CTI 2500P-Jxxx
CTI 2500C-Jxxx

Janus Programmable Automation Controller

Installation and Operation Guide

Version 1.14

This manual is published by Control Technology Inc. (CTI) 5734 Middlebrook Pike, Knoxville, TN 37921.

DOCUMENT DISCLAIMER STATEMENT

Every effort has been made to ensure the accuracy of this document; however, errors do occasionally occur. CTI provides this document on an "as is" basis and assumes no responsibility for direct or consequential damages resulting from the use of this document. This document is provided without express or implied warranty of any kind, including but not limited to the warranties of merchantability or fitness for a particular purpose. This document and the products it references are subject to change without notice. If you have a comment or discover an error, please call us at 1-800-537-8398 or email us at *sales@controltechnology.com*.

REVISION HISTORY		
V1.0	4/28/2020	Initial Release
V1.01	5/20/2020	Corrected typos and improved formatting. Added details to battery installation (Section 3.2.4)
V1.02	7/22/2020	Corrected description of 'SD Card Ethernet Port Setup' (Section 3.2.9)
V1.03	1/27/2021	Updated warnings for battery.
V1.04	4/14/2021	Changed format of 'cti.ini' file used to specify a fixed IP Address using the "SD Card Ethernet Port Setup" (Section 3.2.9).
V1.05	5/18/2021	Added front panel picture of Janus Compact Programmable Automation Controller (Section 2.1). Modified Ethernet port description to reflect that the Janus Compact controller Ethernet ports C and D support a maximum speed of 100Mb (Section 2.6) Added a picture illustrating the location of the internal SD card and switches on the Janus Compact controller (Section 3.2.2). Added chapter for web server description (Chapter 8).
V1.06	6/10/2021	Corrected various bookmark hyperlinks. Added Error Code descriptions and Error Recovery details (Appendix A).
V1.07	6/15/2021	In "Controller Startup", added that we support only FAT32 on the internal SD card. In "Setting the IP Address", added we support only FAT32 and EXFAT on the external SD card. Also added warning about using leading zeroes in IP address octets.
V1.08	8/24/2021	Added display of Auto-IP address to Section 5.2 (Controller Startup). Added "Always Display Auto-IP" option to Section 4.1 (General Settings).
V1.09	10/18/2021	Corrected label for error LED in Sections 2.1 and 2.2
V1.10	10/25/2021	Enhanced description of controller security features in Section 1.1.
V1.10a	11/9/2021	Corrected typos.
V1.11	12/22/2021	Added clarification to PLC startup operation following a reset caused by pressing the front panel 'Clear Exception' button (Section 4.1).
V1.12	5/10/2022	Updated Error Codes in Appendix A.
V.12a	5/11/2022	Provided additional error recovery information for error code 250. Updated copyright date
V1.13	10/18/2022	Corrected various typos. Corrected images showing location of SD card and User Switches for Janus Classic Controller and Janus Compact Controller (Section 3.2.2). Modified table headers throughout document to use same font and shading.
V1.14	4/19/2023	Added product specification matrix from product bulletin and added clarifying description about "max connections".

PREFACE

This ***Installation and Operation Guide (IOG)*** provides information regarding installation, setup, and operation of the *CTI Janus Programmable Automation Controlle*r, also referred to as the *Janus Controlle*r in this manual.

This document is not intended to serve as a programming reference for application development. A comprehensive and thorough programming reference for application development is provided by the ***Janus Workbench*** online help system. This online help is critical for gaining an initial understanding of the product and is intended to be used as a reference for various aspects of the products features. The online help search feature provides for a quick way locate targeted information.

USAGE CONVENTIONS

NOTE

Notes alert the user to special features or procedures.

CAUTION

Cautions alert the user to procedures that could damage equipment.

WARNING

Warnings alert the user to procedures that could damage equipment and endanger the user.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

1.1 Janus Controller Overview

The CTI Janus Process Automation Controller (PAC) is an advanced, high-performance CPU with unmatched built-in communications capabilities. All CPU models provide a number of beneficial features.

Flexible Programming Support

The Janus controller allows you to program in languages that best fit your application requirements and your programming expertise. The following IEC 61131-3 compliant languages are supported:

- Relay Ladder Logic (RLL)
- Function Block Diagram (FBD)
- Structured Text (ST)
- Sequential Function Chart (SFC)
- Instruction List (IL)

A single project can contain programs written in different languages. Programs written in one language can be easily translated to another language to help with long term application support.

Integrated Ethernet Communications

Extensive communications support is included in the Janus controller, eliminating the need for separate communications modules. The controller provides four isolated Ethernet ports, any of which can be used to provide redundant network paths or to connect to different networks. The controller can be configured with multiple IP addresses and communicate concurrently on up to four different IP networks.

Ethernet Data Communications Protocols

The controller supports the following data communications protocols:

- CAMP Client (used to communicate with CTI 2500 Series CPUs and Ethernet modules)
- CAMP Server (allows data access from HMI/SCADA workstations using CAMP Client drivers
- CTI Enhanced Data Cache Client (optimized interface to CTI 2500 Series CPUs)
- Ethernet I/P Tag Client (used to communicate with Rockwell Logix controllers)
- Ethernet I/P Server (allows data access from HMI/SCADA workstations using Tag Client drivers)
- MQTT Client (support for IIOT (Industrial Internet of Things).
- Custom TCP/UDP client and server applications using network socket management functions

Ethernet I/O Protocols

The controller supports:

- Open Modus Client (TCP or UDP)
- Open Modbus Server (TCP or UDP)
- Ethernet I/P Scanner (supports Implicit I/O messages and CIP Explicit messages)
- Ethernet I/P Adapter (provides an interface for EIP I/O Scanners and CIP Explicit Message Clients)
- Profinet Controller I/O support is planned for the near future

Web Server Interface

The controller contains an embedded web server, which provides an interface to detailed information regarding the controller configuration, operation, and history. The web server can be used to:

- Obtain information about the product and application
- Configure the product settings
- Update product firmware
- Perform file transfer operations
- Access user-generated graphics pages (monitor and control application)
- View diagnostic information (such as error and status info)
- Access operational statistics
- View Event Log
- Supports user created web pages that access controller application data.
  (See Section 5.4 - HTTP Data Server)

The web server can be accessed by entering the controller IP address in the URL box of your browser.

Online Change Support

The controller supports a comprehensive change facility that allows you to make extensive changes to the user program, then download the changed program without bumping the I/O. *See the **Janus Workbench** Help for detailed information and limitations.*

Security

The controller supports the following set of security features:

- "Secure Boot" process – encryption keys that verify the controller is running an authenticated CTI version of the firmware;
- Password protection for accessing IEC Controller from Janus Workbench (set via Workbench);
- Password protection for modifying and/or viewing any POU from Janus Workbench (set via Workbench);
- Password protection for modifying controller Configuration settings via web server (Includes File Management and Firmware Update operations);
- Password protection for the controller Operation pages (File Management/Firmware Update);
- Password protection for accessing visualization (HTML5 Graphics);
- User program is compiled on the PC and downloaded, which allows more user options for controlling access to the project source files.

Compatibility

The Janus Controller is designed to work in the same plant environment as the CTI 2500 Series PLC, supporting many of the legacy interfaces. It is compatible with existing CTI 2500 Series and Siemens Series 505 local and remote I/O and Profibus-DP I/O. It can function as an Ethernet CAMP server, allowing it to communicate with existing HMI/SCADA workstations and CTI 2572/2572-A/2572-B communications modules. It can also act as a CAMP client for peer-to-peer communications to existing CTI products. The Enhanced Data Cache Client protocol facilitates high speed communications with CTI 2500 Series PLCs.

High Performance

All Janus Controllers are powered by an ultra-high performance SoC (System on Chip) with ARM®+ FPGA architecture providing extreme I/O bandwidth with low system power requirements. This architecture provides capability to simultaneously execute logic and I/O communications which translates to sub-millisecond cycle times for many small applications.

1.2 Janus Programming Software

The Janus Controller is programmed using ***Janus Workbench.*** Janus Workbench is a full-featured Integrated Development Environment (IDE) tool that includes a configuration tool, programming editor, debugger, data monitor, and simulator. The application program may be developed in any of five IEC-61131 programming languages. A complete library of functions is provided to perform the following tasks:

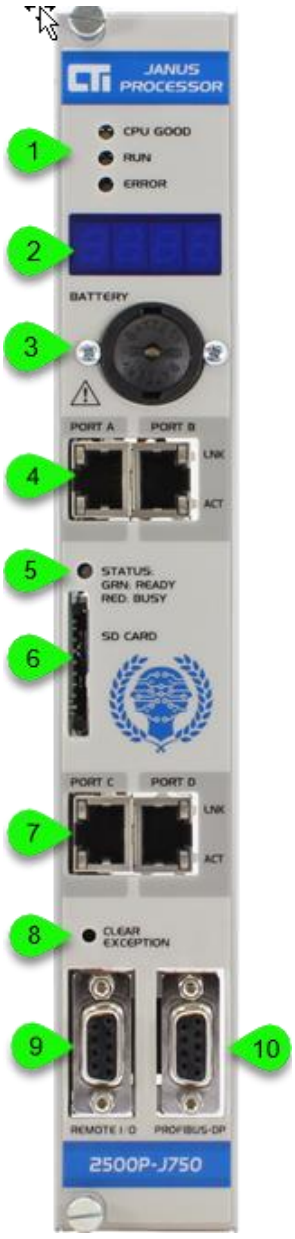
- Complex mathematical computations
- Boolean logic
- Data conversion
- String handling
- Timer/Counter operations
- PID control
- Alarm monitoring
- Data Logging and file access functions
- Protocol driver management

The programming architecture enables the “building block” approach to application design which encourages the re-use of well-documented and proven code sections. Custom logic using complex data types such as structures and enumerations can be embedded into Sub-Programs and User Defined Function Blocks (UDFBs) and re-used in multiple applications.

Janus Workbench also provides a means to select and configure fieldbus drivers supported by the controller. For more information, refer to the Janus Workbench Help system.

CHAPTER 2 FRONT PANEL

2.1 Janus Classic Controller Front Panel



1. **Operational Status LEDs**

   CPU GOOD

   RUN

   ERROR

2. **Alphanumeric Display**

3. **Battery Holder**

4. **Ethernet Ports A and B (1000 Mb)**
   Link LED (LINK)
   Activity LED (ACT)

5. **SD Card Status LED**
   Green- Card Ready
   Red- Card Busy

6. **SD Card Receptacle**

7. **Ethernet Ports C and D (1000 Mb)**
   Link LED (LINK)
   Activity LED (ACT)

8. **Clear Exception Button**

9. **Remote I/O Port**

10. **Profibus Port (Model Dependent)**

2.2 Janus Compact Controller Front Panel

1. **Operational Status LEDs**

   CPU GOOD

   RUN

   ERROR

2. **SD Card Receptacle**
3. **Alphanumeric Display**
4. **SD Card Status LED**
   Green- Card Ready
   Red- Card Busy
5. **Clear Exception Button**
6. **Battery Holder**
7. **Ethernet Ports A and B (1000 Mb)**
   Link LED (LINK)
   Activity LED (ACT)
8. **Ethernet Ports C and D (100 Mb)**
   Link LED (LINK)
   Activity LED (ACT)
9. **Remote I/O Port**
10. **Profibus Port (Model Dependent)**

2.3 Status Indicator LEDs

LED	Color	State	Indication
CPU GOOD	BLUE	Off	Not operational – module initialization failure or no power
		Flash	N/A
		On	Module hardware/firmware passed all power-on tests and operation is normal
RUN	BLUE	Off	Application program stopped or not loaded
		Flash	Program loaded but logic is not running (**LOGIC STOP** state). I/O interface and communication protocols are active.
		On	Application program is executing (RUN state)
ERROR	YELLOW	Off	No active errors
		Flash	Critical error that prevents application from entering RUN mode (Error Code displayed on front panel)
		On	After software boot, indicates active error conditions. These errors can occur while in RUN mode and will not prevent application from transferring to RUN mode. (Error Code displayed on front panel) On initial power up, this signals that the hardware is powered and ready for software boot.

2.4 Alphanumeric Display

The Alphanumeric Display is used to display IP parameters (i.e. IP addresses and subnet information) and active error status information. If desired, the display of IP parameters can be disabled using the embedded web server. When an error state is active, the corresponding error code is displayed. When multiple error states are active, the highest priority active error code is displayed. See APPENDIX A SYSTEM ERROR CODES for a list of system error codes and descriptions.

2.5 Battery

A replaceable high-power Lithium Metal Oxide battery provides an auxiliary power source to provide an orderly system shutdown when DC power from the backplane is lost while the controller is in RUN state. The battery is accessible through the front panel battery cover and can be replaced while the application is running.

The battery circuit is automatically enabled when the backplane power is removed. After a successful shutdown, the battery circuit is disabled to preserve battery life. See Section 3.2.4: Inserting the Battery for instructions regarding battery installation and care.

2.6 Ethernet Communications Ports

The RJ-45 Ethernet ports, labeled **PORT A, PORT B, PORT C, AND PORT D,** are identical in their operation and usage. For the Janus Classic controller, all ports are capable of operating at 1000Mb (1Gb) full duplex. For the Janus Compact controller, Ports A and B are capable of operating at 1000Mb (1Gb) full duplex while ports C and D are capable of operating at 100 Mb full duplex. If connected to a device that does not support the maximum port speed, a port will auto-negotiate with the device a slower speed (100Mb or 10Mb). All ports can be used for multiple purposes, such as programming and monitoring, data communications with SCADA workstations and other devices, and Ethernet based I/O. Duplicate IP Address detection, broadcast/multicast storm protection and traffic rate limiting are enabled for each port.

By default, Ethernet frames arriving at a port are forwarded only to the controller microprocessor. Ethernet frames are not forwarded between the ports, preventing the accidental creation of loops. If ports are connected to different networks, this behavior prevents traffic on a particular network from entering the other networks. To allow for special situations, forwarding between ports can be enabled in the web server CONFIGURATION/NETWORK SETTINGS page. See Section 4.2.3 Internal Ethernet Switch Configuration.

Each Ethernet port connector contains two embedded LEDs. The **LINK** LED (top) indicates whether the Ethernet port is successfully connected to another Ethernet device, such as a network switch. The **ACTIVITY** LED (bottom) provides visual indication that Ethernet packets are being received or transmitted via the port. See the following table below for details.

LED	State	Indication
Link	Off	Ethernet link is not available.
	On	Ethernet link is available.
Act (Activity)	Off	No Ethernet frames are being transmitted on the network to which the port is connected.
	On (Blinking)	Ethernet frames are being transmitted on the network to which the port is connected

2.7 External SD Card Slot

The front panel contains a receptacle for a full-size SD card. Standard (SD) and high capacity (SDHC) memory cards may be used. This SD card is not required for controller operation, and no logic instructions will access (read or write data) from this card. A bicolor **STATUS** LED, mounted in the front panel indicates the following conditions:

- OFF: No SD card is inserted
- GREEN: An SD card is inserted into the receptacle but it is not being accessed by the controller firmware. When this condition exists, the card can be removed.
- RED: The firmware is accessing the SD card (reading or writing). When this condition exists, you should not remove the card. Removing the card will corrupt the data on the card.

This card has three primary uses as described below:

a) ***SD Card Ethernet Port Setup*** provides a method for the user to specify a fixed IP Address when the controller has not been configured (i.e. on initial power-up or after configuration reset). This operation executes only if Module Switch 2 = OPEN and Module Switch 4 = CLOSED. See SD Card Ethernet Port Setup 3.2.9 for more information.

b) ***SD Card Firmware Update*** provides an alternate method for firmware update when *Remote Firmware Update* is not allowed or connection from ***Janus Workbench*** is inconvenient. The ***SD Card Firmware Update*** method is initiated on startup when Module DIP Switch 2 is set to CLOSED position. See Front Panel SD Card Firmware Update for additional information.

c) ***File Operations*** allows you to transfer files between the internal SD card and the external SD card and/or PC. For example, you could use this facility to backup controller system and/or application files while the application is running. These operations can be selected via the web server **File Management** page.

2.8 Clear Exception Pushbutton

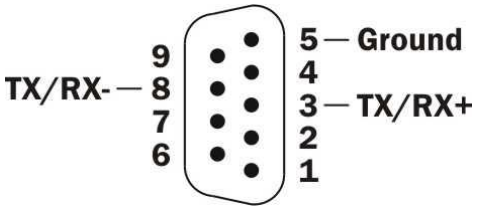
When enabled, the **CLEAR EXCEPTION** pushbutton provides a direct method to clear exceptions, reset controller configuration values to default values, or restore factory defaults without requiring access to ***Janus Workbench*** or the controller web server. See Section 5.3 for more information.

NOTE

The recessed pushbutton will function only when Switch 3 is in the CLOSED position.
See Section 3.2.3 Setting the Module Switches

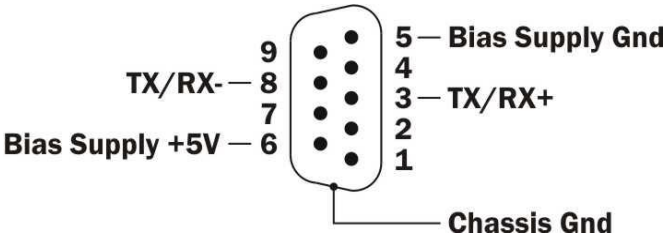
2.9 Remote I/O Port

This DB-9 connector (labeled 'Remote I/O') provides the RS-485 serial interface to the legacy 505/2500 Remote I/O network. The pinout for this connector is shown below:



2.10Profibus DP Port

On models where the controller can be configured as Profibus master, this DB-9 connector (labeled '*Profibus-DP*') provides the RS-485 interface to the Profibus-DP network. The pinout for shown below. The cable shield is connected to 'Chassis Ground'. Pins 5-6 are used for the bias circuit.



CHAPTER 3 INSTALLATION

This section discusses the items to consider while planning the Janus Controller installation and the actual steps for installation of the module.

3.1 Installation Planning

3.1.1 Safety Considerations

Before installing the controller, you must identify the personnel hazards that may be created in the event of a system failure and provide interlocks and safety switches to prevent operation during a system failure.

WARNING

As a system designer, you should be aware that Control devices can fail in an unsafe condition. Unless you incorporate proper safeguards, malfunction of the controller or associated devices, such as operator interface equipment, could cause sudden equipment startup, shutdown, or other unexpected operation. Such startup or shutdown or unexpected operation could result in death or serious injury to personnel, and/or damage to equipment.

If you or your company are using CTI controllers with processes or equipment that requires the presence of a person (such as an operator or attendant), you should be aware of this potential safety hazard and take appropriate precautions.

Safety Recommendations

Consideration should be given to the use of an emergency stop function which is independent of the programmable controller. Where the operator is exposed to the machinery, such as in loading or unloading a machine tool, or where the machine cycles automatically, consideration should be given to the use of an electromechanical override or other redundant means for stopping the machine cycle. If provision is required for changing programs while the equipment is in operation, consideration should be given to the use of locks or other means of assuring that such changes can be made only by authorized personnel. These recommendations are intended as safeguards against the failure of critical components and the effects of such failures or the inadvertent errors that might be introduced if programs are changed while the equipment is in operation.

Operator Safety Switches

Power should be configured so that it can be manually removed from all output devices. You must provide a method that is independent of the control system for disconnecting power from the outputs when a machine is not operating or the operator must reach into the machine. A non-electronic switch or directly wired relay must be used to disconnect the power.

Emergency Stop Switch

You must provide a method for disconnecting power from the outputs if an emergency situation is encountered with the machine operation. Use a non-electronic switch or relay that is wired external to the controller and that is easily accessible.

3.1.2 Electrical Interference

Electrical interference conducted directly through wiring or inducted via electromagnetic coupling can adversely affect the operation of control equipment. The major sources of electrical interference in an industrial environment are devices that use high voltages and current, such as motors and welders.

The Janus Controller is designed to meet or exceed IEC standards for immunity to electrical interference. However, care must be taken to ensure the control equipment is exposed to devices that serve as major sources of electrical interference devices. To ensure a reliable control system, you will need to determine the source of the electrical interference and employ suitable techniques to reduce its effect on the control system.

3.1.3 Grounding

It is very important that the all equipment is properly grounded. Lack of proper grounding may cause intermittent or erratic operation or may cause the control system to fail. A properly installed grounding system will provide a low-impedance path to earth ground, which will give all PLC internal filtering devices a good ground return for reference. The earth ground of the building site typically provides reliable grounding; however, if excessive ground current is present, a separate grounding electrode should be installed.

A common practice is to provide a central ground bus bar as a single point of reference within each enclosure, connecting all chassis and power supply components to the bus bar. The bus bar is then connected to earth ground. When connecting to the bus bar, use 1-inch copper braid or No. 8 AWG wire. To ensure good connections, scrape paint or other non-conductive coatings away from mounting studs and from enclosure surfaces where mounting bolts and washers make contact.

In addition to connecting the controller chassis and power supply to earth ground, you must ensure that the power supply, controller and all modules installed in the base are installed securely and that the thumbscrews are tightened.

3.1.4 Choosing the IP Address and related Parameters

Before you can use the Ethernet port, the controller must be configured with network parameters, including IP address, network mask, and the default gateway. If you already have a network installed, you should contact your network administrator to determine the values to be used. See APPENDIX B: IP ADDRESS INFORMATION for more information on choosing an IP address. See Section 3.2.8 and Section 3.2.9 for information on setting the network parameters.

3.1.5 Power Requirements

The Janus controller consumes 10 watts of +5 VDC power. To calculate the total power required for the base, you need to add the power requirements for the other modules you will install in the base.

3.1.6 SD Card Selection

Size

There are three sizes of SD cards: standard, mini, and micro. The SD card receptacles on the Janus controller are designed for a standard size card. A passive adapter can be used to accommodate the smaller mini or micro sizes, if necessary.

Capacity

The Janus controller accepts standard SD cards and high capacity SDHC cards. SD cards, which have a maximum capacity of 2 GB, are an older technology that may not be readily available. SDHC cards have a maximum capacity of 32 GB and are widely available. For most applications, an SDHC card with a capacity of 16GB is sufficient.

Speed

The SD card access speed is indicated by a class rating, which indicates the minimum continuous write speed. For example, a class rating of ④ indicates 4 MB/sec. Class 4 SD or SDHC cards are usually sufficient for use in the front panel SD receptacle. However, an SDHC card with a class rating of ⑩ is required for the internal SD card.

3.2 Installing the Controller

3.2.1 Unpacking the Module

Open the shipping carton and remove the special anti-static bag that contains the module. Ensure you are properly grounded and have discharged any static buildup before removing the unit from the static bag.
Do not discard the anti-static bag; use it for protection against static damage when the module is not inserted into the I/O base.

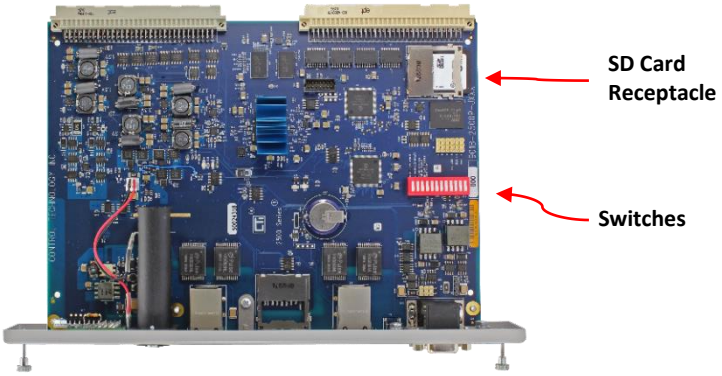
CAUTION

The components on the Janus controller printed circuit card can be damaged by static electricity discharge. To prevent this damage, the module is shipped in a special anti-static bag. Static control precautions should be followed when removing the module from the bag and when handling the printed circuit card during configuration.

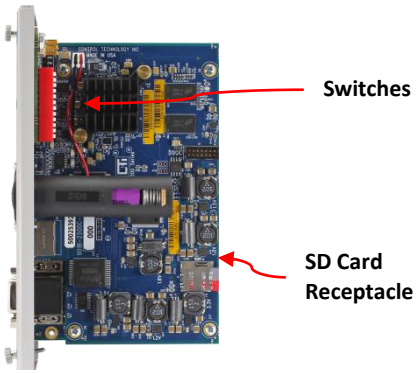
3.2.2 Internal SD Card Installation

The Janus controller uses a Secure Data (SD) card for storage of configuration data, executable program, application program source files, and user data files. A high capacity SDHC card is pre-installed on all units shipped from the factory. Contact CTI support if the SD card is missing. **Because all configuration and operational files are contained on the SD card, the complete controller profile can be transferred to another unit simply by swapping SD cards.**

The receptacle for the internal SD card is located on the controller circuit board as shown in the following pictures.



Janus Classic Controller



Janus Compact Controller

To remove and replace the internal SD card:

- Remove power to the base.
- Remove the controller from the base.
- To remove the card, apply insertion pressure until you hear a click, then release pressure.
- To install the card, insert the card in the receptacle face up, with the beveled edge facing the receptacle. Continue insertion until you hear a click, then release.

NOTE

A replacement SD card must have a write speed rating of at least 10 MB/s (Class 10). CTI recommends you purchase an SD card with an industrial rating.

3.2.3 Setting the Module Switches

The functions of the module user switches are shown below:

Switch Position	Use	Open Position	Closed Position
1	Remote Firmware Update	Disabled	Enables firmware update via web server. See Section 6.3 for details.
2	SD Card Firmware Update	Normal operation	Controller enters *Front Panel SD Card Firmware Update* mode at startup. See Section 6.2 for details.
3	Clear Exception Pushbutton	Disabled	Enables the recessed pushbutton to be used to clear exceptions, configuration reset, or to restore factory settings. See Section 5.3.
4	SD Card Ethernet Port Setup	Disabled	Allows user to configure controller Ethernet Port A via front panel SD card. NOTE: This setting works ONLY if Switch 2 is OPEN. See Section 3.2.9.
5	Remote Controller Reset	Disabled	Enables the ability to clear exceptions, Configuration Reset, and Restore Factory Settings using the embedded web server.
6 - 12	Reserved		

See the illustration in the preceding Section 3.2.2 for the location of the switches.

3.2.4 Inserting the Battery

The Janus controller uses a non-rechargeable lithium battery which supplies power to save processor contents after AC power is removed. The Janus controller is shipped with the battery installed in the unit. The battery is accessible by removing the front panel battery cover. Rotate the cover counterclockwise to remove it by inserting a coin or a screwdriver into the slot on the cover.

WARNING

The controller uses a 4.0 lithium battery, size AA. See Appendix D for additional battery specifications.

Batteries must be changed in an area known to be non-hazardous.

Do not attempt to charge the lithium battery. Charging a lithium battery can cause the battery to explode, resulting in serious injury or death and/or damage to equipment. Replace the battery as shown above.

Lithium batteries contain flammable material. Do not puncture or crush the battery case, since this can release the material and electrolyte. Exposure to electrolyte can cause eye and/or throat irritation. If the electrolyte comes into contact with your skin or eyes, flush thoroughly with water.

Do not place batteries on a metal surface, as this could cause a short circuit. If a lithium battery short-circuits, disconnect it immediately and move it to a well-ventilated area. Wear safety glasses and other protective gear when handling a defective battery.

Do not use lithium batteries in a completely sealed container. There must be a means of relieving pressure if the battery is exposed to high temperature or abuse.

The Janus controller monitors battery status and provides 'Battery Low' indication when the battery has approximately 30% of its usable life remaining. At this point, the battery will still provide adequate power for power-loss conditions for some period of time (based on size of application and number of occurrences). However, a replacement battery should be ordered and installed as soon as possible.

To replace the battery, insert the battery into the battery holder with the button end (+) facing outward. Then align the battery cover tabs with the slots in the holder, press the cover in until it is flush with the holder, and rotate it 90º in a clockwise direction.

Batteries should be stored in the original shipping container in a cool well-ventilated area. Dispose of used batteries according the instructions of its manufacturer and in compliance with all federal, state, and local regulations.

CAUTION

The high-power battery shipped with the Janus controller is different than the one used in the CTI 2500 Series PLC and should be replaced only with the exact same model.

See APPENDIX C for Battery Specifications.

Contact CTI for replacement batteries.

3.2.5 Physical Installation

Before installing the controller, remove AC power from the rack. Align the circuit board with the connector next to the power supply. Slide the controller into the rack until the connector seats. Then use the thumbscrews to secure the controller in the rack.

WARNING

Do not install or remove the controller while line power is applied. It can damage the controller or other equipment and could cause injury or death.

3.2.6 Connecting the Controller to a Data Network

To connect the Janus controller to an Ethernet network, insert an Ethernet cable that is rated Category 5e into the RJ-45 connector of any front panel Ethernet ports: PORT A, PORT B, PORT C, or PORT D. Insert the other end into the RJ-45 connector of the network Ethernet switch. If the connection is successful, the Link LED on the RJ-45 connector will illuminate.

3.2.7 Applying Power to the Base

Apply AC power to the base power supply. The Power Good LED on the power supply should illuminate, indicating that power is being supplied to the base connectors. The Janus controller should power up. See Section 5.2 Controller Startup for additional information.

3.2.8 Startup from Factory Defaults

If you are starting up using the factory default, the controller will attempt to obtain an IP address using DHCP (Dynamic Host Configuration Protocol). If a valid response is received, the controller will use the IP address parameters provided. If not, the controller will assign an IP address from the Link Local IPV4 range.

IP Address in IPV4 link-local address block: 169.254.0.0 – 169.254.255.255
Subnet Mask: 255.255.0.0 (CIDR 16)
Gateway Address: 0.0.0.0

NOTE

The IP address parameters obtained from DHCP or assigned from the link local range are for temporary use only. They are not permanently stored and will be cleared when the controller is restarted. You can set a permanent IP address by using this address to access the web server configuration page or you can use the SD Card Ethernet Port setup described below.

3.2.9 Setting the IP Address

SD Card Ethernet Port Setup

The ***SD Card Ethernet Port Setup*** provides you an alternate method to specify a fixed IP Address for the controller Primary Subnet configuration when the web server is not accessible. This is useful for setting the initial IP address for a new product or following a configuration reset.

This operation executes only if Module Switch 2 is OPEN and Module Switch 4 is CLOSED. If both Switches 2 and 4 are CLOSED, the '*Front Panel SD Card Firmware Update'* operation, which is executed when Switch 2 is CLOSED takes precedence.

This operation requires the following steps:

a) Create a file named 'cti.ini' using your favorite text editor (Notepad works just fine).
The following keywords and associated values must be inserted into this file. The values must be valid network settings expressed in dotted decimal notation. WARNING: Do not use leading zeroes for any of the 4 octets in any of the IP addresses, as leading zeroes in TCP/IP will imply base-8 notation (Don't use: ~~192.168.1.011,~~ Instead use: 192.168.1.11).

```
[NET0]
usingdhcp = false
ip = x.x.x.x
subnetmask = x.x.x.0
gateway = x.x.x.x *
```

* This keyword and associated value is optional. If you don't want to specify a default gateway address, you should omit this entry.

Examples:

<u>With Gateway Address</u>:

```
[NET0]
usingdhcp = false
ip = 198.18.74.56
subnetmask = 255.255.255.0
gateway = 198.18.74.1
```

<u>Without Gateway Address</u>:

```
[NET0]
usingdhcp = false
ip = 198.18.74.56
subnetmask = 255.255.255.0
```

Each keyword/value combination must be entered on a separate line. If keywords are duplicated, only the first entry is processed – the others are ignored.

b) Copy the cti.ini file created above to the root directory of a SD card and insert that card into the front panel SD card slot. The file system of the front panel SD card should be either FAT32 or EXFAT. This is the way they come when newly purchased. If you have reformatted your SD card with the NTFS file system, or any other file systems, it will not work.

c) Turn off power to the base, remove the controller from the base, set Module Switch 4 to CLOSED position (and ensure Module Switch 2 is OPEN). Re-install the controller into the base, and restore power.

d) On power up, the controller enters **Port Parameter Setup** mode and displays **PPSt** on the front panel display. While in this mode, the web server can be accessed using the currently active IP address. However, the controller will not accept connections from ***Janus Workbench***.

e) Next, the controller will attempt to find the 'cti.ini' configuration file in the root directory of the front panel SD card.

- If cti.ini file is found, the file is then validated to ensure all the required data is included and correct.
- If the required keywords are found and validated, the procedure continues at step h below.

f) If any of the following errors occur, **PPEr** is displayed for 5 seconds indicating a **Port Parameterization Error** and the appropriate error (see below) is generated.

- If a properly formatted SD card is not inserted into the front panel receptacle:
  Error 370 (**Front Panel SD Card Not Accessible**) is reported.
- If the cti.ini file cannot be found in the SD card root folder:
  Error 250 (**Front Panel SD Card – Update File Not Found**) is reported.
- If the cti.ini file does not contain the required keywords/values:
  Error 260 (**Front Panel SD Card - Invalid Update File**) is reported.

g) If one of these errors exists, the firmware will repeatedly attempt to perform this operation as long as the controller remains in this mode. This allows you to insert (or modify and insert) an SD card without having to reset the controller. Each time you insert the SD card, the operations in steps (e-f) are repeated.

h) If the operation successfully completes, the parameterization data is saved for the next controller startup, the cti.ini file on the front panel SD card is renamed cti.bak, and **PPdn** indicating **Port Parameterization Done** is displayed on the front panel.

i) To return to normal operation, turn off power to the base, remove the controller from the base, set Module Switch 4 to the OPEN position, re-install the module into the base, and restore power.

j) On power up, the firmware performs subnet validation on the saved values. If they pass, those values are written into system parameter data. A 'Changed Network Settings' event is generated in the Event Log.

Web Server IP Address Configuration

Once your PC and the controller are on the same subnet, you can configure the IP address via the embedded web server.

- Access the embedded web server by typing the IP address of the controller into the URL box of your browser and pressing the ENTER key.
- Navigate to the CONFIGURATION/NETWORK SETTINGS page.
- Ensure the STATIC button is selected.
- For the Primary IP Subnet configuration, enter the parameters for the IPV4 Address, Subnet Mask, and Default Gateway
- Click on the APPLY button to accept the entries and initiate the update.

After the update is complete, the connection will be lost. To re-access the server, you will need to enter the new IP address in the browser URL box.

For additional details regarding network settings, see Section 4.2.

Other Controller Configuration Options

You may also use the embedded web server to configure other controller characteristics, including:

- **Startup and Alphanumeric Display Options -** See Section 4.1 General Settings.
- **Authentication and Encryption Options** – See Section 4.3 Security Settings,
- **Clock Setting or Time Synchronization Method** – See Section 4.4 Clock Settings.

CHAPTER 4 CONFIGURATION

The following parameters can be configured via the embedded web server:

4.1 General Settings

Navigate to the CONFIGURATION/GENERAL SETTINGS web page.

Module Identifier:
This is an optional text field that identifies the particular controller. If Enhanced Data Cache is configured, this name will be displayed in the CTI 2500 Series PLC Host controller scan statistics.

Operation following Module Reset:
This selection determines how the application program will execute on startup following a power cycle.

- **Restore Last State**: Restores application program to state it was in when power was lost. If the application was running, it will be set to RUN mode with Hot Start initialization so that all variables are set to their last value (default)
- **Application Stop:** All logic programs and fieldbus drivers stopped
- **Auto-Run Cold Start**: Starts application in RUN mode with all variables set to their initialization value
- **Auto-Run Warm Start**: Starts in RUN mode with RETAIN variables are set to their last value and all other variables are set to their initialization value
- **Auto-Run Hot Start**: Starts in RUN mode with all variables are set to their last value

NOTE: On startup following reset caused by pressing the front panel 'Clear Exception' button, the application program state is always set to 'RUNNING – Cold Start' unless the PLC Configuration for 'Operation following Reset' is set to 'Application Stop'.

Operation following Project Download from Workbench:

- **Application Stop**: All logic programs and fieldbus drivers are stopped
- **Logic Stop**: All logic programs are stopped, fieldbus drivers execute (default)
- **Run**: Application set to RUN mode – all logic programs and fieldbus drivers execute

Front Panel Display Items:

- Check box to Display Primary Network IP address on front Panel (default is Enabled)
- Check box to display configured Alternate Subnet IP addresses on front panel (default is Enabled)

Click on the APPLY button to apply settings. A confirmation message should be displayed indicating that the parameters have been updated. New parameters will go into effect immediately

NOTE

The "Display Alternate subnet IP addresses" option is available only when "Display Primary Network IP" is enabled.

.

4.2 Network Settings

Navigate to the CONFIGURATION/NETWORK SETTINGS web page. This page allows you to set the following parameters.

4.2.1 IP Parameters

The NETWORK SETTINGS page allows you to configure the Primary Subnet and up to three Alternate Subnets. Alternate Subnets allow you to communicate on additional IP subnets. It is not permitted to configure overlapping subnets or assign more than one IP address to a subnet.

The Primary subnet IP parameters can be automatically obtained by DHCP (Dynamic Host Configuration Protocol) or statically configured by entering the IP parameters. DHCP is not recommended for operational use, since it is possible to receive different IP addresses from DHCP over time. Alternate Subnets must be statically configured. See Alternate IP Subnets in APPENDIX C for more information.

4.2.2 DNS Configuration

It is possible to use DNS (Domain Name Service) to access a device (IP host) by name instead of IP address. This will usually require coordination with your IT department to obtain the IP addresses of the Preferred and Secondary (backup) DNS servers and the Domain Suffix.

If you want others to communicate with this controller by name, you will need to have a DNS entry in the DNS server for it. Similarly, any device you want to communicate with by name must have an entry in the DNS server. DNS settings for the Janus controller can be automatically read from the DNS server or manually entered.

4.2.3 Internal Ethernet Switch Configuration

By default, all Ethernet ports on the Janus controller are isolated from each other. Ethernet frames arriving at a port are not forwarded to other external (front panel) Ethernet ports. Frames are forwarded only between an external port and the controller microprocessor. This configuration protects against accidentally creating loops which can occur when there are multiple connections between two network switches. When connected to different networks, port isolation prevents broadcast and other traffic on each network from entering the other network(s). See Ethernet Port Operation in APPENDIX C for more information.

Since there may be some applications that require forwarding between networks, you can choose other options that allow forwarding in this web page.

4.3 Security Settings

Navigate to the CONFIGURATION/SECURITY SETTINGS web page

HTTP Basic Authentication:

- **No Authentication Required (default):** Select this method to allow free access to the web server and disable password access protection.
- **Allow only the following users**: This option enables password access protection to the web server. After selecting this option, you may enter a list of usernames and passwords. The following rules apply:
  - Password list may contain up to 16 entries.
  - Username can consist of 1 -16 characters and must be unique.
  - Password may consist of 1-16 characters.
  - The following characters may be used in a password:
    a-z A-Z 0-9, ~ @ % ^ _ + = { } [ ] : , . ? /
  - The following characters are excluded:
    # $ & * ( ) - \ | ; ‘ “ < >

NOTE

If enabled, password entry is required to access any CONFIGURATION or CUSTOM HTML (GRAPHICS) page. Once the password is authenticated, the user can access all web pages with re-entering the password until the web browser is closed.

NOTE

If the passwords are forgotten, there is not an administrative (backdoor) method of discovering them. You need to clear all passwords by resetting the configuration settings. See Section 5.3.

HTTPS Encryption

Check this box if you wish to encrypt the transmission between the browser and the web server. The Secure SSL (Secure Sockets Layer) protocol, supported by all modern browsers, is used to connect to the web page. This protocol encrypts all data transmitted between the PC browser and Janus controller including username and password data required to make the connection.

When using HTTPS encryption, the user must accept a security exception the first time a web browser attempts to connect to the web server. This is required because trusted SSL certificates cannot be issued for hosts with changeable IP addresses – as is the case with the Janus controller.

Click on the **APPLY** button to apply settings. A confirmation message should be displayed indicating that the controller must be reset in order to update the configuration parameters. You must acknowledge this message to continue.

4.4 Clock Settings

Navigate to the CONFIGURATION/ CLOCK SETTINGS web page

Set or Synch Time Method:

- **Set Current Time:** Sets clock via manual entry of the time and date and/or use of CTI_PLC_SET_RTC function block in a logic program
- **Use Remote NTP Server:** Obtains the time from an NTP (Network Time Protocol) server.
- **Use Data Cache Client Host:** Sets clock with time read from the CTI 2500 Series Host PLC – requires use of the Enhanced Data Cache fieldbus protocol.

Date / Time: If manually setting the time, you should enter the time and date in these boxes.

The following entries are required only when **Use Remote NTP Server** is selected:

- **Time Zone Region:** Select the region of the time zone.
  For example, in the U.S you would select “Americas”.
- **Time Zone Cities:** Select a city or area in your time zone.
  For example, in the Eastern Time zone, you might select New York.
- **Host IP Address:** Enter IP Address of the network device acting as NTP Server

Click on the **APPLY** button to update settings. An error message will be displayed if there is a problem with your entries. Otherwise, a confirmation message will be displayed indicating that the parameters have been updated. New parameters will go into effect immediately.

CHAPTER 5 OPERATION

This section describes aspects of the Janus Controller operation. Additional information may be found in the ***Janus Workbench*** Help.

5.1 Controller Operation Overview

1. The Janus controller can have the following operational states:
   - **APPLICATION STOP:** Application is halted. All fieldbus protocols and logic are stopped.
   - **RUN (*Janus Workbench displays "RUNNING"):*** All facets of the application operation are active - all configured fieldbus protocols and logic program are executing.
   - **LOGIC STOP:** Application is active. Logic processing is stopped and controlled via the debug "step" operations. Fieldbus protocols are running and the data base is updated.
   - **ERROR:** Application is halted. All fieldbus drivers are stopped. The controller must be rebooted or operation mode changed to **Application Stop** before it can return to RUN state. Alternatively, you can use the **CLEAR EXCEPTION** button (if enabled) to exit **ERROR** state. See Section 2.8 Clear Exception Pushbutton.
2. ***Janus Workbench*** can be used to transfer controller operation from **APPLICATION STOP** to **RUN** mode with the following initialization states:
   - **Cold Start:** All variables are set to their initialization values.
   - **Warm Start:** RETAIN variables are set to their last values, and all other variables are set to their initialization values.
   - **Hot Start:** All variables, instance data, timers, and SFC states are restored to their last values.

   Warm Start and **Hot Start** options are not available immediately after an application is downloaded from ***Janus Workbench*** to the controller.
3. Controller programs can be compiled for *Debug* or *Release* operation.
   - **Debug:** Allows remote debugging of the application program while executing on the target. This includes use of breakpoints, trace points, cycle-to-cycle debug, and step-by-step debug operations.
   - **Release:** Version compiled for faster execution without support for debugging operations. *Release* version will typically execute approximately 10% faster than the corresponding *Debug* version.
4. **RETAIN** variables are special designated Global variables whose latest value is saved to the internal SD card at the end of every scan cycle. There is no limit on the number of variables you can designate as **RETAIN**. This provides following user options:
   - Stored values can be used as "initialization values" for specified variables when application is started using the **Warm Start** option.
   - You can save or restore values of all **RETAIN** variables on demand thru the use of the F_SAVERETAIN and F_LOADRETAIN function blocks.

5. The controller data base is saved to the internal SD card when power is lost, providing an option to execute a **Hot Start** where all variables are set to their last state value.
6. All user data files created by user logic programs will be stored on the internal SD card in the /ctiplc/user folder. To access them externally, the user must manually transfer these files to the front panel SD card using the FILE MANAGEMENT web page.
7. When a project is downloaded from CTI Workbench while the run-time is stopped, that project is stored on the internal SD card as the "active" application. All project source files are downloaded with the program, and they are also copied to the appropriate folder on the internal SD card. The previous program and source files (if they exist) are renamed and saved. Any older versions are overwritten.

   The state of the application program following download is determined by selection **for Operation following Project Download** in CONFIGURATION/GENERAL SETTINGS web page. The application remains in this state until user changes the program state or the controller is reset.
8. The controller includes a predefined **Cycle Instruction Overrun** watchdog to prevent the user program from excessively looping without completing a normal cycle. This watchdog uses a software timer to measure each controller cycle and limits maximum cycle time to one (1) second.
9. The controller firmware also includes a **System Watchdog** with preset of 6 seconds that expires only if the controller operating system becomes inoperable. The expiration of the System Watchdog will cause the Janus controller to reboot.
10. If a controller execution error is detected, the event is recorded in the Event Log and controller will enter the **ERROR** state. **ERROR** state can be cleared by connecting Workbench to the controller or by resetting the controller via web page or **CLEAR EXCEPTION** button (if either is enabled).

NOTE

Logic can be added to the Exception Programs (pOnBadIndex and pOnDivZero) for special handling of these error conditions.

If the CLEAR EXCEPTION button is enabled, it can be used to reset the controllers after critical errors. See Section 2.6 for details.

5.2 Controller Startup

This section describes the sequence of events that occur during a power-on startup or after a controller reset.

NOTE

All CTI boot files are encrypted to provide protection against malicious code by ensuring that only CTI authorized firmware is loaded

1) The yellow ERROR LED is set ON by hardware when power is applied to the controller. This provides indication that the controller is powered and attempting to decrypt and load the contents of the boot.bin file on the internal SD card. If the SD card is missing, or the SD card does not contain a boot.bin file, or the encryption setting or key is invalid, startup is halted and the error LED will remain on. Also note that the INTERNAL SD card must be formatted as FAT32 (only the EXTERNAL SD card supports EXFAT)
2) If step 1 is successful, the controller starts a 'Secure boot' process. Each component of the image file (boot manager, operating system, controller execution engine, FPGA system, firmware drivers, etc.) is checked for authenticity using the encryption key. If verified, the boot is initiated. Otherwise startup is halted and the ERROR LED remains on.
3) At the beginning of the boot process, the ERROR LED is turned OFF and a scrolling decimal point appears on the Alphanumeric Display, indicating the operating system and execution engine are booting. *If the animation continues for more than 30 seconds, this indicates a boot error.*
4) When the operating system is running, the firmware version number is displayed on the front panel Alphanumeric Display in "X.YY" format where "X" is major revision and "YY" is minor revision. This number remains displayed for two (2) seconds, and then is replaced by the IP Address/Subnet and/or Error Codes as specified in the CONFIGURATION/GENERAL SETTINGS web page.

   NOTE: T*he following applies to Janus controllers with firmware version 1.20 or greater.* By default, if an IP address has not been set by other means, a link local IP address, which is automatically created at startup, will be displayed with a prefix of "AIP". This IP address, which is not routable, can be used as a temporary IP address until other IP assignment methods are configured. You can cause the Auto-IP address to always be displayed by selecting the "Always Display Auto-IP' option in the CONFIGURATION/GENERAL SETTINGS web page.

   If an error code is displayed, you can determine the cause by referencing APPENDIX A: SYSTEM ERROR CODES in this manual or accessing the ERROR DESCRIPTIONS & STATUS web page.
5) Application state is then set to the state specified in the General/Configuration web page Startup Options.

5.3 Clear Exception Pushbutton Operation

When enabled, the **CLEAR EXCEPTION** pushbutton provides a direct method to clear exceptions, reset controller configuration values to default values, or restore factory defaults without requiring access to ***Janus Workbench*** or the controller web server. In cases where the user selected password(s) for web server access is lost, this is the only method that can used to clear existing passwords. No universal or developer-embedded "back door" password is allowed in the system. All pushbutton operations are logged in the controller event log. The CLEAR EXCEPTION pushbutton will function only when Switch 3 is in the CLOSED (ON) position.

The following actions may be initiated by depressing the **CLEAR EXCEPTION** button:

- **CLEAR EXCEPTION**

  Pressing and holding the recessed pushbutton for greater than 5 seconds causes the Janus controller to reset and return to normal operation following a System Exception.

  When the button is pressed for one second, the front panel display shows countdown for 'seconds to controller reset' (4-1). If the pushbutton is released any time during this period, the operation is aborted. If the button remains pressed until the countdown reaches zero, the display changes to **rE (**indicating pending reset). Releasing the button at this time initiates the controller reset.

  If the controller is in **RUN** or **LOGIC STOP** state when the **CLEAR EXCEPTION** event is detected, the application must be halted before the reset is triggered.

  The controller startup operation following the reset is specified by **Operation following Module Reset** setting in CONFIGURATION/GENERAL SETTINGS page of the web server. See Section 4.1 General Settings.

- **RESET CONFIGURATION SETTINGS**

  Pressing and holding recessed pushbutton for greater than 10 seconds causes the controller to reset, returning all configuration settings to their default settings.

  The following settings are reset by this action:

  - Startup Mode
  - Alphanumeric Display Options
  - Method for Setting IP Address
  - IP Address / Subnet Mask (all configured)
  - Web Server Password Protection Enable and associated Username/Password List
  - PLC Clock Time Set / Sync Method and associated settings

  After the button is pressed and held for 5 seconds, the display will show **rE** (see **CLEAR EXCEPTION** description above). If the button press is maintained for another second, the front panel display shows countdown for 'seconds to **CONFIGURATION RESET'** (4-1). If the pushbutton is released any time during this period until countdown reaches zero, the button press is treated as a **CLEAR EXCEPTION** event as described above.

  If the button press is held until the **CONFIGURATION RESET** countdown completes, the display changes to **Cr** (indicating pending **CONFIGURATION RESET**). Releasing the button at this time initiates the **CONFIGURATION RESET** event.

  If the controller is in **RUN** or **LOGIC STOP** state when the **CONFIGURATION RESET** event is detected, the application will be halted and operational data stored (equivalent to ending the application from Workbench) before the reset is triggered.

When the application is stopped, all PLC configuration settings (as reported on the PLC Configuration web pages) are restored to default values.

The controller is then reset, and the controller remains stopped on the subsequent startup.

- **RESTORE FACTORY DEFAULTS**

  Pressing and holding the recessed pushbutton for greater than 15 seconds causes the controller to return to as-shipped factory defaults by pressing the button for greater than 15 seconds. This action will reset all PLC configuration settings to default (see list in **RESET CONFIGURATION SETTINGS** section above) and delete all user files including application programs and source files from the internal SD card.

  After the button is pressed and held for 10 seconds, the display shows **Cr** (see **RESET CONFIGURATION SETTINGS** description above). If the button press is maintained for another second, the front panel display shows countdown for 'seconds to Factory Reset' (4-1). If the pushbutton is released any time during this period until countdown reaches zero, the button press is treated as a **RESET CONFIGURATION** event as described above.

  If the button press is held until the **FACTORY RESET** countdown completes, the display changes to **Fr** (indicating pending **FACTORY RESET**) and displays this value until the button is released or power is removed. Releasing the button when **Fr** is displayed initiates a **FACTORY RESET** event.

  If the controller is in **RUN** or **LOGIC STOP** state when the **FACTORY RESET** event is detected, the application will be halted and operational data stored (equivalent to stopping the application from Workbench) before the reset is triggered.

5.4 HTTP Data Server

The Janus controller includes an HTML Data Server that provides an embedded HMI function. Using the Data Server, you can access "live" controller variable data using any recent version of a standard web browser (Microsoft Edge, Internet Explorer 11, Mozilla Firefox, or Google Chrome) on any PC or internet-capable smart device. Variable data is constantly updated from the controller database. Read/write services allow you to modify variables values from the web page based on a user-designed graphics page configuration. You have complete control over which PLC control variables are accessible via the web browser. See the ***Janus Workbench*** help system for information regarding configuration and use of the Data Server.

Access to the Data Server can be controlled via Username/Password set in the controller web server CONFIGURATION/ NETWORK SETTINGS page. If you wish to encrypt the communications between the web server and the Janus controller, secure (https:) connections can optionally be selected (see Section 4.3 Security Settings.

CHAPTER 6 UPDATING FIRMWARE

6.1 Overview

The Janus controller stores the operating firmware in non-volatile flash memory. You can replace the current operating firmware with a different version to correct problems or add new features.

Prior to updating firmware, you will need to obtain a firmware update file for the Janus controller. This file can be downloaded from the CTI website http://www.controltechnology.com/downloads/. After obtaining this file, you should save it to a file on your PC or on an accessible network drive.

The firmware update process is a three-step operation consisting of the following steps:

1) Verification of an encrypted firmware file to ensure the file contains only "trusted executables" before it is installed on the Janus controller
2) Extraction of OS/firmware file,
3) Copy of the OS/firmware file to the root folder of the internal SD card where it will execute after the next module reset.

There are three methods for updating firmware. They are described in the following sections.

6.2 Front Panel SD Card Firmware Update

The procedure requires the following steps:

1) Copy the new firmware file downloaded from CTI website to root directory of a SD card and insert that card into the front panel SD card slot. The firmware file can be a compressed zip file or binary file (boot.bin) extracted from the zip file.
2) Turn off power to the chassis, remove the PLC, set Module Switch 2 to CLOSED position, ensure Module Switch 4 is OPEN, re-install the module into the chassis, and restore power to the chassis.
3) The controller attempts to find the firmware file in the root directory of the front panel SD card.
4) If any of the following errors occur, UF**Er** indicating **Firmware Update Error** is displayed and the appropriate error code (see below) is generated.
   - If a properly formatted SD card is not inserted into the front panel receptacle:
     Error 370 (**Front Panel SD Card Not Accessible**) is reported.
   - If file with '.zip' extension or file named 'boot.bin' cannot be found in the SD card root folder:
     Error 250 (**Front Panel SD Card – Update File Not found**) is reported.
   - If the update file is found but not valid for controller product/ model:
     Error 260 (**Front Panel SD Card - Invalid Update File**) is reported.

   If one of these errors exists, the firmware will repeatedly attempt to perform this operation as long as the controller remains in this mode. This allows you to insert (or modify and insert) an SD card without having to reset the controller. Each time you insert the SD card, the operations in steps 3-4 are repeated.
5) If the firmware file is found and validated, **UFdn** is displayed on the front panel to indicate success. This action is also reported in the Event Log.

6) Repeat step (2) above except set Module Switch 2 to OPEN position to return to normal operation**.**

6.3 Remote Firmware Update

The ***Remote Firmware Update*** method allows the PLC firmware to be updated via network connection to web server. Remote firmware update consists of the following steps:

1) Ensure that Switch 1 is set to the CLOSED Position to enable *Remote Firmware Update*.

2) Use a web browser to access PLC web server and select **Firmware Update** web page. Username/Password authentication is required to access this page if enabled.

3) When firmware update is initiated, the controller operational mode is checked. To update firmware, the controller must be in **APPLICATION STOP** mode.
   - If the application is in **RUN**, **LOGIC STOP**, or **ERROR**, a status message will be displayed informing you that authorization to halt PLC application is required. You can authorize this action by checking the acknowledgement checkbox. After doing so, a status message will inform you that you can proceed with the firmware update.
   - If the application is stopped (**Application Stop**), you can proceed with the firmware update. A status message will be displayed informing you that the controller is ready for firmware update.

NOTE

The [Refresh] button can be pressed at any time to recheck PLC operational mode and update the controller status. If [Refresh] is pressed after the warning message is acknowledged, the acknowledgement checkbox and status message is cleared and updated based on the current Controller operational state.

4) Select the firmware file to download to the controller by pressing the [**BROWSE**] button. The selected file can be a zip file – normally named CTI_JANUS_PAC_Vnn_nn.zip or uncompressed binary file (boot.bin).

5) After the firmware file is selected, press the [**UPDATE FIRMWARE**] button to initiate the firmware update or cancel the operation by leaving the webpage (either close browser window or view a different webpage).

NOTE

If [UPDATE FIRMWARE] is selected, the Remote Firmware Update operation must run to completion (Success or Error). The controller must remain powered and operational throughout this process.
See Section 6.4 Direct File Replacement for recovery options if power is lost during the firmware update operation.

6) If file download fails for any reason, Error Code 250 (**Update File Not Found**) is generated and error message is displayed in the Status window of the web page.

7) If the file download succeeds, the firmware file is copied to a temporary folder on the SD card and validated to ensure it is for proper product/model. If the file validation fails, the firmware update is terminated. Error Code 260 ('Invalid Update File') is generated, and error message is displayed in the Status window on web page.

8) If the validation succeeds, the web page status message is updated to indicate the **Firmware Update is complete and controller is rebooting**. This action is also reported in the Event Log.

9) The controller then resets to complete the operation and restarts using the updated firmware.

During the controller reset, the browser connection to the web server is lost. A new connection to the web server is required to verify the updated firmware is operational. This can be accomplished by pressing the [REFRESH] button on the web page or the 'Reload current page' button on the browser.

NOTE

If the web page is reloaded via the [REFRESH] button or browser 'Reload' button while the controller is still rebooting, the browser may reroute the user to a 'Connection timed out' page. In that case you must use the 'Reload'' button on the browser to reload the ***Firmware Update*** *web page.*

6.4 Direct File Replacement

The Direct Firmware File Replacement method is provided as a means to recover from a failed firmware update, or missing / corrupted SD card. Since the controller is not operational, neither of the traditional methods for updating firmware can be used.

1) Unzip the compressed firmware file downloaded from CTI website (CTI_JANUS_PAC_Vnn_nn.zip) to extract the boot.bin binary file.
2) Copy the boot.bin file to the root directory of a SD card. No other files are required.
3) Turn off power to the base, remove the controller, and insert the SD card containing the boot.bin file into the internal SD card slot (see Section 3.2.2).
4) Ensure Module Switch 2 and Switch 4 are in the OPEN position.
5) Reinstall the controller and restore power to the base.
6) The controller should start up as described in Section 5.2.

CHAPTER 7 LEGACY I/O SUPPORT

7.1 RS-485 I/O Support

The CTI Janus controller supports CTI 2500 2500® Series I/O, Siemens Series 505® I/O and Siemens Series 500® I/O products.

7.1.1 CTI 2500 Series I/O Support

The Janus controller supports all current CTI 2500 Series® discrete and analog I/O modules. Both CTI 2500 Series Classic I/O modules and CTI 2500 Series Compact I/O modules are supported. When using the Janus 2500P-Jxxx controller, Classic I/O modules can be installed in the same base as the Janus controller or installed in a remote base connected to the controller via an RS-485 cable. Compact I/O modules must be installed in a Compact remote base.

CTI 2500 Series Special Function modules are currently not supported. However, due to the enhanced communication capabilities of the Janus controller, Ethernet-based special function modules are no longer necessary.

The controller can communicate with the following CTI 2500 Series Remote Base Controllers:

- CTI 2500-RIO-A and 2500-RIO-B remote base controllers (Classic)
- CTI 2500C-RBC-485 remote base controllers (Compact).

7.1.2 Siemens 505 and Series 500 I/O Support

The CTI Janus controller supports most current Siemens Series 505 discrete and analog I/O modules. Special function modules are not supported. The CTI Janus controller also supports designated Siemens Series 500 discrete and analog I/O modules. ***Janus Workbench*** will present a list of supported modules during configuration.

The controller can communicate with the following Siemens series 505 remote base controllers:

- 505-6851 and 505-6851A (RS-485)
- 505-6850 and 505-6850A (Coax)

When using SIMATIC 505-6850 or 505-6850A remote base controllers, you must attach the RBC to the Janus controller using a Siemens SIMATIC 505-6860 I/O Channel Converter.

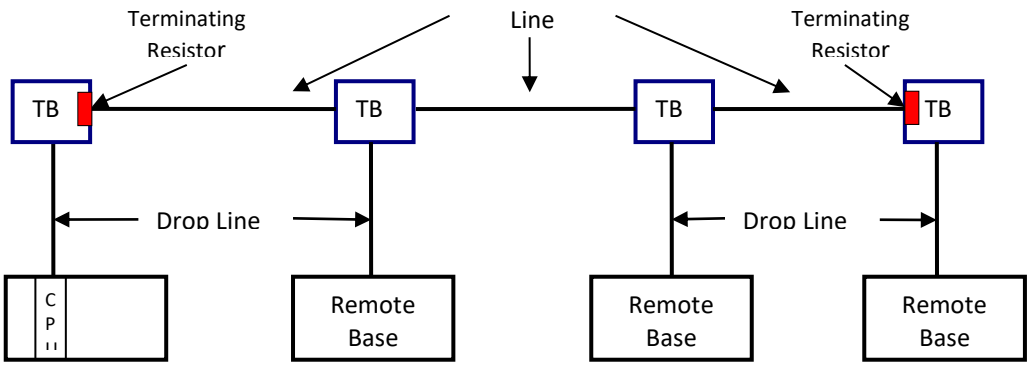
The CTI controller will communicate with Siemens Series 500® I/O installed in a remote base using the following Remote Base Controllers:

- 500-5114 and 500-5114A (RS-485)
- 500-2114 and 500-2114A (Coaxial)

When using a 500-2114 or 500-2114A, you must attach the RBC to the CTI Janus controller using a Siemens 505-6860 I/O Channel Converter.

7.1.3 Connecting to Remote I/O

Remote I/O is connected to the CTI Janus controller via RS-485 cable. Cabling is typically connected in a trunk line/ drop line arrangement as shown below.



TB = Terminal Block

Cable Selection

The following cables (or equivalent) are acceptable for use for remote I/O connections.

Belden Cable Type	Outside Diameter	Impedance	Capacitance	Velocity	Center Conductor
9182	0.35 in. 8.9 mm	150 ohms	28.9 pf/m	0.78c	22 AWG 19x34 46 ohm/km
9271	0.24 in 6.1 mm	124 ohms	40 pf/m	0.66c	25 AWG 7x33 104.3 ohm/km
9860	0.44 in. 11.2.mm	124 ohms	35.8 pf/m	0.78c	16 AWG Solid 13.8.ohm/km

Belden 9182 is suitable for intermediate length trunk lines. This cable cannot be intermixed with other cables for trunk lines. In addition, if this cable is used for a trunk line, it must also be used for all drop lines. It may also be used for drop lines with Belden 9860 or Belden 9271 trunk lines.

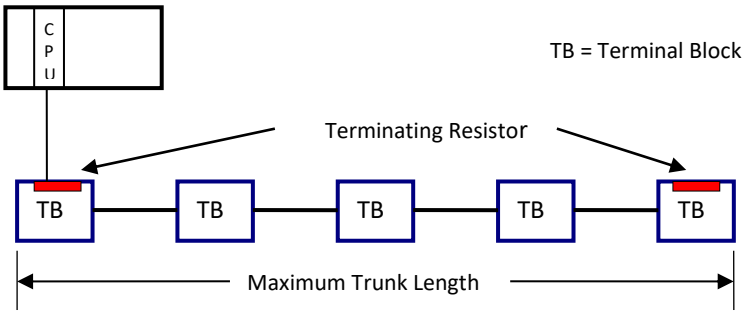
Belden 9271, which is smaller and more flexible, is suitable for use as drop lines as well as short trunk lines. For trunk lines, this cable may be intermixed with Belden 9860.

Belden 9860 cable, which provides low attenuation and distortion, should be used for long trunk lines.

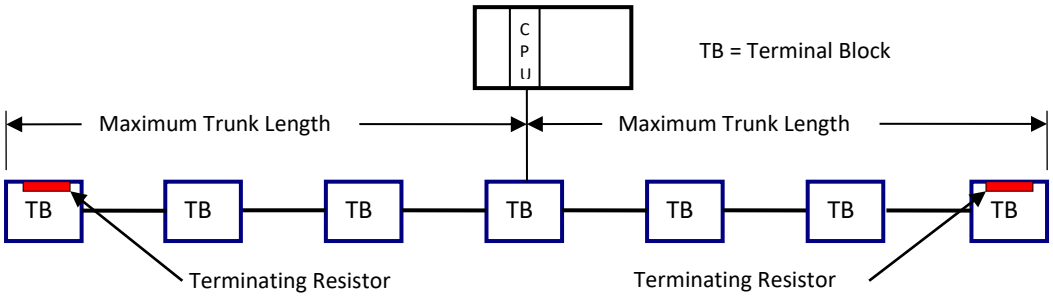
When wiring the cable connectors, see Section 2.9 for the port pinout.

Cable Length and Termination

For each cable type, there is a maximum cable length. As the figure below indicates, the maximum cable length is measured from the CPU to the most distant tap. Note that a terminating resistor **must** be installed on the end terminal blocks.



The maximum trunk length can be doubled by using a "T" topology as show below. Note the location of the terminating resistors.

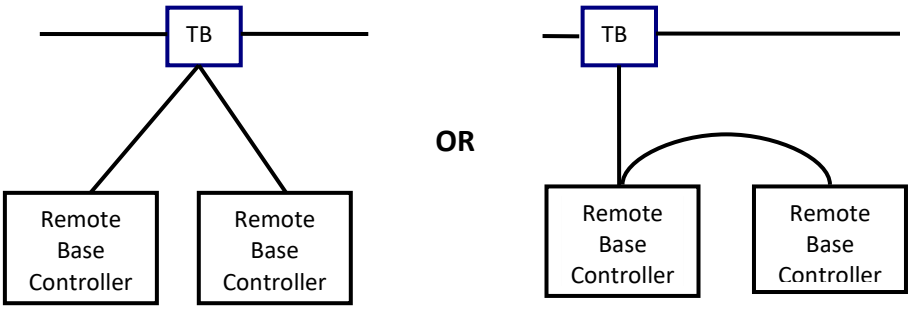


The following table designates the maximum trunk lengths for each cable type.

Number of Terminal Blocks	Maximum Distance		
	Belden 9182	**Belden 9271**	**Belden 9860**
2 - 5	2200 ft (670 m)	1100 ft (335 m)	3300 ft (1006 m)
6	2133 ft (650 m)	1067 ft (325 m)	3200 ft (975 m)
7	2067 ft (630 m)	1033 ft (315 m)	3100 ft (945 m)
8	2000 ft (610 m)	1000 ft (305 m)	3000 ft (914 m)
9	1933 ft (589 m)	967 ft (295 m)	2900 ft (884 m)
10	1827 ft (569 m)	933 ft (284 m)	2800 ft (853 m)
11	1800 ft (548 m)	900 ft (274 m)	2700 ft (823 m)
12	1733 ft (528 m)	867 ft (264 m)	2600 ft (792 m)
13	1677 ft (508 m)	833 ft (254 m)	2500 ft (762 m)
14	1600 ft (488 m)	800 ft (244 m)	2400 ft (732 m)
15	1533 ft (476 m)	767 ft (234 m)	2300 ft (701 m)
16	1400 ft (427 m)	733 ft (223 m)	2200 ft (671 m)

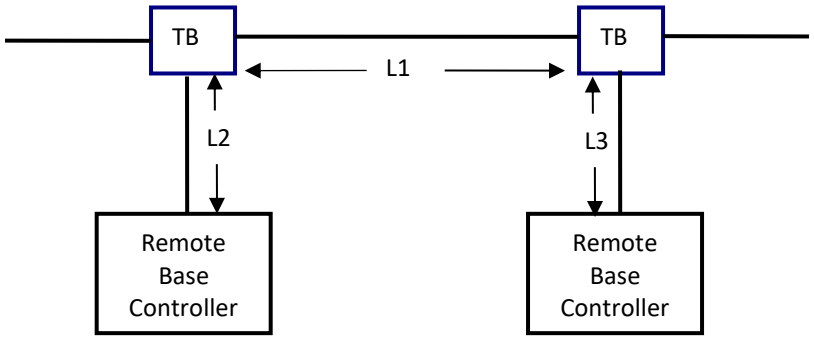
Other Topology Considerations

When multiple connections are required in close proximity, you should connect the equipment to a single terminal block instead of dedicating a terminal block to each connection. See the figure below for connection options.



TB = Terminal Block

Terminal Block connections to the trunk line should be spaced so that the total length of the trunk line separating the taps is greater than the sum of the drop line lengths at the taps. In the illustration below, L1 should be greater than the sum of L2 + L3.



Termination Resistors

Termination resistors must be installed at the ends of the trunk line. The resistor value required depends on the trunk cable as specified in the table below

.

Cable Type	Resistor Value
Belden 9182	150 ohms, 5%, ¼ W
Belden® 9860 or 9271	120 ohms, 5%, ¼ W

7.1.4 Dual RBC Support

The Janus controller supports dual Remote Base Controller (RBC) configurations using an RS-485 network. Coaxial dual media cabling is not supported.

A dual RBC configuration consists of two remote base controllers installed in a special base (CTI 2500-R11-A or Siemens 505-6511). These bases also support the installation of dual power supplies, providing redundant sources of power.

The dual RBC configuration provides redundant control of the I/O base. When power is applied to the base (and two RBCs are installed and operational), the RBC in the rightmost controller slot assumes the role of the active RBC, reading and writing the base I/O. The other RBC assumes the standby role, responding to status requests from the 2500 Series controller, but not accessing the base I/O.

When a dual RBC configuration is detected, the Janus controller continuously monitors the status of the status of both RBCs. If a problem is detected with the standby RBC, the 2500 Series controller will disable it. Should the controller detect a problem with the active RBC while the standby RBC is operational, it will direct the standby RBC to assume the role of active RBC and disable the previously active RBC.

The standby RBC, if operational, also monitors the condition of the active RBC. If the standby RBC detects a problem with the active RBC it will automatically assume the role of the active RBC and will disable the previously active RBC. RBC status is reported to the Remote I/O fieldbus driver.

An RBC that has been disabled can be re-enabled by temporarily changing the address switch to a different address then changing it back to the original address. Alternately, the RBC can be re-enabled by cycling power to the base.

Using ***Janus Workbench***, you can manually direct the RBCs to swap roles (if the standby RBC is operational). This capability is especially useful when executing diagnostic routines on an RBC, since diagnostic routines are always run on the standby RBC in dual RBC configurations.

RS-485 cabling to the dual remote base controllers must comply with the cabling and topology standards described in Section 7.1.3. See *Other Topology Considerations* within this section for typical dual RBC connections.

NOTE

*You can use a CTI 2500-RIO-A (firmware version 7.03 or higher, CTI 2500-RIO-B, or Siemens 505-6851-B remote base controller in a dual RBC configuration. However, you **cannot** intermix CTI and Siemens RBCs in the same base.*

7.1.5 Configuring Local and Remote I/O

Local and Remote I/O can be configured using ***Janus Workbench***. See the Workbench help system for compete information regarding configuration and I/O support.

7.2 Profibus DP I/O

The CTI Janus controller supports Profibus DP I/O devices that comply with the Profibus DPV1 standard. The following Remote Base Controllers can be used to allow CTI 2500 modules or Siemens SIMATIC Series 505® modules to be used on the Profibus network:

- CTI 2500-RBC Profibus Remote Base Controller
- Siemens SIMATIC® 505-6870 Profibus Remote Base controller.

The CTI Janus controller can communicate with up to 64 Profibus slave devices, reading up to 244 bytes per slave and writing up to 244 bytes per slave. The controller supports modular slaves with up to 128 modules per slave. Profibus network baud rates up to 12Mb are supported. See ***Janus Workbench*** help for additional details.

NOTE

The actual amount of data that can be exchanged with a slave is dependent on the capability of the slave. The total amount of data that can be exchanged is limited by the I/O capability of the controller model. Network data rates may be limited by the network configuration.

7.2.1 Connecting to the Profibus Network

Cable Selection

The Profibus network attaches to the Profibus DP connector on the front panel of the CTI Janus controller using shielded twisted pair cable. See Section 2.8 for a pinout diagram of the connector.
The following table specifies the characteristics of the cable.

Characteristic	Requirement
Impedance	135 – 165 ohms (3 – 20Mhz)
Capacitance	< 30pF/m
Resistance	<110 Ω/km
Conductor Area	0.34mm2 (22 AWG)
Cable Diameter	0.34 mm

The following cables meet the Profibus DP cable specifications:

- Belden 3079A
- Belden 3079E (Hi-Flex)

The cable incorporates two color coded wires (red and green) surrounded by a shield. One wire is used for Transmit/Receive+ (TX/RX +) and the other for Transmit/Receive (TX/RX -). The color used to connect to TX/RX+ is arbitrary; however, the same color must be used throughout the system. Do not cross the TX/RX + and TX/RX – signals.

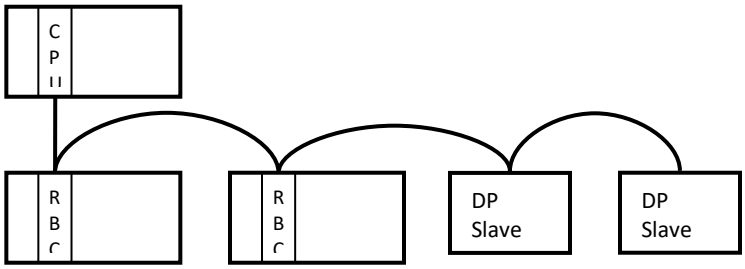
Profibus Connector

A special DB 9 connector is recommended for all Profibus DP installations.

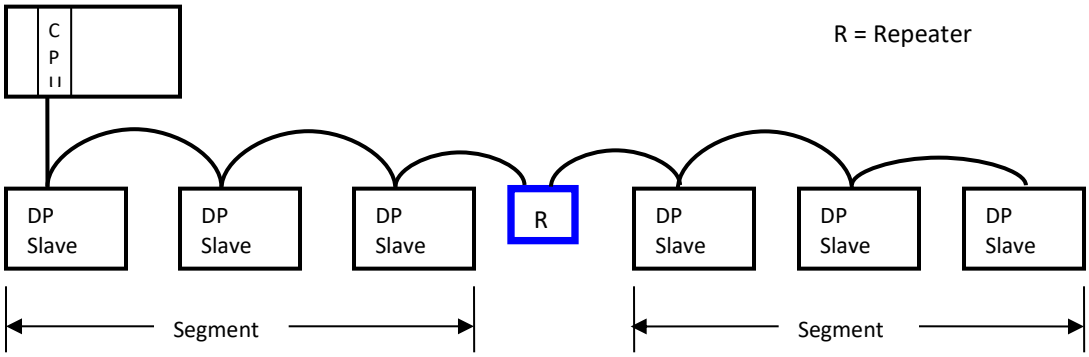
Connector such as the one pictured above, provide either snap-in or screw terminal termination, horizontal cable connection, and switchable termination. Connectors such as these are commonly available from your distributor or other industrial suppliers.

Profibus Topology

The Janus Controller supports up to 64 Profibus slave devices.
Profibus slave devices are connected in a “daisy chain” arrangement as indicated in the following illustration.



Up to 32 devices can be connected on a single segment. To increase distance or the number of devices supported, segments can be interconnected by using repeaters. Up to 10 segments may be connected together.



Cable Distance

Cable distance depends upon the baud rate being used. See the following table.

Baud Rate	Segment Distance	Total Distance (All Segments)
9.6 – 93.75 Kb	1,200 m (3,930 ft)	12,000 m (39,300 ft)
187.5 Kb	1,000 m (3, 280 ft)	10,000 m (32,800 ft)
500 Kb	400 m (1,310 ft)	4,000 m (13,100 ft)
1.5 Mb	200 m (660 ft)	2,000 m (6,600 ft)
3 to 12 Mb *	100 m (330 ft)	1,000 m (3,300 ft)

* Baud rates greater than 1.5 Mb require special connectors and repeaters.

7.2.2 Configuring a Profibus DP Network

The Profibus DP network is configured using ***Janus Workbench***. See the ***Janus Workbench*** help for a complete description of the configuration and operation of the Profibus network.

CHAPTER 8 EMBEDDED WEB SERVER

The product embedded web server displays information about the operation of the Janus controller and provides a means to configure product operation. The web pages are described in the following sections.

8.1 Product Information

This page provides information about the controller

- **Product Number**
- **Product Name**
- **Serial Number**
- **Manufacture Date**
- **Module Identifier:** Assigned by user in General Settings page
- **Hardware Configuration: D**esignator that allows software to determine hardware compatibility
- **Firmware Version**
- **Firmware Date**
- **FPGA Version**
- **Build Information 1 & 2:** (CTI development and support information)
- **Clock Synchronization Mode**: Determines how the controller clock is set)
- **Startup Mode**: Determines how the controller starts up when reset or powered up
- **Front Panel SD Card Status**: If inserted, displays Utilization Percentage
- **DNS (Domain Name Service) Address Method** (Auto/Manual)
- **Primary DNS Server IP Address**
- **Secondary DNS Server IP Address**
- **Domain suffix**
- H**TTPS Basic Authentication Enabled:** Authentication for webserver access
- **HTTPS Encryption Enabled:** Encryption of web server traffic
- **Ethernet MAC Address**
- **Internal Switch Mode**
- **CPU Temperature (° C)**
- **Dipswitch Settings**
- **User Jumper Selections**
- **Network Settings: For Primary and Alternate subnets**

8.2 Application Information

This page contains information about the current application.

- **Project Name/Compile Version**
- **Project Compile Timestamp**
- **CTI Workbench Compiler Version**
- **Session Number:** Session ID of the current session
- **Current Operational Mode**: (APPLICATION STOP / LOGIC STOP/ RUN / ERROR)
- **Active Error Codes**: See Error Descriptions and Status web page description for details.
- **System Resources:** Displays memory, file and socket utilization for the operating system.
- **Product Resources:** Displays memory, file, and socket utilization for the product.
- **Components Configured:** Indicates configuration status of fieldbus drivers and other facilities.
- **Component Errors:** Indicates components that are in an error state.
- **Non-configurable System Element Errors:** Indicates elements that are in an error state.
- **Locked Variables:** Lists variables that are locked (forced).

8.3 Configuration

8.3.1 General Settings

This page contains settings that apply to the general operation of the controller.

- **Module Identifier** - Optional 16-character text field used to identify the controller
- **Operation following Module Reset**
  - Restore Last State (Default)
  - Application Stop
  - Auto-Run Cold Start,
  - Auto-Run Warm Start
  - Auto-Run Hot Start
- **Operation following Project Download from Janus Workbench**
  - Application Stop - Logic programs and fieldbuses are stopped
  - Logic Stop – Logic programs stopped/ Fieldbuses execute (Default)
  - Run – Logic programs and fieldbuses execute
- **Front Panel Display Items**
  - Display Primary Network IP on Front Panel: Displays the Primary IP Address when enabled.
  - Display Subnet IP's on Front Panel: Displays IP address of configured alternate subnets when enabled.
  - Always Display Auto-IP on Front Panel: Always displays the automatically created IP address when enabled. *When not enabled, the Auto-IP address is displayed only when the controller IP address is not set by other methods.*

The new parameters go into effect immediately after clicking the APPLY button and confirming the action.

NOTE: If both display options are disabled, the front panel alphanumeric display will be blank when no error conditions are active.

8.3.2 Network Settings

This page sets the IP parameters for the controller and configures how the embedded switch forwards Ethernet frames.

- **Primary Subnet Configuration** (configuration is required)
    - Automatic (DHCP): Designates that IP parameters will be assigned using DHCP (Dynamic Host Configuration Protocol)
    - Static: IP parameters will be entered in the boxes below
- **Alternate Subnet Configuration** enables the controller to communicate on additional IP subnets. Each subnet must be unique. Subnet configurations that overlap other configured subnets will be rejected. See Appendix C for more information.
- **Internal Ethernet Switch Configuration.** Allows you to configure how Ethernet frames will be forwarded among the front panel Ethernet ports. See Appendix C for additional information.

New configurations go into effect immediately after clicking on the APPLY button and confirming the action.

8.3.3 Security Settings

This page sets the security requirements for access to the following web pages: Configuration, File Management, Firmware Update, and Custom HTML (graphics) web pages.

- **HTTP Basic Authentication** (Web Server Password Protection)
    - No Authentication Required (Disables Password Protection)
    - Allow only the following users (Enables Password Verification)
      If selected, allows user to create 'Password List' containing up to 16 entries. Each entry consists of a unique Username (1-16 characters) and password (1-16 characters. The following characters may be used in password: `a-z A-Z 0-9 ~ @ % ^ _ + = { } [ ] : , . ? /.`
- **HTTPS Encryption:** Encrypts the communications with the web server when the box is checked..
  Checkbox to 'Use HTTPS Encryption' when selected (Default = Disabled)

When [APPLY] button is pressed, the updated configuration parameters are saved to the database and a confirmation message is displayed.

8.3.4 Clock Settings

Determines how the controller clock is set

- **Set Current Time** – Enables manual entry of the date and time.
  - Date (in YYYY-MM-DD format)
  - Local Time (formatted as HH:MM AM/PM)
- **Remote NTP Server** – Obtains date and time from an NTP (Network Time Protocol) server.

  The NTP Server poll rate is determined by the clock discipline algorithm designed to maximize accuracy while minimizing network overhead. The actual poll interval depends on clock accuracy and offset differences, called "clock jitter". The algorithm also includes provisions to further reduce network load when the NTP Server is unreachable.

  The NTP specifications allow one large time adjustment when first connected to the server, but avoids additional large corrections. This means it may take a few hours to correct a clock that was set incorrectly after the system was started.

  The Janus controller monitors the connection to the Remote NTP Server and generates Error 595 (Remote NTP Server Error) and logs an event when the connection is lost. The status of the connection is checked at startup (or when 'Sync Time Method' on the *Clock Settings* webpage is changed to 'Use Remote NTP Server') and periodically every hour. The error condition is cleared and event logged when communications is received from the NTP Server.

  The following must be entered when 'Remote NTP Server' selected:
  - Time Zone Region
  - Time Zone City
  - Sync Host IP Address
- **CTI Data Cache Host PLC**

  The CTI Data Cache interface reads time from the Host PLC immediately after the connection/validation process and in following cases:
  - The Host PLC indicates the PLC Clock time/date has been changed,
  - Approximately every 2 hours.

  When the [APPLY] button is pressed, entries will be validated and error message displayed if necessary. If no errors are detected, a confirmation message will be displayed. The new parameters go into effect immediately after the message is acknowledged,.

8.3.5 File Management

This page allows you to perform operations on the controller files. The following operations can be performed.

- **Copy to Front Panel SD Card:** Copies selected user file(s) from the internal SD card '/ctiplc' folder
- **Copy from Front Panel SD Card:** Copies selected user file(s) or folder to the internal SD card '/ctiplc/user' or '/ctiplc/graphics' folder
- **Replicate the System:** Copies files from internal SD card to front panel SD card necessary to replicate the OS and application on another Janus controller
- **Download File to Computer:** Downloads a selected file from the internal SD card to the PC 'Downloads' folder
- **Upload File from Computer:** Uploads a single file from the PC to the '/ctiplc/user' or '/ctiplc/graphics' folder on the internal SD card
- **Delete User Area Files:** Deletes selected files from the '/ctiplc/user' or '/ctiplc/graphics' folder on the internal SD card.
- **Copy Core Dump Files to Computer:** Creates a zip file of the selected Core Dump file and transfers it to the computer.
- **Copy Core Dump Files to Front Panel SD Card:** Creates a zip file of the selected Core Dump file an transfers it to the external SD card.
- **Delete Core Dump Files:** Deletes selected Core Dump files on the internal SD card.

NOTES:

- An error message will be displayed if the all selected files cannot be copied.
- The [REFRESH] button can be used to check SD card status
- The [COPY] button initiates the selected file transfer. For operations that access the external SD card, it must be inserted and detected by the system (via Status message) before SD card file transfer can start.
- The ***File Management*** operation can be cancelled by the user at any time before the [COPY] or [DELETE] pushbutton is pressed by selecting a different web page or closing the browser window. Once the button is pressed, the file transfer will continue until successful completion or an error condition occurs.

8.3.6 Firmware Update

This page provides a method to initiate a *Remote Firmware Update* for the Janus controller. For more details, see Section 6.3.

- [REFRESH] pushbutton is used to recheck the controller C operational status.
- [BROWSE] pushbutton displays a File Explorer window when pressed. This allows navigation through PC/Network drives to select the Firmware Update file to download..
- [UPDATE FIRMWARE] button initiates the firmware update process when pressed. All interlocks (User Switch 1 position, Warning Acknowledgement checkbox, and PLC operational state) must be met before firmware update process will start.

  NOTE: The ***Remote Firmware Update*** procedure can be cancelled any time prior to pressing the [UPDATE FIRMWARE] pushbutton by selecting a different web page or closing the browser window. Once the button is pressed, firmware update will continue until successful completion or error.
- [STATUS] window that provides information on the current state of the firmware update process.

8.3.7 Product Reset

This page provides a method to remotely the reset of the Janus controller. Remote reset is allowed only when module Switch 5 is in the CLOSED position. The following resets are allowed:

- Clear Exception
- Reset Configuration Settings
- Restore Factory Defaults

See Section 5.3 for description of reset options.

NOTE: The connection to the PLC web server will be lost after any of the above actions are taken. Any action other than 'Clear Exception' will force the PLC to lose its IP address.

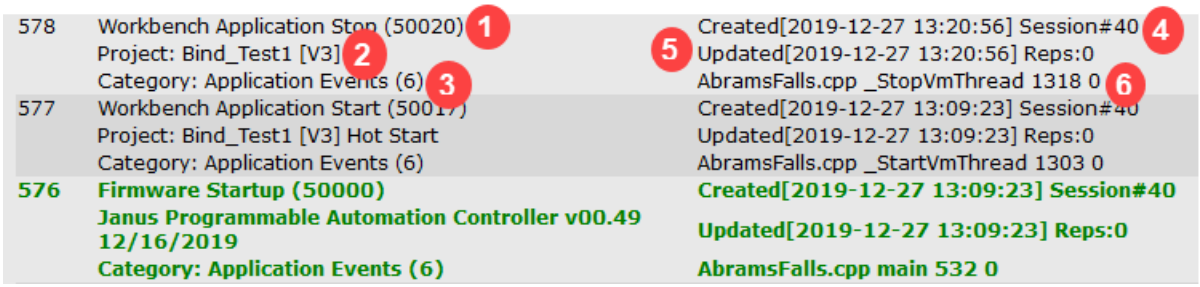
8.4 Event Log

The Event Log maintains a history of user actions, operational states, application settings, and system-level errors that affect the controller operation. The Event Log is an extremely useful tool for “post event” analysis for determining the events leading up to an unexpected operation or error condition.

The Event Log record format includes the following data:

1) Event Text / Event ID
2) Project Name / Version Number
3) Event Category Text / Category ID
4) Record Creation Date / Session Number
5) Update Time / Number Repetitions
6) File / Line Number that Logged Event

The location of these fields in the Event Log record is shown below:



The Event Log records are also color-coded to aid in spotting startup and fatal error events. Startup messages (logged immediately after boot) are GREEN (see above), and fatal error events are colored RED.

The Event Log also incorporates a filtering algorithm to detect duplicate messages. This prevents a single or a series of repetitive actions (such as a toggling error state condition) from filling the Event Log. Any event that is repeated within a one-hour period causes an update to the ‘Timestamp’ and ‘Repetition Count’ (item 5 above) in the original record instead of creating a new record each time an event is detected.

8.5 Statistics

This section will display statistics related to the Communication Sessions, PLC cycles, and Fieldbus Protocols (excluding EIP Tag Client, EIP Tag Server, EIP Scanner, and EIP Adapter, and services controlled by the TCP/UDP Management functions in user logic programs). All counts are reported since application was last started (transfer from APPLICATION STOP).These counts are automatically reset only on next transfer from APPLICATION STOP.

The following statistics categories are available:

- **Active Communications Sessions:** Displays information for data transfers to/from each connected device.
- **Closed Communications Sessions:** Displays information for TCP connections that have closed since last power cycle. The list is limited to the last 200 closed connections. The information for the oldest closed connection(s) in excess of 500 will be overwritten.
- **Cycle Statistics:** Displays information regarding the following:
    - Controller scan
    - Binding Subscriber
    - I/O Exchange
    - Modbus Master and Slave
    - Binding Publisher
    - User Logic Programs
    - Ethernet/IP
    - I/O Exchange Details
- **Data Cache Client**
- **Fieldbus Statistics:** Displays information regarding configured fieldbus drivers (except Modbus).
- **Net Statistics:** Displays information regarding the TCP/IP stack.
- **Past Sessions:** Displays statistics from previous sessions. A session is started when the controller boots up and ends immediately before the next time the controller boots up.

8.6 Error Descriptions and Status

This page lists all controller error codes and provides the following information for each:

- Error Description
- Error Count
- Start Timestamp
- End Timestamp

Active Errors are shown in red.

8.7 Display All Pages

This selection groups all web server pages into a page and provides an easy method for the user to “save all web data and statistics” when required for troubleshooting and analysis.

8.8 Custom HTML (graphics)

Displays list of user-generated graphics pages that have been created and downloaded to the appropriate folder (ctiplc/graphics) on the internal SD card. You can display a graphics page directly by selecting the corresponding file from this list. The appropriate security options as set in the *Security Settings* configuration are applied to all graphics web pages.

8.9 Acknowledgements

Displays third-party software used in the CTI products in accordance with their open-source license policies.

8.10 Product Support

Opens browser connection to the Control Technology Inc. home page.

APPENDIX A: SYSTEM ERROR CODES

NOTE

*When more than one error exists, the highest priority error code will be displayed on the alphanumeric display. When this error is cleared, if another error exists, the next highest priority error code will be displayed. When multiple errors exist with the same (highest) priority, the codes are alternately displayed. In the tables below, the **Priority** column contains the error priority. The highest priority is 1.*

*The **Error Descriptions and Status** web page will display all current errors.*

CPU Startup Errors

Error Code	Description	Priority	Operation	Error Recovery
010	No Network Configuration	X	Controller stopped.	Configure CPU via Web Server or use SD Card Ethernet Port Setup to specify Controller IP Address.
020	Ethernet Port Switch Configuration error (not set for 'Full Duplex' or '10/100mb' operation)	X	Controller stopped.	Cycle power to Controller. Contact CTI.
030	Manufacturing Data Checksum Error	X	Controller stopped.	Cycle power to Controller. Contact CTI.
050	Duplicate IP Address detected on network NOTE: This condition is checked every minute while PLC is active.	X	Controller stopped.	Check Event Log for details. Correct IP addresses for conflicting devices. Error is cleared after 2 consecutive probes report no duplicate IP Address (3 minutes max).
070	Configuration Settings Missing or Invalid	X	Controller stopped.	Configure CPU via Web Server. Download program from Janus Workbench.

Controller Run Mode Startup Errors

Error Code	Description	Priority	Operation	Error Recovery
080	No Application Program Found	8	Controller stopped.	Download program from Janus Workbench.
085	Specified Startup Mode Unavailable (Application cannot start as configured due to abnormal shutdown, unsupported program version, or PLC installed in I/O module slot with application that includes Local I/O)	9	Controller stopped.	Two possible reasons: (1) PLC could not complete an orderly shutdown due to loss of power. Connect Workbench to start application or press *Clear Exception* button to trigger "Cold Start". (2) PLC inserted into I/O module slot 1-16 and application includes a Local I/O config. Modify application to remove LIO config or move PLC to Slot 0.
090	Incompatible Application Program	11	Controller Stopped	Recompile Program with correct controller model/firmware version or update firmware.
110	Local I/O driver failed to start	11	Controller stopped.	Reset Controller. Contact CTI.
120	Remote I/O driver failed to start	11	Controller stopped.	Reset Controller Contact CTI.
140	Profibus I/O driver failed to start	11	Controller stopped.	Reset Controller. Contact CTI.
150	CTI Data Cache Client driver failed to start	12	Controller stopped.	Reset Controller. Contact CTI.
160	CAMP Client driver failed to start	12	Controller stopped.	Reset Controller. Contact CTI.
165	CAMP Server driver failed to start	12	Controller stopped.	Reset Controller Contact CTI.
170	MODBUS Client driver failed to start	12	Controller stopped.	Reset Controller. Contact CTI.
175	MODBUS Server driver failed to start	12	Controller stopped.	Reset Controller. Contact CTI.
180	Ethernet/IP Scanner driver failed to start	12	Controller stopped.	Reset Controller. Contact CTI.
185	Ethernet/IP Adapter driver failed to start	12	Controller stopped.	Reset Controller Contact CTI.
187	Ethernet/IP FlexIO driver failed to start	12	Controller Stopped	Reset Controller Contact CTI.
190	Ethernet/IP Tag Client driver failed to start	12	Controller stopped.	Reset Controller Contact CTI.
195	Ethernet/IP Tag Server failed to start	12	Controller stopped.	Reset Controller. Contact CTI.

Error Code	Description	Priority	Operation	Error Recovery
210	MQTT Client driver failed to start	12	Controller stopped	Reset Controller. Contact CTI.
215	OPCUA Server failed to start	12	Controller Stopped	Reset Controller. Contact CTI
220	HTML5 Data Server driver failed to start	12	Controller stopped.	Reset Controller. Contact CTI.

Firmware/Configuration Update Errors

Error Code	Description	Priority	Operation	Error Recovery
250	Front Panel SD Card – File Not Found (Could be detected by 'SD Card Firmware Update' or 'SD Card Ethernet Port Setup' operations)	10	Occurs during referenced procedures while controller is stopped.	Occurs when file download fails during 'Remote Firmware Update' or expected file not found on SD card during 'Front Panel Firmware Update' or 'SD Card Ethernet Port Setup'. Ensure that module switches 2 and 4 are not CLOSED. Retry download, or copy appropriate file to root directory of SD card and insert card into front panel holder.
260	Front Panel SD Card – Invalid File (Could be detected by 'SD Card Firmware Update' or 'SD Card Ethernet Port Setup' operations)	11	Occurs during referenced procedures while the controller is stopped.	Ensure appropriate file is in SD card root directory. Check contents of 'cti.ini' file if error detected by 'SD Card Ethernet Port Setup' utility. Verify firmware file name (*.zip) matches product being updated for 'Firmware Update'. Try using a different SD card if performing 'Front Panel Update'. If condition persists, contact CTI.

Execution Errors

Error Code	Description	Priority	Operation	Error Recovery
310	System Exception Error (Detected after CPU reset following Segmentation Fault or Firmware Error)	6	System restarts. Controller remains stopped after restart.	Connect Workbench and transfer to RUN or use CLEAR EXCEPTION button to restart CPU. Contact CTI Support.
320	System Watchdog Timeout (Detected after CPU reset following Segmentation Fault or Firmware Error)	7	System restarts. Controller remains stopped after restart.	Connect Workbench and transfer to RUN or use Reset button to restart CPU. Contact CTI Support.
330	Program Logic Error	7	Controller enters ERROR state (Logic programs and fieldbus protocols are stopped).	This condition most likely caused by 'Infinite Logic Loop' or 'Bad Array Index'. Connect Workbench to correct problem and transfer to RUN or use 'Clear Exception' button to restart CPU.

SD Card Errors

Error Code	Description	Priority	Operation	Error Recovery
350	Internal SD Card Disk Full (no further writes to internal SD card)	15	Controller continues to run, but database updates, user file functions, and program downloads are prohibited.	Use Web Server 'SD Card File Management' page to transfer or delete user files.
355	Internal SD Card Free Space Limit (disk > 90% full)	16	Controller continues to run, but all user file access functions are disabled (should return errors when called).	Use Web Server 'SD Card File Management' page to transfer or delete user files
360	Internal SD Card Free Space Warning (disk > 80% full)	17	Controller continues to run normally.	Use Web Server 'SD Card File Management' page to transfer or delete user files
370	Front Panel SD Card Not Accessible (Missing, Incompatible, Unformatted or Write-Protected)	16	Controller continues to run normally	Cancel function that is using Front Panel SD Card, or correct problem with SD card.

I/O Subsystem Errors

Error Code	Description	Priority	Operation	Error Recovery
410	Local I/O Module Error (module slot configuration mismatch or module failure).	22	Controller continues to run normally	Ensure Local I/O configuration matches I/O modules installed in local base.
415	Local I/O Interface Timeout Error (Local I/O Driver or FGPA Interface Task watchdog expired due to communication timeout).	14	'Output Disable' for Local Base asserted. Controller continues to run normally	Local I/O Subsystem attempts to recover automatically. Reset PLC and contact CTI if condition repeats.
420	Remote I/O RBC Error (One or more bases are enabled but not exchanging data with PLC.)	21	Controller continues to run normally	Ensure RBC addresses and cabling are correct.
425	Remote I/O Module Error (Module slot configuration mismatch or module failure).	22	Controller continues to run normally	Check Event Log for details. Ensure RBC configurations match I/O modules installed in bases.
430	Remote I/O Interface Timeout Error (Remote I/O Driver or FGPA Interface Task watchdog expired due to communication timeout).	14	'Output Disable' for RBCs asserted. Controller continues to run normally	Remote I/O Subsystem attempts to recover automatically. Reset PLC and contact CTI if condition repeats.

Profibus Network Errors

Error Code	Description	Priority	Operation	Error Recovery
440	Profibus Network Error (Profibus configured but not in 'Operate' mode due to Profibus subsystem error or DP bus error)	20	Controller continues to run normally	Check Event Log. Check Profibus cable for secure connection. Set application mode to STOP and back to RUN. Cycle power to CPU and restart application. Contact CTI if error persists.
450	Profibus Slave Error (One or more slaves are configured but not exchanging I/O data with DP-Master)	21	Controller continues to run normally	Check web server 'Profibus' page for details. Ensure slave configuration matches device and cabling/ termination is correct.
455	Profibus CTI/505 RBC Slave Module Error (Module configuration mismatch or module failure)	22	Controller continues to run normally	Check Event Log for details. Ensure RBC configurations match I/O modules installed in bases.
460	Profinet Controller Error (Connection to device or IO communications failed)	21	Controller continues to run normally	Check web server 'Profinet Controller' webpage for details. Ensure Profinet Device configuration matches device settings and Ethernet connection to Profinet Device.

Client Communication Errors

Error Code	Description	Priority	Operation	Error Recovery
470	CTI Data Cache Client: Host TCP Connection Failure	28	Controller continues to run normally	Correct connection and/or Host settings
475	CTI Data Cache Client has non-CTI MAC Address	25	Controller continues to run normally	Remove DC Client from application or force creation of new 'cti.ini' file to update MAC Address
480	CTI Data Cache Client Incompatible Host PLC Firmware	25	Controller continues to run normally	Update Host PLC firmware
485	CTI Data Cache Client: Host PLC Registration Failed (PLC already has max number of connections)	25	Controller continues to run normally	If replacing an existing Data Cache module, remove old module before connecting new one.

Error Code	Description	Priority	Operation	Error Recovery
490	CTI Data Cache Client: Host PLC Link Inactive	28	Controller continues to run normally	Correct connection to Host PLC. Ensure Host PLC is online.
510	CTI Data Cache Client: Host PLC Fatal Error	26	Controller continues to run normally	Clear Host PLC Fatal Error
515	CTI Data Cache Client: Host PLC in Program Mode	29	Controller continues to run normally	Change Host PLC mode to RUN
520	CTI Data Cache Client: Inaccessible PLC Address	29	Controller continues to run normally	Check that CTI Data Cache configuration matches PLC memory configuration
525	CTI Data Cache Client: No Memory Buffers Available for Data Write to Host PLC (too many Write requests during one Host PLC scan).	*	Controller continues to run normally. Error clears next IEC PLC cycle.	Increase Host PLC time slice for CTI Data Cache interface. Set “fixed” IEC PLC cycle time.
540	CAMP Client Error (Connection to servers or communication failed)	28	Controller continues to run normally	Check configuration and connection to CAMP Server(s).
550	MODBUS Client Error (Connection to servers or communication failed)	28	Controller continues to run normally	Check configuration and connection to Modbus Server(s).
560	Data Exchange Error (Subscriber not receiving data from one or more Publishers).	27	Controller continues to run normally	Check Global Binding configuration and connection to Data Exchange Publisher device.
570	Ethernet/IP Scanner Error (Connection to servers or communication failed)	28	Controller continues to run normally	Check configuration and connection to EIP Adapter(s).
575	Ethernet/IP FlexIO Error (Connection to Adapters or I/O communications failed)	28	Controller continues to run normally	
580	Ethernet/IP Tag Client Error (Error is default at startup when configured)	28	Controller continues to run normally	Check configuration and connection to EIP Server.
590	MQTT Client Error (Connection to broker or communication failed)	28	Controller continues to run normally	Check configuration and connection to MQTT broker.
595	NTP Server Error (Connection to NTP Server lost/failed)	28	Controller continues to run normally	Check configuration and connection to NTP Server.

* Not displayed on Alphanumeric Display

Hardware Errors

Error Code	Description	Priority	Operation	Error Recovery
600	Battery Low Warning	29	Controller continues to run normally	Battery voltage has dropped to “warning” level. Replace battery as soon as possible.
610	Battery Unavailable (Battery voltage below usable level or missing)	16	Controller continues to run normally. The PLC is currently without battery backup if power is lost while the controller is running.	Battery is not installed or battery voltage has dropped below usable level. Replace battery immediately.
620	Real-Time Clock Access Error (firmware unable to read or write RTC)	23	Controller continues to run normally	This indicates a hardware error. Error clears if future attempt to access the RTC is successful. Contact CTI Support.
630	Processor High Temperature Warning	16	Controller continues to run normally	This indicates a serious issue with CPU internal temperature. User should lower ambient temperature and/or shutdown CPU if temperature does not return to normal.

APPENDIX B: IP ADDRESS INFORMATION

IP Address Nomenclature

IP Address

Every host interface on a TCP/IP network is identified by a unique IP Address. This address is used to uniquely identify the host device, such as a workstation or communications module, and the network to which the host belongs.

Each IPV4 Address consists of 32 bits, divided into four 8 bit entities called *octets*. An IP Address is expressed in *dotted notation,* with each octet expressed as its decimal equivalent. See the example below.

Notation	Octet 1	Octet 2	Octet 3	Octet 4
Binary	11000000	11011111	10110001	00000001
Decimal	192	223	177	1

Although an IP Address is a single value, it contains two types of information: the *Network ID* and the *Host ID*. The Network ID identifies the IP network to which the host belongs. The Host ID identifies a specific IP host on that IP network. All IP hosts on a particular local area network must have the same network ID. Each IP host on a particular local area network must use a unique Host ID.

Address Classes

The Internet community originally defined network classes to accommodate networks of varying sizes. The network class can be discerned from the first octet of its IP Address.

The following table summarizes the relationship between the first octet of a given address and its Network ID and Host ID fields. It also identifies the total number of Network IDs and Host IDs for each address class that participates in the Internet addressing scheme.

Class	First Octet Value*	Network ID	Host ID	Number of networks	Number of hosts per net
A	1-126	First Octet	Last 3 Octets	126	16,777,214
B	128-191	First 2 Octets	Last 2 Octets	16,384	65,534
C	192-223	First 3 Octets	Last Octet	2,097,151	254

* Address 127 is reserved for loopback testing and inter-process communication on the local computer; it is not a valid network address. Addresses 224 – 239 are used for Class D (IP multicast).

Subnet Mask

Used alone, the designation of network classes proved to be inflexible. Assigning large numbers of devices to the same network is impractical considering performance, topology, and security constraints. The Subnet Mask, sometimes called the Network Mask, provides a flexible means of designating the Network ID portion and Host ID portions of the network address. In modern TCP/IP implementations, the network class is largely ignored, except for setting the default subnet mask

The subnet mask is a collection of 32 bits that distinguish the network ID portion of the IP address from the host ID. Subnet masks are implemented by assigning 1's to bits that belong to the network ID and 0's to the bits that belong to the host ID. To represent the mask, the 32-bit value is converted to dotted decimal notation or CIDR (Classless Inter-Domain Routing) notation, a commonly used alternate. The CIDR notation counts the number of bits in Network ID portion of the address (bits that are set to 1). The count is preceded by a slash. See the example below.

Bits for Network Mask				Dotted Decimal Format	CIDR Format
11111111	00000000	00000000	00000000	255.0.0.0	/8
11111111	11111111	11110000	00000000	255.255.240.0	/20
11111111	11111111	11111111	00000000	255.255.255.0	/24

For example: when the IP address is 128.54.177.97 and the network mask is 255.255.255.0, the Network ID is 128.54.177 and the Host ID is 97. When using the CIDR format, the network mask is appended to the IP address. Thus the IP address and subnet mask shown above would be represented as 128.54.177.97 /24.

NOTE

*The binary representation of a Network Mask must be a single continuous block 1's followed by a contiguous block of zeroes. When entering the Network Mask in dotted decimal notation, you must ensure that this requirement is maintained. For example, a network mask of 255.247.0.0 is not valid because the binary equivalent (11111111111**0**111000000000000000) violates this rule.*

The Network Mask must allow at least two bits of host address. In addition, a network mask which causes the derived host ID to be 0 or a broadcast address (all Host ID bits set to 1) should not be used.

Using the Subnet Mask

For Class A, B, and C IP addresses, the IP Host uses the Subnet Mask to determine where to send an IP message. After deriving the Network ID and Host ID portion of the IP Address using the Subnet Mask, the IP Host compares the Network ID of the destination IP Address with the Network ID of the Host IP Address. If the Network IDs are the same, the message is sent to another Host on the local network. If the Network IDs are different, the message is sent to an IP Gateway, for routing to another network, if possible.

When you are configuring the IP Address of devices that must communicate on a local network, you must ensure that:

- The Subnet Mask of all devices is the same.
- The Network ID of all hosts is the same.
- The Host ID of each host is different.

If you are using Subnet Masks that are aligned with the IP Address octets, this can easily be done by examining the dotted decimal values. The octets of the IP Address where the corresponding octet of the Subnet Mask is 255 belong to the Network ID and the octets of the IP Address where the corresponding octet of the Subnet Mask is 0 belong to the Host ID.

For example, where the IP Address is 127.18.40.3 with a Subnet Mask of 255.255.0.0, the Network ID is 127.18 and the Host ID is 40.3.

IP Address	127	18	40	3
Subnet Mask	255	255	0	0
Network ID	127	18		
Host ID			40	3

However, if you are using a Subnet Mask that does not align with the octet boundaries, this is more difficult. You will need to perform a bitwise “and” calculation to arrive at the Network address. See the following illustration.

Assuming an IP Address of 127.18.40.3 and a Subnet Mask of 255.255.240.0, the following table illustrates the bitwise “and” operation. In essence, wherever the Subnet Mask bit is one, the corresponding IP Address bit is part of the Network ID.

Item	**Dotted Decimal**	**Binary Equivalent**			
		1st Octet	2nd Octet	3rd Octet	4th Octet
IP Address	127.18.40.3	**01111111**	**00010010**	**0010**1000	00000011
Subnet Mask	255.255.240.0	**11111111**	**11111111**	**1111**0000	00000000
Derived Network Address	127.18.32.0	**01111111**	**00010010**	**0010**0000	00000000

An easier way to determine this is to compare only non-aligned Subnet Mask octet with the corresponding octet of the IP Address. For example, since the Subnet Mask of the first two octets is 255.255, the first two octets of the Network ID are the same as the dotted decimal values (127.18) of the IP Address. However, since the third octet of the subnet mask is not 255 or 0, you must perform a bitwise “and” calculation using the third octet of the IP Address and Subnet Mask.

This can be accomplished by using the Windows calculator Programmer view. Using this example, you would enter the value of the third octet (40), click on the “and” button, enter the Subnet Mask (240), and then click on the “=” button. The result, in this case, is 32. Thus, the Network Address is 127.18.32.0.

CIDR Notation

CIDR notation (Classless Inter-Domain Routing) is an alternate method of representing a subnet mask. It is simply a count of the number of network bits (bits that are set to 1) in the subnet mask. It provides a more concise way to represent the subnet mask. The CIDR number is typically preceded by a slash “/” and follows the IP address. For example, an IP address of 131.10.55.70 with a subnet mask of 255.0.0.0 (which has 8 network bits) would be represented as 131.10.55.70 /8. The following table can be used to convert between subnet mask and CIDR.

CIDR	Dotted Decimal		CIDR	Dotted Decimal
/1	128.0.0.0		/17	255.255.128.0
/2	192.0.0.0		/18	255.255.192.0
/3	224.0.0.0		/19	255.255.224.0
/4	240.0.0.0		/20	255.255.240.0
/5	248.0.0.0		/21	255.255.248.0
/6	252.0.0.0		/22	255.255.252.0
/7	254.0.0.0		/23	255.255.254.0
/8	255.0.0.0		/24	255.255.255.0
/9	255.128.0.0		/25	255.255.255.128
/10	255.192.0.0		/26	255.255.255.192
/11	255.224.0.0		/27	255.255.255.224
/12	255.240.0.0		/28	255.255.255.240
/13	255.248.0.0		/29	255.255.255.248
/14	255.252.0.0		/30	255.255.255.252
/15	255.254.0.0		/31	255.255.255.254
/16	255.255.0.0		/32	255.255.255.255

Selecting an IP Address

The Janus Controller typically requires a fixed IP Address. If you are connecting to an existing network, you should obtain an unused static IP Address and Subnet Mask from the network administrator.

If you are establishing your own IP Addresses, you should select IP Addresses from a block of ‘private” addresses established by the Internet Assigned Numbers Authority (IANA). The private address blocks are:

- 10.0.0.0 through 10.255.255.255 (Class A)
- 172.16.0.0 through 172.31.255.255 (Class B)
- 192.168.0.0 through 192.168.255.255 (Class C)

These addresses will not be forwarded by the Internet backbone routers; therefore, you are free to use any address in this group as long as it does not conflict with the usage by your local organization.

Selecting a Multicast Address

The address range of 239.0.0.0 thru 239.255.255.255 has been designated as an administratively scoped Multicast Address space (RFC 2365). Addresses in this range are designated for use by private multicast domains. They do not conflict with other multicast address spaces that are explicitly assigned by Internet Assigned Numbers Authority (IANA). Within this range, addresses 239.255.0.0 thru 239.255.255.255 are designated for the IPV4 multicast local scope.

If you are choosing a Multicast Address for a new factory floor application, you should choose a Multicast Address in the IPV4 local scope range (239.255.0.0 thru 239.255.255.255) unless you have a specific reason to do otherwise. You should verify there is no conflict with other Multicast Addresses being used locally.

In case you are using the Janus controller in an existing multicast application that uses a Multicast Address outside of the administratively scoped address space, the configuration program allows you to enter the complete range of assignable multicast addresses (224.0.0.1 thru 239.255.255.255).

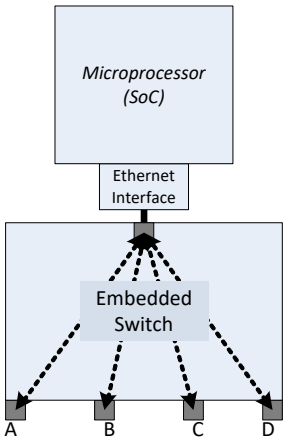
For a current list of IANA assigned multicast addresses, see the IANA website:
www.iana.org/assignments/multicast-addresses/

APPENDIX C: ETHERNET PORT OPERATION

The following sections describe how the ports on the Janus controller work and how Alternate IP subnets are applied.

Ethernet Port Operation

Ethernet (layer 2) is responsible for sending and receiving Ethernet frames, which contain the TCP/IP protocol and related data. Among other information, Ethernet frames contain a source address, which identifies the originator of the frame and a destination address, which indicates how the frame will be delivered. The source address contains the MAC (Media Access Control) address of the originator. The destination address may contain a **unicast** address (the MAC address of the intended recipient), a **multicast** address, or an address that indicates a **broadcast** address.



The Ethernet ports on the Janus controller are connected to an Ethernet switch on the Janus circuit board. This switch is also connected to an internal Ethernet interface of the Janus microprocessor. By default, the external ports (PORTS A, B, C, and D) are isolated from each other. Frames entering one port are never forwarded to the other ports. This is important when connecting ports to different Ethernet networks. It prevents traffic (especially broadcast and multicast traffic) on one network from propagating to other networks. This is also important to prevent network loops, which can cause broadcast storms, when connecting multiple ports to the same Ethernet network, as you might do when designing redundant networks.

NOTE

You can enable forwarding between external ports for unusual applications.
See Section 4.2.3 Internal Ethernet Switch Configuration.

Frames entering the external ports are forwarded to the internal Ethernet interface if the Ethernet destination address is the same as the MAC address of the interface (Unicast) or when the destination address is a multicast or broadcast address. The switch does not forward frames that do not meet these criteria, preventing them from consuming microprocessor resources.

So, when a frame is sent *from* the internal Ethernet interface, how does the switch determine which port to forward it to? The answer to this is in the way Ethernet switches work. Ethernet switches learn the MAC address(es) of the device(s) connected to the ports. Once the port associated with a MAC address is known, the switch will forward a frame whose destination address matches this address to this port only.

NOTE

Broadcast and Multicast frames from the internal Ethernet interface will be forwarded to all frames. In the majority of cases, this traffic is insignificant. Broadcast frames are primarily transmitted when resolving IP addresses to MAC addresses. Once known, this information is cached. If you are sending substantial multicast traffic, network switches can be configured to limit Multicast forwarding (using IGMP Snooping). Alternatively, you may want to use only one network port.

Alternate IP Subnets

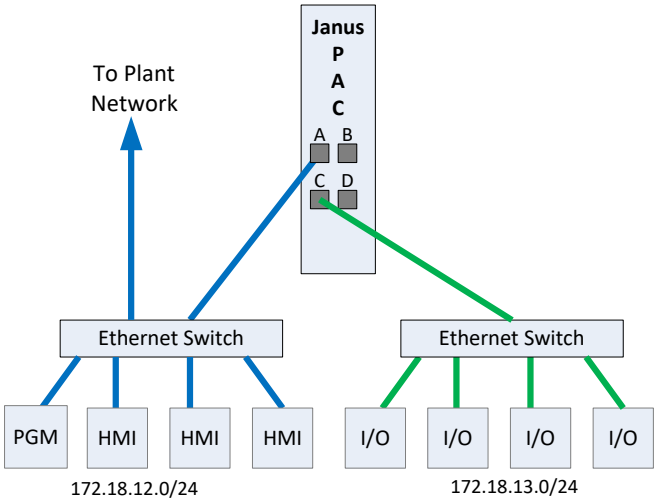
TCP/IP is responsible for functions such as routing IP packets among local area networks, establishing connections between devices (IP Hosts), and associating IP addresses with Ethernet MAC addresses. As noted above, on Ethernet networks, the TCP/IP protocol is contained as data in Ethernet frames.

An IP Host, such as the Janus controller, can communicate directly with other IP Hosts on the same Ethernet Local Area Network only if they belong to the same IP subnet (see APPENDIX B: IP ADDRESS INFORMATION). Otherwise IP packets transmitted by the device are sent to an IP gateway, which attempts to route them to another network.

Typically, a single set of IP address parameters (IP address and subnet mask) are associated with a device's Ethernet interface. As a result, the device is limited to communicating directly with devices on a single IP subnet.

However, the Janus controller allows you to associate up to four sets of IP parameters with its Ethernet Interface, enabling the controller to communicate directly with devices on four different IP subnets, if desired.

This capability is especially useful when connecting the controller to multiple Local Area Networks. See the example below. For simplicity, separate Ethernet switches for each network are illustrated. This topology can also be accomplished with one switch using VLAN (Virtual Local Area Network) technology.



Example

Port A is connected to a plant "data" network, used for programming and data access (HMI and SCADA workstations). Devices on this network are members of the IP subnet 172.18.12.0/24 (172.18.12.1, 172.18.12.2, etc.).

Port B is connected to an "I/O" network, used to communicate with Ethernet I/O. Devices on this network are members of the IP subnet 172.18.13.0/24 (172.18.13.1, 172.18.13.2, etc.).

The Janus controller is configured to be a member of both IP subnets.

- Primary Subnet IP Address = 172.18.12.10 with Subnet Mask = 255.255.255.0.
- Alternate Subnet 1 IP Address = 172.18.13.10 with Subnet Mask =255.255.255.0.

Consequently, the Janus controller is able to communicate directly with devices on either subnet. A CAMP Server application would be able to communicate with devices on the "data" network subnet and an Open Modbus Client would be able to communicate with I/O devices on the "I/O" network.

NOTE

IP subnets are not directly associated with an Ethernet Port.
As explained earlier, the Ethernet switch is responsible for delivering frames containing the IP Protocol to the correct device via the corresponding port. It is acceptable (although unusual) for devices on different IP subnets to exist on the same Ethernet Local Area Network.

Also, IP subnets are not associated with an application. The internal TCP/IP software (TCP/IP stack) routes data to an application based on the IP port number.

APPENDIX D: PRODUCT SPECIFICATIONS

Environmental Specifications

Operating Temperature	0 to 60 C (32 to 140 F)
Storage Temperature	-40 to 70C (-40 to 158 F)
Relative Humidity	5% to 95% non-condensing
Pollution Degree	2, IEC 664, 664A
Vibration Sinusoidal Random	 IEC 68-2-6 Test Fc 0.15 peak to peak, 10 – 57 Hz 1.0g. 57 – 150 Hz IEC 68-2-34 or NAVMAT p-9492 Test Fdc with 0.04 g^2 /Hz, 80 – 350 Hz and 3db/Octave roll off, 80 -20 Hz and 350 – 2000Hz at 10 min/Axis
Impact Shock	IEC 68-2-27, Test Ea. Half Sine 15g, 11ms
Isolation, Inputs to Controller	1500 VRMS except where specified
Corrosion Protection	All parts of corrosion resistant material or plated/painted as corrosion protection
Electric Noise Immunity Conducted Noise Radiated Noise Electrostatic Discharge	 IEC 801 Part 4 Level 3 MIL-STD-461B, Part 4:CS01, CS02, CS06 IEC 255-4, Appendix C IEC 4517/79 Com(78) 766 Final, Part 4 IEC 472, 2.5 KV IEC 801 Part 3, Level 3 MIL-STD-461B, Part 4 RS01, RS02 IEC 801. Part 2, Level 4 (15kV)

Battery Specifications

Non-Rechargeable
System: Lithium Metal Oxide
Nominal voltage: 4.0V
Nominal capacity: 500m mAh
Nominal current: 100 mA
Maximum continuous discharge current: 7A
Pulse current capability: 15A
Temperature range: -40°C to.+85°C
Replacement Part Number: Tidiran TLM-1550HPM or equivalent

Agency Approvals (pending)

- UL, ULC
- FM (Class 1, DIV 2 - Hazardous Location) or equivalent
- CE Low Voltage Directive (73/23/EEC) and Electro-magnetic Compatibility Directive (89336/EEC)

Functional Specifications

2500P-J750 "Janus" Controller	
Built-in display for IP address and errors	yes
Ethernet	
Number of IP/Subnet Configurations	4
Number of connections	64
I/O	
Max I/O Points (Digital / Analog)	16K / 16K
Local I/O	yes
Remote I/O	yes
Ethernet I/O	future
Profibus - 64 Slaves	yes
Max I/O Data (Bytes)	32K
User Memory	
Code (Programs + Fieldbus)	3MB
Data	15MB
Web Server	yes
Web Visualization (variables)[1]	256
Enhanced On-line change	yes
Communication Protocols	
Binding (peer-peer)	yes
CAMP Server	yes
Camp Client	yes
Modbus UDP/TCP Client	choose 2**
Modbus UDP/TCP Server	yes
Data Cache Client Connections / Variables	1 / 6144
DataCache Client Block Disable	yes
Data Cache Server	future?
Ethernet/IP Scanner & Flex I/O	choose 2**
Ethernet/IP Adapter	yes
Ethernet/IP Tag Server	yes
Ethernet/IP Tag Client	choose 2**
MQTT Client (communicates with broker)	yes
OPC-UA Server	yes
Profinet Controller and Device	future
SFIO Block Transfer	no

NOTES

**Project may include two of these protocols

ETHERNET CONNECTION LIMIT
The 2500P-J750 permits a maximum of 64 Ethernet connections. This is the TOTAL of all Client protocol connections that are configured, plus whatever external devices connect to Server protocols.

For example, suppose an application has:

- 5 Modbus clients configured
- 4 Modbus devices which connect to the Modbus Server
- 16 Ethernet/IP scanner devices configured
- 2 devices which connect to the Ethernet/IP Tag Server
- 8 CAMP Client connections configured
- 4 devices which connect to CAMP Server
- 4 devices which connect to OPC-UA Server

This application has used (5+4+16+2+8+4+4) or 43 out of the possible 64 connections.

LIMITED PRODUCT WARRANTY

Warranty. Control Technology Inc. ("CTI") warrants that this CTI Industrial Product (the "Product") shall be free from defects in material and workmanship for a period of one (1) year from the date of purchase from CTI or from an authorized CTI Industrial Distributor, as the case may be. Repaired or replacement CTI products provided under this warranty are similarly warranted for a period of 6 months from the date of shipment to the customer or the remainder of the original warranty term, whichever is longer. This Product and any repaired or replacement products will be manufactured from new and/or serviceable used parts which are equal to new in the Product. This warranty is limited to the initial purchaser of the Product from CTI or from an authorized CTI Industrial Distributor and may not be transferred or assigned.

2. Remedies. Remedies under this warranty shall be limited, at CTI's option, to the replacement or repair of this Product, or the parts thereof, only after shipment by the customer at the customer's expense to a designated CTI service location along with proof of purchase date and an associated serial number. Repair parts and replacement products furnished under this warranty will be on an exchange basis and all exchanged parts or products become the property of CTI. Should any product or part returned to CTI hereunder be found by CTI to be without defect, CTI will return such product or part to the customer. The foregoing will be the exclusive remedies for any breach of warranty or breach of contract arising therefrom.

3. General. This warranty is only available if (a) the customer provides CTI with written notice of a warranty claim within the warranty period set forth above in Section 1 and (b) CTI's examination of the Product or the parts thereof discloses that any alleged defect has not been caused by a failure to provide a suitable environment as specified in the CTI Standard Environmental Specification and applicable Product specifications, or damage caused by accident, disaster, acts of God, neglect, abuse, misuse, transportation, alterations, attachments, accessories, supplies, non-CTI parts, non-CTI repairs or activities, or to any damage whose proximate cause was utilities or utility-like services, or faulty installation or maintenance done by someone other than CTI.

4. Product Improvement. CTI reserves the right to make changes to the Product in order to improve reliability, function or design in the pursuit of providing the best possible products.

5. Exclusive Warranty. THE WARRANTIES SET FORTH HEREIN ARE CUSTOMER'S EXCLUSIVE WARRANTIES. CTI HEREBY DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED. WITHOUT LIMITING THE FOREGOING, CTI SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, COURSE OF DEALING, AND USAGE OF TRADE.

6. Disclaimer and Limitation of Liability. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, CTI WILL NOT BE LIABLE FOR ANY BUSINESS INTERRUPTION OR LOSS OF PROFIT, REVENUE, MATERIALS, ANTICIPATED SAVINGS, DATA, CONTRACT, GOODWILL OR THE LIKE (WHETHER DIRECT OR INDIRECT IN NATURE) OR FOR ANY OTHER FORM OF INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND. CTI'S MAXIMUM CUMULATIVE LIABILITY RELATIVE TO ALL OTHER CLAIMS AND LIABILITIES, INCLUDING OBLIGATIONS UNDER ANY INDEMNITY, WHETHER OR NOT INSURED, WILL NOT EXCEED THE COST OF THE PRODUCT(S) GIVING RISE TO THE CLAIM OR LIABILITY. CTI DISCLAIMS ALL LIABILITY RELATIVE TO GRATUITOUS INFORMATION OR ASSISTANCE PROVIDED BY, BUT NOT REQUIRED OF CTI HEREUNDER. ANY ACTION AGAINST CTI MUST BE BROUGHT WITHIN EIGHTEEN (18) MONTHS AFTER THE CAUSE OF ACTION ACCRUES. THESE DISCLAIMERS AND LIMITATIONS OF LIABILITY WILL APPLY REGARDLESS OF ANY OTHER CONTRARY PROVISION HEREOF AND REGARDLESS OF THE FORM OF ACTION,

WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR OTHERWISE, AND FURTHER WILL EXTEND TO THE BENEFIT OF CTI'S VENDORS, APPOINTED DISTRIBUTORS AND OTHER AUTHORIZED RESELLERS AS THIRD-PARTY BENEFICIARIES. EACH PROVISION HEREOF WHICH PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTY OR CONDITION OR EXCLUSION OF DAMAGES IS SEVERABLE AND INDEPENDENT OF ANY OTHER PROVISION AND IS TO BE ENFORCED AS SUCH.

7. Adequate Remedy. The customer is limited to the remedies specified herein and shall have no others for a nonconformity in the Product. The customer agrees that these remedies provide the customer with a minimum adequate remedy and are its exclusive remedies, whether based on contract, warranty, tort (including negligence), strict liability, indemnity, or any other legal theory, and whether arising out of warranties, representations, instructions, installations, or non-conformities from any cause. The customer further acknowledges that the purchase price of the Product reflects these warranty terms and remedies.

8. Force Majeure. CTI will not be liable for any loss, damage or delay arising out of its failure (or that of its subcontractors) to perform hereunder due to causes beyond its reasonable control, including without limitation, acts of God, acts or omissions of the customer, acts of civil or military authority, fires, strikes, floods, epidemics, quarantine restrictions, war, riots, acts of terrorism, delays in transportation, or transportation embargoes. In the event of such delay, CTI's performance date(s) will be extended for such length of time as may be reasonably necessary to compensate for the delay.

9. Governing Law. The laws of the State of Tennessee shall govern the validity, interpretation and enforcement of this warranty, without regard to its conflicts of law principles. The application of the United Nations Convention on Contracts for the International Sale of Goods shall be excluded.

REPAIR POLICY

In the event that the Product should fail during or after the warranty period, a Return Material Authorization (RMA) number can be requested orally or in writing from CTI main offices. Whether this equipment is in or out of warranty, a Purchase Order number provided to CTI when requesting the RMA number will aid in expediting the repair process. The RMA number that is issued and your Purchase Order number should be referenced on the returning equipment's shipping documentation. Additionally, if the product is under warranty, proof of purchase date and serial number must accompany the returned equipment. The current repair and/or exchange rates can be obtained by contacting CTI's main office at 1-800-537-8398 or go to www.controltechnology.com/support/repairs/.

When returning any module to CTI, follow proper static control precautions. Keep the module away from polyethylene products, polystyrene products and all other static producing materials. Packing the module in its original conductive bag is the preferred way to control static problems during shipment. Failure to observe static control precautions may void the warranty.