have the option to choose the default BIOS settings and layout, or request a custom branded configurable BIOS to support specific project requirements.

The COMeT10-3900 supports Linux, Windows® 10, and other x86-compatible real-time operating systems. Drivers are available from the WINSYSTEMS website at https://www.winsystems.com/product/comet10-3900/.

4. Features

The COMeT10-3900 provides the following features.

COM Express mini Type10 Module

- Multi-core Intel Atom E3900 processors
  - X5 E3930 dual core, up to 1.8 GHz (base frequency 1.3 GHz)
  - X5 E3940 quad core, up to 1.8 GHz (base frequency 1.6 GHz)
  - X7 E3950 quad core, up to 2.0 GHz (base frequency 1.6 GHz)

Operating Systems (compatibility)

- Windows 10 x64, IoT Enterprise, IoT Core, and Professional
- Linux x64
- Most PC architecture operating systems, including real time options

Memory

- Up to 8 GB soldered down LPDDR4

BIOS

- AMI UEFI-compliant BIOS in SPI flash device

Video Interfaces (supports two simultaneous displays)

- 1x Digital Display Interface (DisplayPort, HDMI, DVI)
- 1x eDP or 1x single-channel, low-voltage differential signaling (LVDS)

Ethernet

- 1x Intel 10/100/1000 Mbps controller using Intel i210
- Wake-on-LAN support

Storage

- On-board eMMC 5.x solid state disk

Data Acquisition

- 4x General Purpose Inputs (GPI)
- 4x General Purpose Outputs (GPO)

COM Express Type 10 mini Expansion

- 4x PCIe lanes configurable as 4x1, 2x1 + 1x2, or 1x4
- 2x USB 3.2 Gen 1, 6x USB 2.0
- 1x i210 1Gb/s Ethernet RGMII with IEEE 1588 support
- HD Audio
- 2x SATA III (6 Gb/s)
- 2x UART
- 4x GPI, 4x GPO (SDIO option for MicroSD socket)

Power

- Supports a wide range DC input power: 4.75V to 20V

Industrial Operating Temperature

- -40 to +85°C (-40 to +185°F)[1]

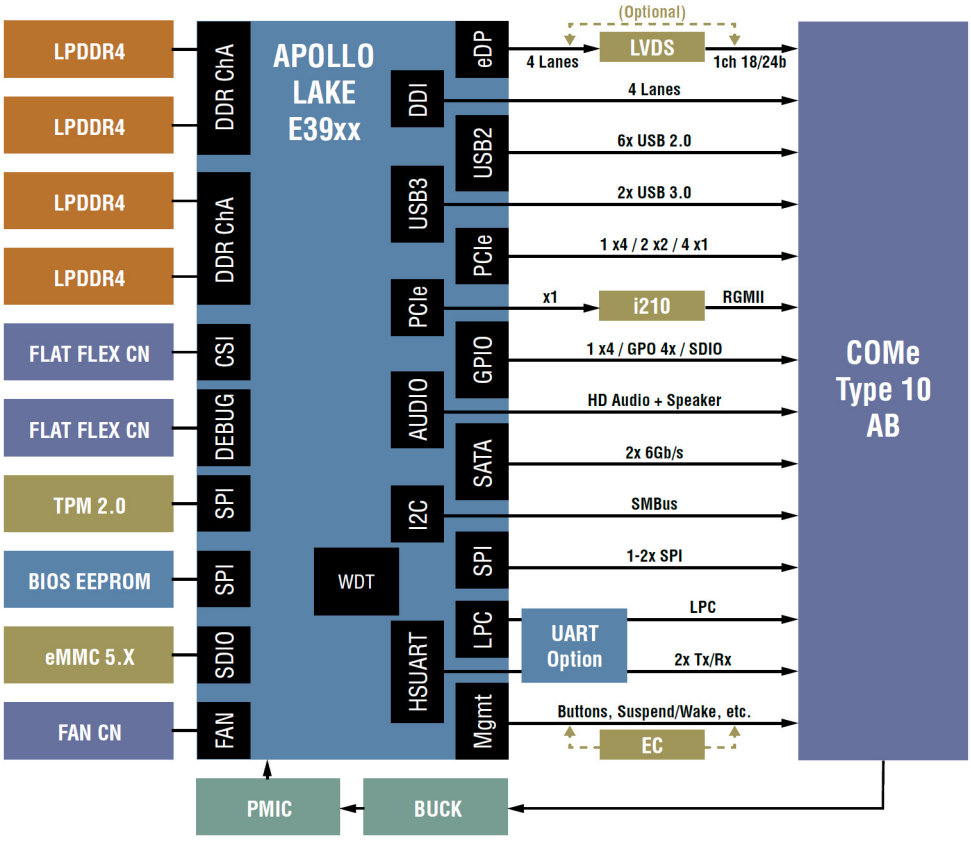
Additional Features

- On-board Discrete TPM 2.0 Hardware Security
- Custom configurable UEFI based AMI BIOS
- System Management Libraries and Tools
- EAPI v1.1 support for System Info, WDT, I2C, Brightness, GPIO, and User Storage Area

1. Requires thermal solution via heat spreader/heat sink and/or airflow.

5. General Operation

5.1 System Block Diagram



6. Specifications

The COMeT10-3900 adheres to the following specifications and requirements.

Table 1: COMeT10-3900 specifications

Feature	Specification
Electrical	
V_{CC}	Supports a wide range DC input power: 4.75V to 20V
Models	**COMET10-CCCC-REEEVUI** -3950- **CCCC** = CPU (3930, 3940, 3950) 8 **R** = RAM SIZE (4, 8) 128 **EEE** = EMMC SIZE (64, 128) E **V** = Video Option (E = eDP, L = LVDS) L **U** = UART Option (A = HSUART, L = Legacy UART)

Table 1: COMeT10-3900 specifications (Continued)

Feature	Specification
Processor	E3930 x5 dual core up to 1.8 GHz E3940 x5 quad core up to 1.8 GHz E3950 x7 quad core up to 2.0 GHz
Mechanical	
Dimensions	3.31 in x 2.17 in (84 mm x 55 mm)
Weight	1.6 oz. (45 g), without heat sink
PCB thickness	0.078 in. (2.00 mm)
Environmental	
Temperature	-40 to +85°C (-40 to +185°F)[a]
Humidity (RH)	5% to 95% non-condensing
RoHS compliant	Yes
Operating Systems	
Runs 64-bit Windows, Linux, and other x86-64-compatible operating systems.	

a. Requires thermal solution via heat spreader/heat sink and/or airflow. The maximum measurable temperature on any spot of the heat spreader or heat sink, and module surfaces must not exceed the operating temperature specified in the table above.

7. Configuration

This section describes the COMeT10-3900 components and configuration.

7.1 Component Layout

7.1.1 Top/Bottom Views

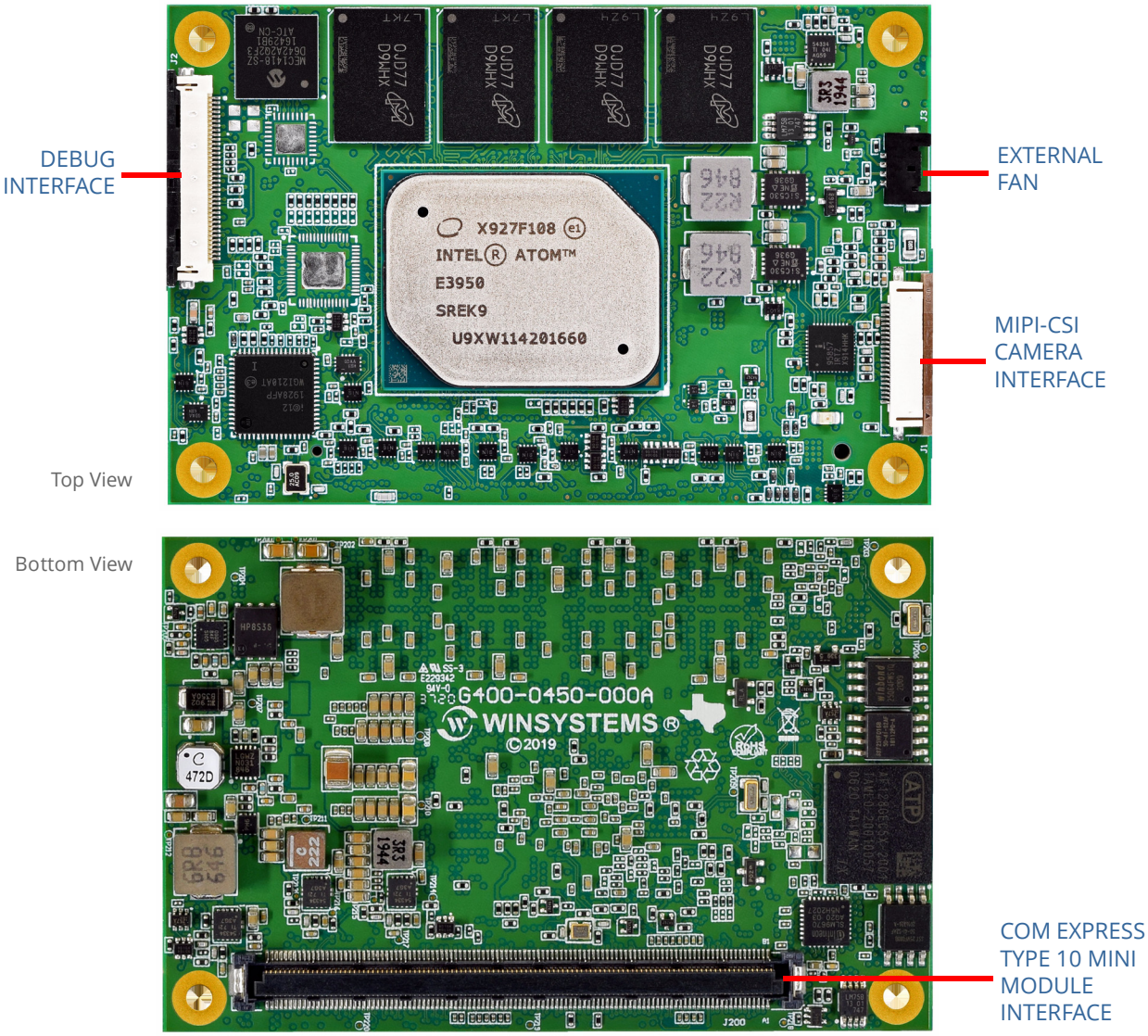


Table 2: Top/bottom view components

Item	Description	Reference
J1	MIPI-CSI Camera Interface Connector	page 15
J2	Debug Interface Connector	page 16
J3	External Fan Connector	page 16
J200	COM Express Type 10 mini Module Interface Connector	page 18

7.2 Watchdog Timer (WDT)

7.2.1 WDT Register Usage

The Watchdog Timer (WDT) implemented in the COMeT10-3900 board's embedded controller (EC) can be used to reset the system if a lock-up prevents a software task from periodically resetting the watchdog timer. The WDT is controlled through a set of virtual registers that are exposed to Apollo Lake applications by the EC on the COMeT10-3900 board. The WDT can be programmed to count in either seconds or minutes; it has a minimum granularity of 1 second, and a maximum granularity of 255 minutes.

7.3 Real-time Clock/Calendar

A real-time clock is used as the AT-compatible clock/calendar. It supports a number of features including periodic and alarm interrupt capabilities. In addition to the time and date-keeping functions, the system configuration is kept in CMOS RAM contained within the clock section. A battery must be enabled for the real-time clock to retain time and date during a power down.

7.4 System Management Software

The system management software for the COMeT10-3900 board consists of a set of library functions and example applications that demonstrate the functionality of the system management software. The software is available for both Windows 10 and Ubuntu Linux.

The system management software is custom software designed to use the built-in functionality of the COMeT10-3900 board's embedded controller (MicroChip MEC1418) to perform system management tasks such as reporting of board voltages (3.3V, 5V, 12V, V_{ddq}, V_{core}, V_{bat}, and the pair of user ADC inputs), the control of the system fan, reporting of the ambient temperature and setting of temperature sensor thresholds. Additional functionality allows applications to determine the version of the EC firmware, report the boot image used when the system started, and allow the EC to update its own firmware image. The EC contains a pair of identical images for redundancy and rolls over to a correct image if the first image is compromised.

7.5 Configuration and Installation

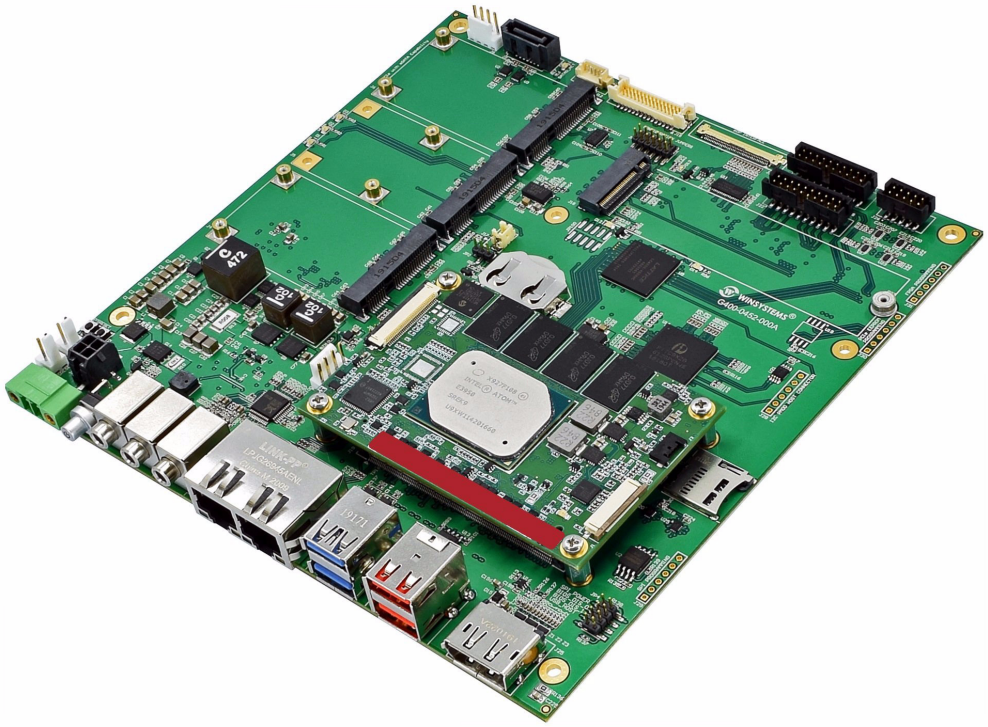
When installing the COMeT10-3900 onto a compatible COM Express Type 10 carrier board, please follow the instructions below to ensure there is no damage to the COMeT10-3900 or the carrier board.

Avoid Electrostatic Discharge (ESD)
Only handle the circuit board and other bare electronics when electrostatic discharge (ESD) protection is in place. Having a wrist strap and a fully grounded workstation is the minimum ESD protection required before the ESD seal on the product bag is broken.

1. Align the COMeT10-3900 standoffs with the mounting holes on the carrier board.
2. Ensure that the COM Express Type 10 mini interface connector (J200) is nicely seated in the COMe connector socket on the carrier board.
3. Apply pressure to the red region denoted in the following figure.

NOTE To minimize board flex on the carrier board, make sure the carrier board is supported on the opposite side prior to applying pressure to the COMe10-3900 module.

4. Insert and tighten down the screws supplied with your WINSYSTEMS heat spreader/ heat sink (sold separately). See “Accessories and Cables” on page 27 for a list of heat spreader and heat sink kits.



7.6 Thermal Management

WINSYSTEMS offers multiple heat spreader and heat sink kits to provide a way to transfer heat generated by the processor and other components away from the COMeT10-3900. Choosing a solution depends on how the system will be used, as well as its environmental conditions. Dissipating heat away from the COMeT10-3900 is crucial for maintaining system performance and counteracting CPU throttling. Contact a WINSYSTEMS Applications Engineer at +1-817-274-7553 for more information on our heat spreader and heat sink kits.

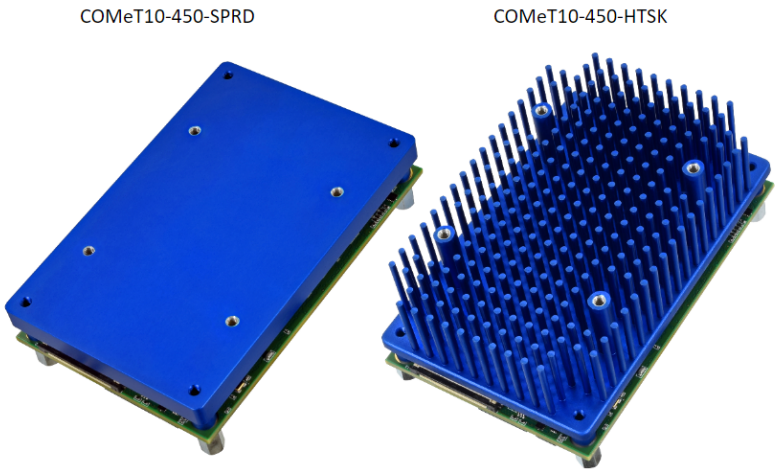
7.6.1 Heat Spreader

The WINSYSTEMS heat spreader (COMe10-450-SPRD) allows the COMeT10-3900 to be attached to a larger metal surface allowing heat to dissipate across a larger surface area. This method of passive cooling is extremely efficient and does not require an external fan. The maximum measurable temperature on any spot of the heat spreader must not exceed the operating temperature specified in Table 1, “COMeT10-3900 specifications,” on page 9.

NOTE Applying thermal compound between the heat spreader and the larger metal surface will increase the heat transfer efficiency.

7.6.2 Heat Sink

For projects that do not have a larger metal surface to attach the COMeT10-3900, WINSYSTEMS provides a heat sink (COMe10-450-HTSK) solution. Heat sinks are great for dissipating heat by natural convection or through active cooling with an external fan. The maximum measurable temperature on any spot of the heat sink must not exceed the operating temperature specified in Table 1, “COMeT10-3900 specifications,” on page 9.



7.7 On-board Features

7.7.1 eMMC Storage

The COMeT10-3900 provides an on-board high-speed eMMC for data storage, compliant with JEDEC e.MMC v5.1 standard. Typical use case for the on-board industrial eMMC is storing your operating system and enabling a write-protection method to lock down the OS from being written to. See the following table for a list of specifications regarding the on-board industrial eMMC.

Table 3: On-board industrial eMMC

Size	HS400 Sequential Read	HS400 Sequential Write	TBW	Data Rention
64 GB	290 MB/s	170 MB/s	412 TB	~300 P/E Cycles
128 GB	300 MB/s	170 MB/s	824 TB	~300 P/E Cycles

7.7.2 TPM 2.0

The COMeT10-3900 provides an on-board discrete TPM 2.0 hardware security chip.

7.7.3 Memory

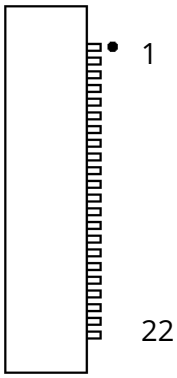
Up to 8GB of soldered down LPDDR4 memory is available on the COMeT10-3900. This memory can operate up to 2400 MT/s.

7.8 Connectors

7.8.1 J1 - MIPI-CSI Camera Interface Connector

The COMeT10-3900 provides a four-lane MIPI Camera Serial Interface 2 (MIPI-CSI-2) D-PHY 1.2 camera input. This camera input includes trigger and sync GPIO signals as well as I2C control lines.

Layout and Pin Reference

Diagram	Pin	Name	Pin	Name
	1	GND	12	D2 P
	2	D0 N	13	GND
	3	D0 P	14	D3 N
	4	GND	15	D3 P
	5	D1 N	16	GND
	6	D1 P	17	TRIGGER 3.3V
	7	GND	18	FLASH SYNC 3.3V
	8	CLK0 N	19	GND
	9	CLK0 P	20	MIPI I2C SCL 3.3V
	10	GND	21	MIPI I2C SDA 3.3V
	11	D2 N	22	3.3V

Flat Flex Connector

- Easy-On FFC/FPC Connector, 0.50mm Pitch

  Part Number: 52437-2271

Matching Flat Flex Ribbon Cable

- Molex Premo-Flex FFC, 0.50mm Pitch

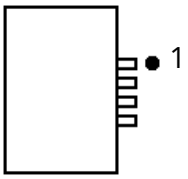
  Part Number: 15020 Series

7.8.2 J2 - Debug Interface Connector

JTAG debug at connector J2 is available upon request. Contact a WINSYSTEMS Applications Engineer at +1-817-274-7553. Alternatively, USB debugging is supported via USB 3.2, Gen 1 Port 0 for code development.

7.8.3 J3 - External Fan Connector

Layout and Pin Reference

Pin	Name
	
1	Vin
2	TACH
3	PWM
4	GND

Connector

- Pico-Lock PCB Header, 1.00mm Pitch

  Part Number: 503763-0491

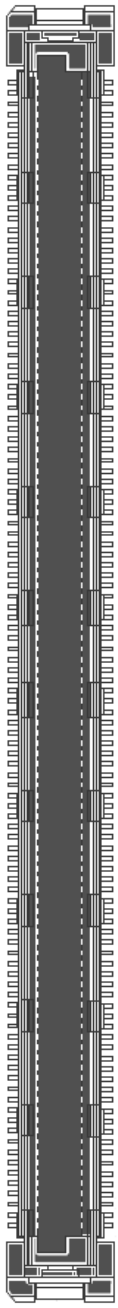
Matching Connector

- Molex Pico-Lock Receptacle Crimp Housing, 1.00mm Pitch

  Part Number: 503764-0401

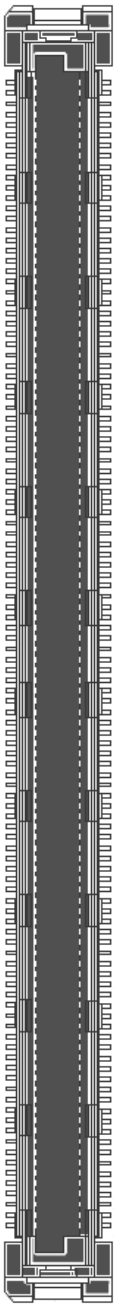
7.8.4 J200 - COM Express Type 10 mini Module Interface Connector

Layout and Pin Reference Row A



Pin	Description	Pin	Description	Pin	Description
A1	GND(FIXED)	A38	USB_6_7_OC#	A75	LVDS_A2+
A2	GBE0_MDI3-	A39	USB4-	A76	LVDS_A2-
A3	GBE0_MDI3+	A40	USB4+	A77	LVDS_VDD_EN
A4	GBE0_LINK100#	A41	GND(FIXED)	A78	LVDS_A3+
A5	GBE0_LINK1000#	A42	USB2-	A79	LVDS_A3-
A6	GBE0_MDI2-	A43	USB2+	A80	GND(FIXED)
A7	GBE0_MDI2+	A44	USB_2_3_OC#	A81	LVDS_A_CK+
A8	GBE0_LINK#	A45	USB0-	A82	LVDS_A_CK-
A9	GBE0_MDI1-	A46	USB0+	A83	LVDS_I2C_CK
A10	GBE0_MDI1+	A47	VCC_RTC	A84	LVDS_I2C_DAT
A11	GND(FIXED)	A48	EXCD0_PERST#	A85	GPI3
A12	GBE0_MDI0-	A49	EXCD0_CPPE#	A86	RSVD
A13	GBE0_MDI0+	A50	LPC_SERIRQ	A87	eDP_HPD
A14	GBE0_CTREF	A51	GND(FIXED)	A88	PCIE_CLK_REF+
A15	SUS_S3#	A52	RSVD	A89	PCIE_CLK_REF-
A16	SATA0_TX+	A53	RSVD	A90	GND(FIXED)
A17	SATA0_TX-	A54	GPI0	A91	SPI_POWER
A18	SUS_S4#	A55	RSVD	A92	SPI_MISO
A19	SATA0_RX+	A56	RSVD	A93	GPO0
A20	SATA0_RX-	A57	GND	A94	SPI_CLK
A21	GND(FIXED)	A58	PCIE_TX3+	A95	SPI_MOSI
A22	USB_SSRX0-	A59	PCIE_TX3-	A96	TPM_PP
A23	USB_SSRX0+	A60	GND(FIXED)	A97	TYPE10#
A24	SUS_S5#	A61	PCIE_TX2+	A98	SER0_TX
A25	USB_SSRX1-	A62	PCIE_TX2-	A99	SER0_RX
A26	USB_SSRX1+	A63	GPI1	A100	GND(FIXED)
A27	BATLOW#	A64	PCIE_TX1+	A101	SER1_TX
A28	(S)ATA_ACT#	A65	PCIE_TX1-	A102	SER1_RX
A29	AC/HDA_SYNC	A66	GND	A103	LID#
A30	AC/HDA_RST#	A67	GPI2	A104	VCC_12V
A31	GND(FIXED)	A68	PCIE_TX0+	A105	VCC_12V
A32	AC/HDA_BITCLK	A69	PCIE_TX0-	A106	VCC_12V
A33	AC/HDA_SDOUT	A70	GND(FIXED)	A107	VCC_12V
A34	BIOS_DIS0#	A71	LVDS_A0+	A108	VCC_12V
A35	THRMTRIP#	A72	LVDS_A0-	A109	VCC_12V
A36	USB6-	A73	LVDS_A1+	A110	GND(FIXED)
A37	USB6+	A74	LVDS_A1-		

Layout and Pin Reference Row B



Pin	Description	Pin	Description	Pin	Description
B1	GND(FIXED)	B38	USB_4_5_OC#	B75	DDI0_PAIR2+
B2	GBE0_ACT#	B39	USB5-	B76	DDI0_PAIR2-
B3	LPC_FRAME#	B40	USB5+	B77	DDI0_PAIR4+
B4	LPC_AD0	B41	GND(FIXED)	B78	DDI0_PAIR4-
B5	LPC_AD1	B42	USB3-	B79	LVDS_BKLT_EN
B6	LPC_AD2	B43	USB3+	B80	GND(FIXED)
B7	LPC_AD3	B44	USB_0_1_OC#	B81	DDI0_PAIR3+
B8	LPC_DRQ0#	B45	USB1-	B82	DDI0_PAIR3-
B9	LPC_DRQ1#	B46	USB1+	B83	LVDS_BKLT_CTRL
B10	LPC_CLK	B47	EXCD1_PERST#	B84	VCC_5V_SBY
B11	GND(FIXED)	B48	EXCD1_CPPE#	B85	VCC_5V_SBY
B12	PWRBTN#	B49	SYS_RESET#	B86	VCC_5V_SBY
B13	SMB_CK	B50	CB_RESET#	B87	VCC_5V_SBY
B14	SMB_DAT	B51	GND(FIXED)	B88	BIOS_DIS1#
B15	SMB_ALERT#	B52	RSVD	B89	DDI0_HPD
B16	SATA1_TX+	B53	RSVD	B90	GND(FIXED)
B17	SATA1_TX-	B54	GPO1	B91	DDI0_PAIR5+
B18	SUS_STAT#	B55	RSVD	B92	DDI0_PAIR5-
B19	SATA1_RX+	B56	RSVD	B93	DDI0_PAIR6+
B20	SATA1_RX-	B57	GPO2	B94	DDI0_PAIR6-
B21	GND(FIXED)	B58	PCIE_RX3+	B95	DDI0_DDC_AUX_SEL
B22	USB_SSTX0-	B59	PCIE_RX3-	B96	USB_HOST_PRSNT
B23	USB_SSTX0+	B60	GND(FIXED)	B97	SPI_CS#
B24	PWR_OK	B61	PCIE_RX2+	B98	DDI0_CTRLCLK_AUX+
B25	USB_SSTX1-	B62	PCIE_RX2-	B99	DDI0_CTRLDATA_AUX-
B26	USB_SSTX1+	B63	GPO3	B100	GND(FIXED)
B25	WDT	B64	PCIE_RX1+	B101	FAN_PWMOUT
B28	AC/HDA_SDIN2	B65	PCIE_RX1-	B102	FAN_TACHIN
B29	AC/HDA_SDIN1	B66	WAKE0#	B103	SLEEP#
B30	AC/HDA_SDIN0	B67	WAKE1#	B104	VCC_12V
B31	GND(FIXED)	B68	PCIE_RX0+	B105	VCC_12V
B32	SPKR	B69	PCIE_RX0-	B106	VCC_12V
B33	I2C_CK	B70	GND(FIXED)	B107	VCC_12V
B34	I2C_DAT	B71	DDI0_PAIR0+	B108	VCC_12V
B35	THRM#	B72	DDI0_PAIR0-	B109	VCC_12V
B36	USB7-	B73	DDI0_PAIR1+	B110	GND(FIXED)
B37	USB7+	B74	DDI0_PAIR1-		

8. COM Express Type 10 Features

8.1 Input Power

The COMeT10-3900 supports a wide range DC Input power of 4.75V to 20V via the COMe Type 10 connector at J200.

8.2 LVDS / eDP

WINSYSTEMS provides two variations of the COMeT10-3900: an eDP output, or a single channel LVDS output. The eDP output is powered by the integrated Intel HD Graphics 505 and is capable of 4k resolution output at 24 bits per pixel and 60Hz refresh rate.

The LVDS output is a population option that adds an LVDS bridge to the eDP output providing support for single channel LVDS panels.

Contact a WINSYSTEMS application engineer for additional information.

8.3 Digital Display Interface (DDI)

The COMe module provides one Dual Mode Display output via DDI0. This output can be used for DisplayPort, HDMI, or DVI. This eDP output is powered by the integrated Intel HD Graphics 505 and is capable of 4k resolution output at 24 bits per pixel and 60Hz refresh rate.

8.4 HD Audio

HD Audio signals from the Intel Atom E3900 processor are brought up through the COM Express Type 10 connector per PICMG specifications.

8.5 UART

The COMeT10-3900 provides two TTL compatible, 3.3V HSUART channels to the COM Express Type 10 connector. If legacy UART's are required, a build option is available that replaces the two HSUARTS with two legacy UARTS (2F8, 3F8).

8.6 PCI Express

Five channels of PCI Express Gen 2.0 lanes are provided from the Intel Atom E3900 processor. Four PCIe lanes (channels 0-3) connect directly to the COM Express Type 10 connector. The fifth lane (channel 4) provides on-board LAN via an Intel i210 1Gb/s Ethernet RGMII.

The four PCIe lanes (channels 0-3) can be arranged in different configurations as shown in the list below. Contact a WINSYSTEMS application engineer for additional information.

- Three x1 PCIe lanes (default)
  - Four x1 PCIe lanes if not using on-board LAN
- Two x1 PCIe lanes, One x2 PCIe lane
- Two x2 PCIe lanes
- One x4 PCIe lane

NOTE If using configuration 1, only three x1 PCIe lanes will be available due to the LAN (Intel i210) using one of the available four root ports.

8.7 USB Channels

Two channels of USB 3.2 Gen 1 (5 Gb/s), and six channels of USB 2.0 are provided directly from the Intel Atom E3900 processor to the COM Express Type 10 connector.

8.8 SATA 6 Gb/s

The COMeT10-3900 provides two SATA III (6 Gb/s) channels directly to COM Express Type 10 connector.

8.9 Ethernet

One Intel i210 1Gb/s Ethernet RGMII is provided via PCIe (channel 4). See 8.6 PCI Express for more information on PCIe lanes and configurations.

8.10 GPIO (General Purpose Input/Output)

The COMeT10-3900 provides 4x GPI and 4x GPO lanes. These GPI/O lanes are 3.3V CMOS level and EAPI compatible. A build option is available that replaces the GPI/O lanes with SDIO to allow the use of SD card interfaces.

8.11 LPC Bus

An LPC bus is provided for adding peripheral devices to the Carrier Board design. It allows the integration of low-bandwidth legacy I/O components within the system, which are typically provided by a Super I/O controller.

Furthermore, it can be used to interface Firmware Hubs, Trusted Platform Module (TPM) devices, general-purpose inputs and outputs, and Embedded Controller solutions.

8.12 SPI Bus

The SPI bus is specifically designed for carrier board BIOS storage. There is no SPI bus availability for external sensors and other peripherals.

8.13 I2C Bus

An I2C bus is provided for attaching external peripherals.

9. BIOS Functionality

The COMeT10-3900 BIOS settings and option descriptions can be found in our supplemental COMeT10-3900 BIOS Manual.

9.1 Software Description

This section provides details on the AMI BIOS components to be used in the implementation of the COMeT10-3900 BIOS firmware.

9.1.1 Software Design Specification: UEFI Operating System Support

The BIOS supports the booting of the following UEFI compliant operating systems:

- Windows 10 x64, IoT Enterprise, IoT Core, and Professional
- Linux x64
- Most x86 operating systems

9.1.2 Software Design Specification: Legacy Operating System Support

The BIOS supports the booting of the following legacy OS capabilities:

- MS-DOS 6
- Compatibility support module (CSM)
- Legacy boot support
- Legacy option ROM support

9.1.3 Software Design Specification: Boot Device Configuration

The BIOS supports booting an OS from the following devices:

- USB mass storage device
- Serial ATA (SATA) device
- Network boot - PXE
- eMMC
- M.2 mass storage device

9.1.4 Software Design Specification: BIOS Update Mechanisms

The BIOS supports the following update mechanisms:

- BIOS update with UEFI shell
- Software utilities
- Flash recovery via USB mass storage device

- Flash recovery via eMMC device
- Embedded controller (EC) firmware update with UEFI shell

9.1.5 Software Design Requirements: BIOS Components

The BIOS includes the following components:

- **Advanced Host Controller Interface (AHCI) support:** Provides SATA host controller functionality.
- **Display switching in setup:** Implements display switching using the UEFI GOP driver under the SETUP environment.
- **Boot order:** Generates the default boot order on the platform's first boot.
- **Boot/resume from S4 device:** Allows the platform to boot from the last S4 hibernated device, disregarding the current boot priority.
- **Cryptographic support:** Provides cryptographic related libraries, PPI, and UEFI protocols for security modules (secure FW update, secure boot, etc.)
- **Source level support:** Provides source level debug functionality for the BIOS project.
- **Fastboot:** Provides optimization of the boot time.
- **Fixed boot order:** Provides infrastructure that allows custom handling of available boot options to meet specific customer needs. Custom boot behavior may include different requests, such as always boot from specific device, default support of various kinds of grouping of boot devices.
- **Generic error logging:** Provides support for logging POST and runtime errors to the GPNV area.
- **Keyboard controller emulation** for USB keyboard/mouse.
- **Physical memory testing:** Supports testing of physical memory present in the system.
- RTC registration and ability to handle wakeup from S5 sleep state.
- **Secure boot support:** provides support and functionality to conform with UEFI 2.3.1 secure boot requirements and includes the following components:
  - Extended functionality of EFI NVRAM driver with support for authenticated EFI variables.
  - EFI image authentication module that installs EFI security architecture protocol with image authentication and image execution policy.
  - Secure boot variable (PK, KEK, db, and dbx) provisioning.
- Support for the booting to the built in UEFI shell.

9.2 BIOS Update with UEFI Shell

9.2.1 Scope

The Unified Extensible Firmware Interface (EFI or UEFI for short) is a new model for the interface between operating systems and firmware. It provides a standard environment for booting an operating system and running pre-boot applications.

An optional feature of a UEFI implementation is the ability to boot the system to a built-in shell. The UEFI shell provides a command prompt and a rich set of commands that extend and enhance the capability of the UEFI BIOS.

This section describes the process for updating the COMeT10-3900 BIOS firmware image using the built-in UEFI shell.

9.2.2 Process

1. Insert a USB flash drive containing the BIOS update program into a USB socket on the COMeT10-3900 platform.
2. Turn on the COMeT10-3900 and press the **ESC** or **DEL** key during the boot process, which starts the BIOS setup utility.
3. In the BIOS setup utility, use the cursor keys to highlight the **Save & Exit** menu option.
4. Use the cursor keys to select **UEFI: Built-In EFI Shell** from the list of boot devices displayed under the **Boot Override** section.
5. Press **Enter**.

   The COMeT10-3900 executes the built-in UEFI shell, and displays a list of attached storage devices. The USB flash drive shows up in the list; depending on other boot devices attached, it may be listed as **fs0**, **fs1**, etc.

6. From the UEFI shell command prompt, enter the following command where `N` is the number of the fs device representing the USB flash drive:

   ```
   fsN:
   ```

   Example: `fs1:`

   The shell prompt changes to indicate that device fsN is now the active storage device, e.g., `fs1:`

7. Execute the following command:

   ```
   ls
   ```

   The output of the `ls` command is similar to the display listing available with the Linux or MS-DOS list directory command. If the correct storage device was selected in step 6 above, the `ls` command should

show the BIOS update program in the directory listing obtained with the ls command.

8. Assuming the BIOS update program is named `Update.efi`, enter the following command at the shell command prompt:

   ```
   Update.efi
   ```

   The BIOS update program begins executing.

9. When the update program completes, power cycle the platform to force the new BIOS image to load and execute.
10. Verify that the BIOS update was successful by comparing the displayed BIOS version with the version specified in the BIOS update notification.

9.3 Embedded Controller (EC) Update with UEFI Shell

9.3.1 Scope

The Unified Extensible Firmware Interface (EFI or UEFI for short) is a new model for the interface between operating systems and firmware. It provides a standard environment for booting an operating system and running pre-boot applications.

An optional feature of a UEFI implementation is the ability to boot the system to a built-in shell. The UEFI shell provides a command prompt and a rich set of commands that extend and enhance the capability of the UEFI BIOS.

This section describes the process for updating the COMeT10-3900 Embedded Controller (EC) image using the built-in UEFI shell.

9.3.2 Process

1. Insert a USB flash drive containing the EC update program into a USB socket on the COMeT10-3900 platform.
2. Turn on the COMeT10-3900 and press the **ESC** or **DEL** key during the boot process, which starts the BIOS setup utility.
3. In the BIOS setup utility, use the cursor keys to highlight the **Save & Exit** menu option.
4. Use the cursor keys to select **UEFI: Built-In EFI Shell** from the list of boot devices displayed under the **Boot Override** section.
5. Press **Enter**.

   The COMeT10-3900 executes the built-in UEFI shell, and displays a list of attached storage devices. The USB flash drive shows up in the list; depending on other boot devices attached, it may be listed as **fs0**, **fs1**, etc.

6. From the UEFI shell command prompt, enter the following command where `N` is the number of the fs device representing the USB flash drive:

   `fsN:`

   Example: `fs1:`

   The shell prompt changes to indicate that device fsN is now the active storage device, e.g., `fs1:`

7. Execute the following command:

   `ls`

   The output of the `ls` command is similar to the display listing available with the Linux or MS-DOS list directory command. If the correct storage device was selected in step 6 above, the `ls` command should show the EC update program in the directory listing obtained with the ls command.

8. Assuming the EC update program is named `Update.efi`, enter the following command at the shell command prompt:

   `Update.efi`

   The EC update program begins executing.

9. When the update program completes, power cycle the platform to force the new EC image to load and execute.

10. Verify that the EC update was successful by comparing the displayed EC version in the BIOS with the version specified in the EC update notification.

10. Accessories and Cables

WINSYSTEMS provides accessories to complete your embedded computing solution. Our Application Engineers are available to guide you through product selection and customized options.

Table 4: Accessory and cable specifications

Item	Part Number	Description
Thermal Solution	COMe10-450-SPRD-0	Heat spreader though-hole, necessary hardware
Thermal Solution	COMe10-450-SPRD-1	Heat spreader threaded, necessary hardware
Thermal Solution	COMe10-450-HTSK-0	Heat sink though-hole, necessary hardware
Thermal Solution	COMe10-450-HTSK-1	Heat sink threaded, necessary hardware
COMeT10 Reference Carrier	ITX-M-CC452-T10	Mini-ITX reference carrier board specifically designed for COMe10-3900
Cable	CBL-FFC05-22-152A	MIPI/CSI-2 flat flex ribbon cable

11. Software Drivers

Go to www.winsystems.com for information on available software drivers.

Appendix A. Best Practices

The following paragraphs outline the best practices for operating the COMeT10-3900 in a safe, effective manner, that does not damage the board. Read this section carefully.

Power Supply

Avoid Electrostatic Discharge (ESD)
Only handle the circuit board and other bare electronics when electrostatic discharge (ESD) protection is in place. Having a wrist strap and a fully grounded workstation is the minimum ESD protection required before the ESD seal on the product bag is broken.

Power Supply Budget

Evaluate your power supply budget. It is usually good practice to budget twice the typical power requirement for all of your devices.

Zero-load Power Supply

Use a zero-load power supply whenever possible. A zero-load power supply does not require a minimum power load to regulate. If a zero-load power supply is not appropriate for your application, then verify that the COMe Type 10 module and carrier board's typical load is not lower than the power supply's minimum load. If the COMe Type 10 module and carrier board does not draw enough power to meet the power supply's minimum load, then the power supply does not regulate properly and can cause damage to the COMeT10-3900.

Use Proper Power Connections (Voltage)
When verifying the voltage, measure it at the power connector on the COMeT10-3900. Measuring it at the power supply does not account for voltage drop through the wire and connectors.

The COMeT10-3900 requires 4.75V to 20V to operate. Verify the power connections. Incorrect voltages can cause catastrophic damage.

Power Harness

Minimize the length of the power harness. This reduces the amount of voltage drop between the power supply and the COMeT10-3900.

Gauge Wire

Use the largest gauge wire that you can. Most connector manufacturers have a maximum gauge wire they recommend for their pins.

Contact Points

WINSYSTEMS boards mostly use connectors with gold finish contacts. Gold finish contacts are used exclusively on high-speed connections. Power and lower speed peripheral connectors may use a tin finish as an alternative contact surface. It is critical that the contact material in the mating connectors is matched properly (gold to gold and tin to tin). Contact areas made with dissimilar metals can cause oxidation/corrosion, resulting in unreliable connections.

Pin Contacts

Often the pin contacts used in cabling are not given enough attention. The ideal choice for a pin contact would include a design similar to Molex or Trifurcon designs, which provide three distinct points to maximize the contact area and improve connection integrity in high shock and vibration applications.

Power Down

Make sure that power has been removed from the system before making or breaking any connections.

Power Supply OFF—Always turn off the power supply before connecting to the embedded system. Do not hot-plug the COMeT10-3900 on a host carrier board that is already powered.

I/O Connections OFF—Turn off all I/O connections before connecting them to the embedded computer modules or any I/O cards. Connecting hot signals can cause damage whether the embedded system is powered or not.

Mounting and Protecting the COMeT10-3900

To avoid damage, mount the COMeT10-3900 properly. Standoff kits are available and recommended for use with the COMeT10-3900.

Placing the COMeT10-3900 on mounting standoffs—Be careful when placing the COMeT10-3900 on the mounting standoffs. Sliding the board around until the standoffs are visible from the top can cause component damage on the bottom of the board.

Do not bend or flex the COMeT10-3900—Bending or flexing can cause irreparable damage. Embedded computer modules are especially sensitive to flexing or bending around ball grid array (BGA) devices. BGA devices are extremely rigid by design, and flexing or bending the embedded computer module can cause the BGA to tear away from the printed circuit board.

Mounting holes—The mounting holes are plated on the top, bottom, and through the barrel of the hole. Traces are often routed in the inner layers right below, above, or around the mounting holes.

- Never use a drill or any other tool in an attempt to make the holes larger.
- Never use screws with oversized heads. The head could come in contact with nearby components causing a short or physical damage.
- Never use self-tapping screws; they compromise the walls of the mounting hole.
- Never use oversized screws that cut into the walls of the mounting holes.
- Always use all of the mounting holes. By using all of the mounting holes, you provide the support the embedded computer module needs to prevent bending or flexing.

Avoid cutting the COMeT10-3900—Never use star washers or any fastening hardware that cut into the COMeT10-3900.

Avoid over-tightening of mounting hardware—Causing the area around the mounting holes to compress could damage interlayer traces around the mounting holes.

Use appropriate tools—Always use tools that are appropriate for working with small hardware. Large tools can damage components around the mounting holes.

Conformal Coating

Conformal coating by any source other than WINSYSTEMS voids the product warranty and will not be accepted for repair by WINSYSTEMS. If such a product is sent to WINSYSTEMS for repair, it will be returned at customer expense and no service will be performed. A WINSYSTEMS product conformally coated by WINSYSTEMS will be subject to regular WINSYSTEMS warranty terms and conditions.

Operations/Product Manuals

Every WINSYSTEMS product has an Operations manual or Product manual.

Periodic updates—Operations/product manuals are updated often. Periodically check the WINSYSTEMS website (https://www.winsystems.com) for revisions.

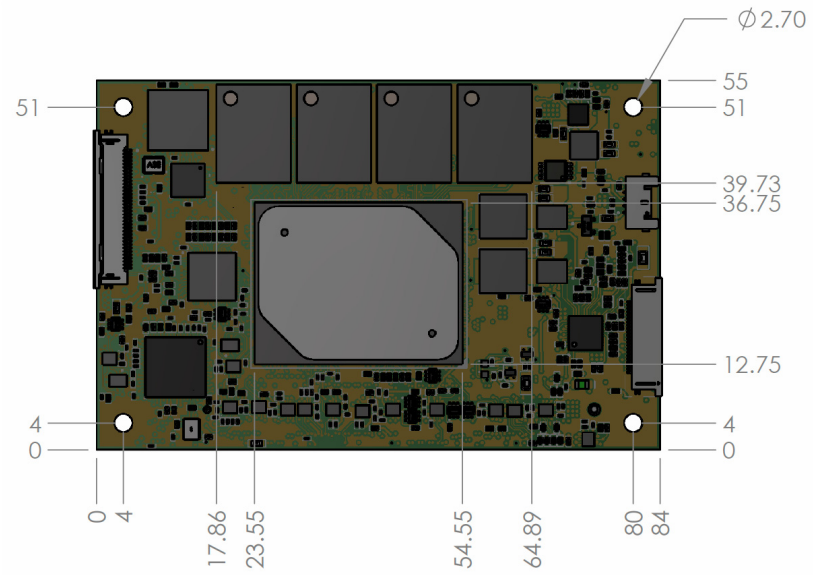
Check pinouts—Always check the pinout and connector locations in the manual before plugging in a cable. Many I/O modules have identical

headers for different functions and plugging a cable into the wrong header can have disastrous results.

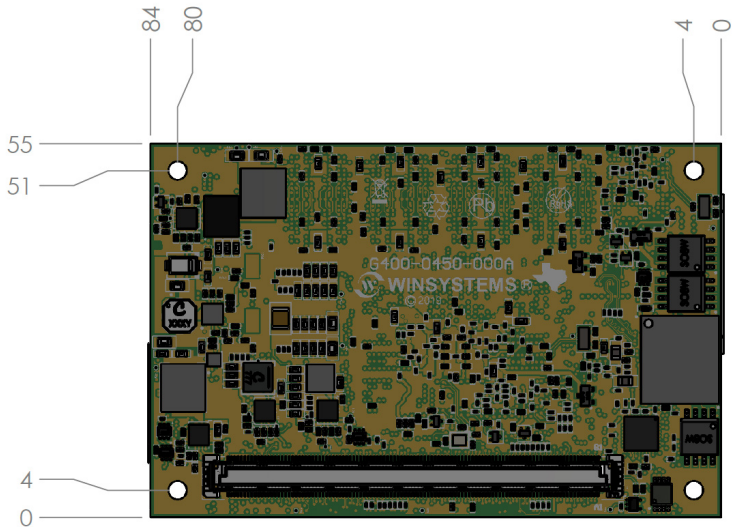
Contact an Applications Engineer—If a diagram or chart in a manual does not seem to match your board, or if you have additional questions, contact a WINSYSTEMS Applications Engineer at +1-817-274-7553.

Appendix B. Mechanical Drawings

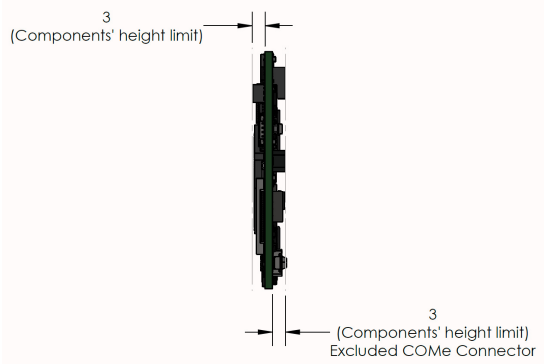
COMeT10-3900 Mechanical Drawings



Top View



Bottom View



Side View

Appendix C. Warranty Information

Full warranty information can be found at https://winsystems.com/company-policies/warranty/.