

**CTI 2500P-JACP**

**Janus Application Coprocessor**

**Installation and Operation Guide**

**Version 2.96**

**Copyright 2022-2026 Control Technology Inc.  
All rights reserved.**

This manual is published by Control Technology Inc. (CTI) 5734 Middlebrook Pike, Knoxville, TN 37921. This manual contains references to brand and product names which are trade names, trademarks, and/or registered trademarks of Control Technology Inc. Siemens® and Series 505® are registered trademarks of Siemens AG. Other references to brand and product names are trade names, trademarks, and/or registered trademarks of their respective holders.

## **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](mailto:sales@controltechnology.com).

| REVISION HISTORY |           |                                                                                                                                                                                                                                                                  |
|------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V1.0             | 15FEB2023 | Initial Release                                                                                                                                                                                                                                                  |
| V1.1             | 19APR2023 | Added product specification matrix from product bulletin and added clarifying description about “max connections”.                                                                                                                                               |
| V1.2             | 10AUG2023 | Added potential use case configurations and information regarding remote base installation.                                                                                                                                                                      |
| V1.3             | 03JAN2024 | Added shipping configuration of switches and jumpers at Section 3.2.4                                                                                                                                                                                            |
| V1.4             | 09JAN2024 | Added note to Error 370 that error 250 will also be returned if Switch 2 or 4 is closed.                                                                                                                                                                         |
| V1.5             | 11APR2024 | Added SD card selection requirements in Section 3.1.3                                                                                                                                                                                                            |
| V1.6             | 10MAY2024 | Added ⚠ to all WARNING notices                                                                                                                                                                                                                                   |
| V1.7             | 14JUN2024 | Updated Item 3 in Section 6.2 to read “User” SD card instead of “Front Panel SD Card”                                                                                                                                                                            |
| V1.8             | 21OCT2024 | Added warning about simultaneous Workbench connections and online change to Section 1.1                                                                                                                                                                          |
| V1.9             | 14NOV2024 | Added Profinet activation as a possible cause of Error 090.                                                                                                                                                                                                      |
| V2.0             | 14FEB2025 | Added note in Section 1.1 clarifying which Siemens PLCs are supported by the Block Transfer Driver                                                                                                                                                               |
| V2.1             | 26FEB2025 | Updated SD card requirements in Section 3.1.3 (CTI-166)                                                                                                                                                                                                          |
| V2.2             | 02OCT2025 | Added note in <a href="#">Janus Application Coprocessor Overview</a> that CTI recommends 2500 Series PLC firmware to be at V9.22 or above for proper operation with 2500P-JACP                                                                                   |
| V2.3             | 13NOV2025 | Clarified error recovery description for E530 in <a href="#">Client Communication Errors</a> (DOCS-243)                                                                                                                                                          |
| V2.4             | 31DEC2025 | Added note in <a href="#">JACP Module Operation Overview</a> about minimizing the use of RETAIN variables when fast cycle times are important (JACP-87)                                                                                                          |
| V2.5             | 16FEB2026 | Added note that Auto-Run Hot start from Janus PLCs is not supported on JACP (DOCS-244)                                                                                                                                                                           |
| V2.6             | 20MAY2026 | Added more information to Error 090 in <a href="#">Module Run Mode Startup Errors</a> to include the case where an invalid function block in a POU or a field I/O configuration that is not applicable for the target product.                                   |
| V2.7             | 21MAY2026 | <ul style="list-style-type: none"> <li>Added notes showing User SD Card Ethernet Port setup is no longer available beginning with Firmware V2.00 (PL2023-96)</li> <li>Added new section describing how to edit the cti.ini file on the System SD Card</li> </ul> |
| V2.8             | 09JUN2026 | Updated labels on clock sync method in <a href="#">Clock Settings</a> (JACP-265)                                                                                                                                                                                 |
| V2.9             | 18JUN2026 | Added new error 031 for MRAM failure in <a href="#">CPU Startup Errors</a> (PL2023-104)                                                                                                                                                                          |
| V2.91            | 18JUN2026 | Updated default cti.ini configuration in <a href="#">System SD Card Ethernet Port Setup</a> (DOCS-245)                                                                                                                                                           |
| V2.92            | 17JUL2026 | <ul style="list-style-type: none"> <li>Added error codes 023-027</li> <li>Added note in <a href="#">CPU Startup Errors</a> that E031 is displayed on the front panel only and not on the Error Status webpage (PL2023-104)</li> </ul>                            |
| V2.93            | 27JUL2026 | Updated error display in <a href="#">User SD Card Firmware Update</a> (JACP-299)                                                                                                                                                                                 |
| V2.94            | 07AUG2026 | Added networking 2.0 documentation                                                                                                                                                                                                                               |
| V2.95            | 14AUG2026 | Updates from internal reviews                                                                                                                                                                                                                                    |

| REVISION HISTORY |           |                                                                                                            |
|------------------|-----------|------------------------------------------------------------------------------------------------------------|
| V2.96            | 26AUG2026 | Added note in <a href="#">Clock Settings</a> that Default Gateway setting is required to use NTP time sync |

---

## ***PREFACE***

---

This ***Installation and Operation Guide (IOG)*** provides information regarding installation, setup, and operation of the *CTI Janus Application Coprocessor*, also referred to as the *JACP module* 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 to 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**

---

|                                                             |           |
|-------------------------------------------------------------|-----------|
| <b>PREFACE</b>                                              | <b>5</b>  |
| <b>USAGE CONVENTIONS</b>                                    | <b>6</b>  |
| <b>TABLE OF CONTENTS</b>                                    | <b>7</b>  |
| <b>CHAPTER 1 INTRODUCTION</b>                               | <b>10</b> |
| 1.1 Janus Application Coprocessor Overview                  | 10        |
| 1.2 Janus Programming Software                              | 13        |
| <b>CHAPTER 2 FRONT PANEL</b>                                | <b>15</b> |
| 2.1 JACP Module Front Panel                                 | 15        |
| 2.2 Status Indicator LEDs                                   | 16        |
| 2.3 Alphanumeric Display                                    | 16        |
| 2.4 Reset Pushbutton                                        | 16        |
| 2.5 Ethernet Communications Ports                           | 17        |
| 2.6 Serial Ports                                            | 18        |
| <b>CHAPTER 3 INSTALLATION</b>                               | <b>19</b> |
| 3.1 Installation Planning                                   | 19        |
| 3.1.1 <i>Choosing the IP Address and related Parameters</i> | 19        |
| 3.1.2 <i>Power Requirements</i>                             | 19        |
| 3.1.3 <i>SD Card Selection</i>                              | 19        |
| 3.2 Installing the Module                                   | 20        |
| 3.2.1 <i>Unpacking the Module</i>                           | 20        |
| 3.2.2 <i>SD Card Installation</i>                           | 20        |
| 3.2.3 <i>Setting the Module Switches</i>                    | 21        |
| 3.2.4 <i>Shipping Configuration of Switches</i>             | 21        |
| 3.2.5 <i>Physical Installation</i>                          | 22        |
| 3.2.6 <i>Applying Power to the Base</i>                     | 22        |
| 3.2.7 <i>Connecting the Module to a Data Network</i>        | 22        |
| 3.2.8 <i>Startup from Factory Defaults</i>                  | 22        |
| 3.2.9 <i>Setting the IP Address</i>                         | 23        |
| <b>CHAPTER 4 CONFIGURATION</b>                              | <b>27</b> |
| 4.1 General Settings                                        | 27        |
| 4.2 Network Settings                                        | 28        |
| 4.2.1 <i>IP Parameters</i>                                  | 28        |
| 4.2.2 <i>Fieldbus Port Group Assignments</i>                | 28        |
| 4.2.3 <i>Internal Ethernet Switch Configuration</i>         | 28        |
| 4.3 Security Settings                                       | 28        |
| 4.4 Clock Settings                                          | 30        |
| <b>CHAPTER 5 OPERATION</b>                                  | <b>31</b> |
| 5.1 JACP Module Operation Overview                          | 31        |
| 5.2 Module Startup                                          | 32        |
| 5.3 Reset Pushbutton Operation                              | 33        |

|                                                                                                                                                                               |           |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 5.4 HTTP Data Server .....                                                                                                                                                    | 34        |
| <b>CHAPTER 6 UPDATING FIRMWARE .....</b>                                                                                                                                      | <b>35</b> |
| 6.1 Overview .....                                                                                                                                                            | 35        |
| 6.2 User SD Card Firmware Update .....                                                                                                                                        | 35        |
| 6.3 Remote Firmware Update .....                                                                                                                                              | 36        |
| 6.4 Direct File Replacement .....                                                                                                                                             | 37        |
| <b>CHAPTER 7 EMBEDDED WEB SERVER .....</b>                                                                                                                                    | <b>38</b> |
| 7.1 Product Information .....                                                                                                                                                 | 38        |
| 7.2 Application Information .....                                                                                                                                             | 39        |
| 7.3 Configuration.....                                                                                                                                                        | 39        |
| 7.3.1 General Settings.....                                                                                                                                                   | 39        |
| 7.3.2 Network Settings .....                                                                                                                                                  | 39        |
| 7.3.3 Security Settings.....                                                                                                                                                  | 40        |
| 7.3.4 Clock Settings.....                                                                                                                                                     | 41        |
| 7.3.5 File Management.....                                                                                                                                                    | 42        |
| 7.3.6 Firmware Update .....                                                                                                                                                   | 43        |
| 7.3.7 Product Reset.....                                                                                                                                                      | 43        |
| 7.4 Event Log.....                                                                                                                                                            | 43        |
| 7.5 Statistics.....                                                                                                                                                           | 44        |
| 7.6 Error Descriptions and Status .....                                                                                                                                       | 45        |
| 7.7 Display All Pages.....                                                                                                                                                    | 45        |
| 7.8 Custom HTML (graphics).....                                                                                                                                               | 45        |
| 7.9 Acknowledgements .....                                                                                                                                                    | 45        |
| 7.10 Product Support.....                                                                                                                                                     | 45        |
| <b>CHAPTER 8 ETHERNET PORT OPERATION .....</b>                                                                                                                                | <b>46</b> |
| 8.1 Ethernet Port Hardware Operation .....                                                                                                                                    | 46        |
| 8.2 Overview .....                                                                                                                                                            | 46        |
| 8.3 New Network Design Overview .....                                                                                                                                         | 47        |
| 8.3.1 Operational Notes for V2.00 Networking.....                                                                                                                             | 47        |
| 8.3.2 Ethernet Switch Configuration: NONE.....                                                                                                                                | 49        |
| 8.3.3 Ethernet Switch Configuration ALL.....                                                                                                                                  | 51        |
| 8.4 Existing Use Cases in 2500P-JACP Networking .....                                                                                                                         | 52        |
| 8.5 Networking V2.00 Setup Guide.....                                                                                                                                         | 53        |
| 8.5.1 All Installations.....                                                                                                                                                  | 54        |
| 8.5.2 Installation with 1 cable connected to JACP .....                                                                                                                       | 55        |
| 8.5.3 Installation with 2 cables connected to JACP, where Port 2 connects to a single downstream device (2500-Cxxx PLC or Ethernet/IP device).....                            | 56        |
| 8.5.4 Installation with 2 cables connected to JACP, where Port 2 connects to physically separate network with Ethernet/IP devices and/or SCADA communicating with OPC-UA..... | 58        |
| 8.6 New IP Address Display.....                                                                                                                                               | 59        |
| <b>APPENDIX A: SYSTEM ERROR CODES .....</b>                                                                                                                                   | <b>61</b> |
| CPU Startup Errors .....                                                                                                                                                      | 61        |
| Module Run Mode Startup Errors .....                                                                                                                                          | 62        |
| Firmware/Configuration Update Errors.....                                                                                                                                     | 64        |
| Execution Errors .....                                                                                                                                                        | 64        |
| SD Card Errors .....                                                                                                                                                          | 65        |
| Client Communication Errors .....                                                                                                                                             | 65        |
| Hardware Errors .....                                                                                                                                                         | 67        |

|                                                 |           |
|-------------------------------------------------|-----------|
| <b>APPENDIX B: IP ADDRESS INFORMATION .....</b> | <b>68</b> |
| IP Address Nomenclature .....                   | 68        |
| Using the Subnet Mask .....                     | 70        |
| CIDR Notation.....                              | 71        |
| Selecting an IP Address .....                   | 71        |
| Selecting a Multicast Address.....              | 72        |
| <b>APPENDIX C: SERIAL PORT WIRING .....</b>     | <b>74</b> |
| RS232 Wiring.....                               | 74        |
| RS422 Wiring.....                               | 75        |
| RS485 Wiring.....                               | 76        |
| <b>APPENDIX D: PRODUCT SPECIFICATIONS .....</b> | <b>77</b> |
| Environmental Specifications .....              | 77        |
| Agency Approvals (pending).....                 | 77        |
| Functional Specifications .....                 | 78        |
| <b>LIMITED PRODUCT WARRANTY .....</b>           | <b>80</b> |
| <b>REPAIR POLICY .....</b>                      | <b>82</b> |

---

# **CHAPTER 1 INTRODUCTION**

---

## **1.1 Janus Application Coprocessor Overview**

The CTI Janus Application Coprocessor (JACP) module augments the communications capability of CTI Janus Programmable Automation Controllers and CTI 2500 Series® Programmable Controllers. It also enables Simatic®/TI 505® Programmable Controllers to communicate using modern Ethernet protocols, such as Ethernet/IP and OPCUA. In some applications, it can function as a standalone controller, using Ethernet IO protocols, such as Ethernet/IP scanner and Modbus Client drivers.

The JACP module can be used in the following configurations:

- The module can be used as a co-processor and share data with a Simatic®/TI 505 PLC using the block transfer driver (Note: block transfer driver works with all 545/555 PLCs but does NOT work with 525/535 PLCs)
- The module can be used as a co-processor and share data with a CTI 2500 PLC using data cache or block transfer driver
- The module can be used as a co-processor and share data with a CTI Janus PAC using the binding protocol
- The module can be used in a standalone control situation the need to share data with another PLC is not required

**IMPORTANT NOTE:** CTI recommends that if the 2500-JACP is used with the CTI 2500-Cxxx PLC, the PLC firmware should be V9.22 or above for proper operation.

The JACP module can be installed in a local or remote base. When installed in a remote base with a standard Remote Base Controller (RBC), the performance of the Block Transfer driver, if used, will likely be degraded. When installed in a remote base with a Profibus RBC, the Block Transfer driver will not work, since the Profibus RBC does not support SFIO.

### **Flexible Programming Support**

The JACP module 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)

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**

The module provides two isolated Ethernet ports, which can operate independently of each other. They can be used to provide redundant network paths or to connect to different Ethernet networks. Since the module can be configured with two IP addresses, it can communicate concurrently on two different IP networks. **IMPORTANT NOTE:** Beginning with 2500-JACP firmware V2.00, changes are implemented in networking configuration and operation to prepare the product for later addition of PROFINET. See [ETHERNET PORT OPERATION](#) for more details.

## Ethernet Data Communications Protocols,

The JACP module supports the following data communications protocols:

- CAMP Client (used to communicate with CTI 2500 Series PLCs 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® Programmable Controllers)
- Block Transfer (enables communications with CTI 2500 Series® and Simatic®/TI 505 Programmable Controllers using the Special Function I/O protocol)
- 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))
- OPCUA Server (Provides data access services to any product that supports an OPCUA client)
- Custom TCP/UDP client and server applications using network socket management functions
- Network Data Exchange (binding)

## Ethernet I/O Protocols

The module supports:

- Open Modbus 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).
- Ethernet/IP Flex IO Client

## Serial Protocols

The module provides two serial ports. Each port can be configured for RS-232, RS-422, or RS-485 electrical interfaces. The serial ports can be used for the following communications protocols:

- Modbus RTU Master – Allows the module to function as a Modbus RTU Master
- Modbus RTU Slave – Allows the module to function as a Modbus RTU Slave
- General ASCII – Allows the module to send and receive ASCII Characters

## Web Server Interface

The module contains an embedded web server, which provides an interface to detailed information regarding the JACP 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 application data. (See Section [5.4 HTTP Data Server](#)).

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

## Online Change Support

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



### WARNING

***When making Online Changes, you MUST ensure no other users are connected to the JACP with Janus Workbench before proceeding with an online change. Having two or more users connected who are simultaneously making program changes and forcing variables can result in unexpected system operation.***

## Security

The module supports the following set of security features:

- “Secure Boot” process – encryption keys that verify the JACP is running an authenticated CTI version of the firmware
- Password protection for accessing JACP module 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 module Configuration settings via web server (Includes File Management and Firmware Update operations)
- Password protection for the JACP Operation pages (File Management/Firmware Update)
- Password protection for accessing visualization (HTML5 Graphics)
- The user program is compiled in Workbench on the PC and downloaded, which allows more user options for controlling access to the project source files
- Certificate-based security for OPCUA message signing and encryption.

## Compatibility

The JACP module is designed to work in the same manufacturing environment as CTI 2500 Series® PLCs and the CTI Janus PACs. It uses the same programming software as the CTI Janus PACs. 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. The Block Transfer protocol enables communication with Siemens®/TI505 PLCs using the Special Function IO protocol.

## High Performance

The JACP Module is powered by a high-performance SoC (System on Chip) with ARM®+ FPGA architecture providing considerable 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 JACP module 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 four 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
- Integrated version control.

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 module. For more information, refer to the Janus Workbench Help system.



---

## **CHAPTER 2    FRONT PANEL**

---

### **2.1 JACP Module Front Panel**

**1. Operational Status LEDs**

CPU GOOD  
RUN  
ERROR

**2. Alphameric Display**

**3. Reset Button**

**4. Ethernet Port 1 (1000 Mb)**

Link LED (LINK)  
Activity LED (ACT)

**5. Ethernet Port 2 (1000 Mb)**

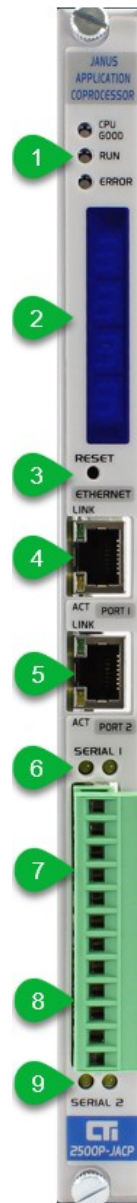
Link LED (LINK)  
Activity LED (ACT)

**6. Transmit and Receive LEDs – Serial Port 1**

**7. Serial Port 1 (Top Six Pins)**

**8. Serial Port 2 (Bottom Six Pins)**

**9. Transmit and Receive LEDs – Serial Port 2**



## 2.2 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 ( <b>LOGIC STOP</b> 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 display)                                                                                                                                                                                                    |
|          |        | 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.<br>(Error Code displayed on front panel display)<br>On initial power up, this signals that the hardware is powered and ready for software boot. |

## 2.3 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 along with 3 dots after the error code indicating multiple errors. See [APPENDIX A SYSTEM ERROR CODES](#) for a list of system error codes and descriptions.

## 2.4 Reset Pushbutton

When enabled, the **RESET** pushbutton provides a direct method to clear exceptions, reset module configuration values to default values, or restore factory defaults without requiring access to **Janus Workbench** or the module 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 [Setting the Module Switches](#)*

## 2.5 Ethernet Communications Ports

The RJ-45 Ethernet ports, labeled **PORT 1 AND PORT 2**, are identical in their operation and usage. Both ports are capable of operating at 1000Mb (1Gb) 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). Both 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 JACP 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](#).

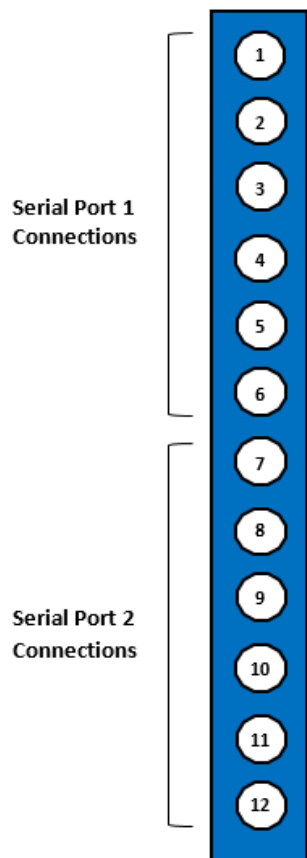
Each Ethernet port connector contains two embedded LEDs. The **LINK** LED (top) indicates whether the Ethernet port is successfully connected to another Ethernet device, such as a network switch. The **ACTIVITY** LED (bottom) provides visual indication that Ethernet packets are being received or transmitted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

| LED               | State            | Indication                                                                              |
|-------------------|------------------|-----------------------------------------------------------------------------------------|
| Link              | Off              | Ethernet link is not established (unconnected)                                          |
|                   | On               | Ethernet link is established (connected)                                                |
| Act<br>(Activity) | Off              | No Ethernet frames are being transmitted on the network to which the port is connected. |
|                   | On<br>(Blinking) | Ethernet frames are being transmitted on the network to which the port is connected     |

## 2.6 Serial Ports

The front panel 12-pin plug connector provides the interface to both serial ports. This connector replaces the DB9 Male D-Sub connector used for serial port connections in most legacy devices. The plug connector provides user-friendly terminals that do not require soldering, and wiring connections can be easily verified and/or changed as necessary.

The top six pins are connections for **Serial Port 1** and the bottom six pins are used for connection to **Serial Port 2**.



The pin-out (i.e. function for each serial port terminal) varies according to the specified electrical interface (RS232, RS422, or RS485). See [APPENDIX C: Serial Port Wiring](#) for the pin-out for each electrical interface.

---

## **CHAPTER 3    INSTALLATION**

---

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

### **3.1 Installation Planning**

#### **3.1.1 Choosing the IP Address and related Parameters**

Before you can use the Ethernet ports, the JACP must be configured with network parameters for the IP Address 1, including IP address, network mask, and the default gateway. The module also allows you to set an additional address, IP Address 2 if you wish (see [ETHERNET PORT OPERATION](#) for more information). 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 [Network Settings](#) for information on setting the network parameters.

#### **3.1.2 Power Requirements**

The JACP module consumes 7 watts of +5 VDC power. To calculate the total power required for the base, you need to add the power requirements for the JACP and other modules you will install in the base.

#### **3.1.3 SD Card Selection**

**System SD Card** (see [SD Card Installation](#), [Setting the IP Address](#) and [Direct File Replacement](#))

The JACP ships with software pre-installed on a standard-size 16GB SDHC card with a speed rating of Class 10 / U1 (10MB/sec). If it becomes necessary to replace the card, it must be replaced with one of equivalent or better capabilities.

Cards with this speed rating will usually be marked with one of these symbols:



**User SD Card** (see [SD Card Installation](#) and [User SD Card Firmware Update](#))

The User SD card slot works with standard (SD) and high capacity (SDHC) memory cards with speed rating of 4MB/sec (Class 4) or higher.

## 3.2 Installing the Module

### 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 JACP module 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 SD Card Installation

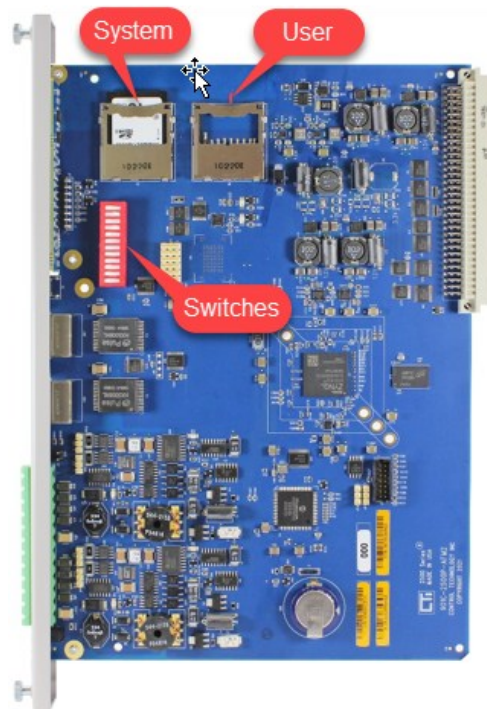
The JACP module uses a Secure Data High Capacity (SDHC) card to store configuration data, executable program, application program source files, and user data files. This card is pre-installed in the System SD card receptacle on all units shipped from the factory. Contact CTI support if the SD card is missing. If you need to replace the System SD card, an SDHC card with a class rating of  is required. CTI recommends you purchase an SD card with an industrial rating. A capacity of 16GB is usually sufficient.

**Because all configuration and operational files are contained on the System SD card, the complete module profile can be transferred to another unit simply by swapping SD cards.**

To remove and replace the System SD card:

- Remove power to the base.
- Remove the JACP 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

Some operations require a second (User) SD card. When required, insert an SDHC card in the User SD Card receptacle. For this card, an SDHC card with class rating of  is sufficient.



### 3.2.3 Setting the Module Switches

The location of the module switches is shown above. See the following table for information about the switch functions.

| Switch Position | Use                         | Open Position    | Closed Position                                                                                                                                                                                                                           |
|-----------------|-----------------------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1               | Remote Firmware Update      | Disabled         | Enables firmware update via web server. See <a href="#">Section 6.3</a> for details.                                                                                                                                                      |
| 2               | SD Card Firmware Update     | Normal operation | JACP enters <i>User SD Card Firmware Update</i> mode at startup. See <a href="#">Section 6.2</a> 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 <a href="#">Section 5.3</a> .                                                                                    |
| 4               | SD Card Ethernet Port Setup | Disabled         | Allows user to configure JACP Ethernet Port 1 via User SD Card. NOTE: This setting works <u>ONLY</u> if Switch 2 is OPEN. See <a href="#">Section 3.2.8</a> . NOTE: SD Card Ethernet Port setup is removed beginning with Firmware V2.00. |
| 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                    |                  |                                                                                                                                                                                                                                           |

### 3.2.4 Shipping Configuration of Switches

| Switch Position | Use                                                                                                        | Shipping Configuration | Open Position    |
|-----------------|------------------------------------------------------------------------------------------------------------|------------------------|------------------|
| 1               | Remote Firmware Update                                                                                     | Open                   | Disabled         |
| 2               | SD Card Firmware Update                                                                                    | Open                   | Normal operation |
| 3               | Clear Exception Pushbutton                                                                                 | Open                   | Disabled         |
| 4               | SD Card Ethernet Port Setup<br>NOTE: SD Card Ethernet Port setup is removed beginning with Firmware V2.00. | Open                   | Disabled         |
| 5               | Remote Controller Reset                                                                                    | Open                   | Disabled         |
| 6 - 12          | Reserved                                                                                                   | Open                   |                  |

### 3.2.5 Physical Installation

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



#### WARNING

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

### 3.2.6 Applying Power to the Base

Apply AC power to the base power supply. The CPU GOOD LED on the module should illuminate, indicating that power is being supplied to the base connector. The JACP module should power up. See [Section 5.2 Module Startup](#) for additional information.

### 3.2.7 Connecting the Module to a Data Network

To connect the JACP module to an Ethernet network, insert an Ethernet cable that is rated Category 5e into the RJ-45 connector of either front panel Ethernet port: PORT 1, or PORT 2. 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.

### 3.2.8 Startup from Factory Defaults

If you are starting up using the factory default, the module will attempt to obtain an IP address using DHCP (Dynamic Host Configuration Protocol). If a valid response is received, the module will use the IP address parameters provided. If not, the module 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 module 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. NOTE: SD Card Ethernet Port setup is removed beginning with Firmware V2.00.*

## 3.2.9 Setting the IP Address

### User SD Card Ethernet Port Setup

**NOTE:** User SD Card Ethernet Port setup is removed beginning with Firmware V2.00.

The **User SD Card Ethernet Port Setup** procedure provides an alternate method to specify a fixed IP Address for the module 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 'User 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: 192.168.001.011, 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 are optional. If you don't want to specify a default gateway address, you should omit this entry.

Examples:

With Gateway Address:

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

Without Gateway Address:

```
[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. The file system of the user 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 module from the base, set Module Switch 4 to CLOSED position (and ensure Module Switch 2 is OPEN) and insert that card into the User SD Card receptacle on the JACP PC board. Re-install the module into the base and restore power.
- d) On power up, the module 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 module will not accept connections from **Janus Workbench**.

- e) Next, the module will attempt to find the 'cti.ini' configuration file in the root directory of the User 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 User SD Card receptacle:  
Error 370 (**User SD Card Not Accessible**) is reported.
  - If the cti.ini file cannot be found in the SD card root folder:  
Error 250 (**User SD Card – Update File Not Found**) is reported.
  - If the cti.ini file does not contain the required keywords/values:  
Error 260 (**User SD Card - Invalid Update File**) is reported.
- g) If an error is encountered, the procedure will stop. After correcting the problem, you must re-power the module.
- h) If the operation successfully completes, the parameterization data is saved for the next module startup, the cti.ini file on the User 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 module from the base, set Module Switch 4 to the OPEN position, remove the SD card from the User SD receptacle (optional), 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.

## System SD Card Ethernet Port Setup

Beginning with Firmware V2.00, User SD Card Ethernet support is no longer available. In the unlikely event that it is not possible to use the Web Server for Ethernet port setup, it is possible to directly edit the "cti.ini" file on the system SD card to set up the IP addressing and other parameters for your Ethernet ports. **IMPORTANT: Use extreme care when making changes to the System SD card. If the wrong files are accidentally deleted, you can inadvertently delete your user application and/or the JACP operating system. When making changes, you should ONLY edit the "cti.ini" file and follow the directions below carefully.**

- Power off the module
- Remove the System SD Card
- Place the system SD card into an SD Card reader and plug into your PC
- Navigate to the "ctiplc" folder on the SD card
- Rename the existing "cti.ini" file to "cti.bak"
- Using a text editor, create a text file with the following contents. Alternatively, you can copy the cti.ini from another working JACP module to save time creating and editing this file. The contents below are the "default" configuration which brings the module up using a DHCP server for its IP address. If you prefer to have a static IP, you would change "usingdhcp" to false and put in your desired IP/subnet in the [NET0] section.

```
[NET0]
usingdhcp = true
displayed = true
ip =
```

```
subnetmask =  
gateway =  
default =
```

```
[SWITCH]  
mode = none  
profinetgroup = -1  
datacachegroup = -1  
eipgroup = -1
```

```
[DNS]  
usemanualdns = false  
domainsuffix =  
dns1 =  
dns2 =
```

```
[NET1]  
usingdhcp = false  
displayed = false  
ip =  
subnetmask =  
gateway =  
default = false
```

[NET0] contains the configuration for IP Address 1  
[NET1] contains the configuration for IP Address 2  
[SWITCH] contains the switch configuration.  
[DNS] contains the dns configuration

Note: default" may be present in a file but it is no longer used, included it because it may exist in a file.

**displayed** – determines whether the IP Address is displayed on the front panel or not. Possible values: true, false

**gateway** – the gateway address for the IP. When isolating ports, this value should be blank.

**mode** - this is either "none" for no isolation or "all" for both ports are isolated from each other. See [ETHERNET PORT OPERATION](#) and [Network Settings](#) for more information.

**profinetgroup, datacachegroup, and eipgroup** define the port group the protocol is assigned to. Possible values are can be 0, 1, or -1 (disabled). See [ETHERNET PORT OPERATION](#) and [Network Settings](#) for more information.

**usemanualdns** – TRUE means use the DNS parameters in this section. FALSE means do not use the parameters in this setting.

**domainsuffix** - a domain name appended to short, unqualified computer names (like "server1") to create a [Fully Qualified Domain Name](#) (FQDN, like "server1.example.com") for network communication

- Save the file using the name "cti.ini" to the "ctiplc" folder on the SD card.
- Return the System SD card to the JACP and power up
- The JACP should come up and the programmed IP Address(es) should be displayed on the front panel (if you have elected using the "displayed" parameter

## Web Server IP Address Configuration

Once your PC and the module 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 module 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 Module Configuration Options

You may also use the embedded web server to configure other module 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 module. 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 (Default):** If startup state is *Restore Last State*, the project startup state is dependent on operational state when the JACP was reset.
  - If the operational state was APPLICATION STOP, the project will start in APPLICATION STOP state.
  - If the operational state was RUN, the project will start in RUN state with *Warm Start* initialization.
  - If the operational state was ERROR, the project will start in APPLICATION STOP state.
- **Application Stop:** Starts with 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
- **NOTE:** Auto-Run Hot Start is not supported on JACP because the product does not have a battery to support saving of variable values on power-down. Janus PLCs DO support Auto-Run Hot Start.

NOTE: On startup following reset caused by pressing the front panel 'Reset' button, the application program state is always set to 'RUNNING – Cold Start' unless the JACP 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

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.

## 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 IP Address 1 and IP Address 2. The two IP addresses must be on different subnets with no overlap.

The IP Address 1 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. IP Address 2 must be statically configured. See [ETHERNET PORT OPERATION](#) for more information.

### 4.2.2 Fieldbus Port Group Assignments

These settings configure which Port Groups fieldbus protocols use. See [ETHERNET PORT OPERATION](#) for information on Port Groups.

- Data Cache – possible settings are Disabled, Port Group 1, Port Group 2
- Ethernet/IP – possible settings are Disabled, Port Group 1, Port Group 2

The default settings are “Disabled”. If your application uses Data Cache and/or Ethernet/IP, you must change these settings to one of the Port Groups.

### 4.2.3 Internal Ethernet Switch Configuration

The Internal Ethernet Switch configuration determines how the 2 ports on the JACP operate. See [ETHERNET PORT OPERATION](#) for more information. By default, switch setting is NONE, meaning the ports are not isolated from each other. In this configuration, typically only IP Address 1 is configured and only a single network cable is inserted into Port 1.

When the switch mode is NONE, you must not insert cables into both ports unless:

- The cables go to 2 physically separate networks OR
- You are “daisy chaining” to another device which is not connected to a network (ie directly to a 2500-Cxxx PLC)

Inserting cables into both ports which go to the same network will result in a switch loop.

When the switch mode is ALL, both ports are isolated from each other, and cables can be inserted into both ports regardless of whether the cables are connected to the same network or different physical networks. This mode is typically used when you want to configure an IP Address 2 which is used to communicate using some fieldbus protocols on a different network.

## 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: Anyone with Administrator privileges can delete other users (administrators) from the configuration. This is done for simplicity and ease of use. It allows for the deletion of users who forgot their passwords.

#### 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 without 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 JACP module 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 JACP module.

Click on the **APPLY** button to apply settings. A confirmation message should be displayed indicating that the module 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 JACP\_SET\_RTC function block in a logic program
- **Sync with Remote NTP Server:** Obtains the time from an NTP (Network Time Protocol) server.
- **Sync with 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.
- **Sync with Block Transfer Host:** Sets clock with time read from a Siemens 505 Series or CTI 2500 Series Host PLC using Special Function I/O in the Block Transfer driver

**NOTE:** you must have a default gateway set in [Network Settings](#) to use NTP time sync.

**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.
- **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 JACP module operation. Additional information may be found in the *Janus Workbench* Help.

### 5.1 JACP Module Operation Overview

1. The JACP module 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 module 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 2.4 RESET Pushbutton](#).
2. *Janus Workbench* can be used to transfer module 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.

**Warm Start** option is not available immediately after an application is downloaded from *Janus Workbench* to the module.
3. Module 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 System SD card at the end of every scan cycle. **NOTE:** *The limit for RETAIN variables is 12,232 bytes.* 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.
  - **IMPORTANT NOTE:** When using **RETAIN** variables, the JACP firmware must calculate an error checking algorithm on each cycle and must store the variable values in non-volatile MRAM since there is no battery backup. When there are just a few **RETAIN** variables, the time to do this process is negligible,

but with large numbers of variables the time can become significant. Projects on JACP should minimize the use of **RETAIN** variables if short cycle times are important.

5. All user data files created by user logic programs will be stored on the System SD card in the /ctiplc/user folder. To access them externally, the user must manually transfer these files to the SD card in the User SD Card receptacle on the PC board using the FILE MANAGEMENT web page.
6. When a project is downloaded from CTI Workbench while the run-time is stopped, that project is stored on the System 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 System SD card. The previous program and source files (if they exist) are renamed and saved. Any older versions are overwritten. **WARNING:** *Be sure that you do not store extraneous files in your project source file area on your PC or else the source file download will grow and the procedure may take longer than needed*

The state of the application program following download is determined by selection for **Operation following Project Download** in the [CONFIGURATION/GENERAL SETTINGS](#) web page. The application remains in this state until user changes the program state or the module is reset.

7. The module 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 module cycle and limits maximum cycle time to one (1) second.
8. The module firmware also includes a **System Watchdog** with preset of 6 seconds that expires only if the module operating system becomes inoperable. The expiration of the System Watchdog will cause the JACP module to reboot.
9. If a module execution error is detected, the event is recorded in the Event Log and module will enter the **ERROR** state. **ERROR** state can be cleared by connecting Workbench to the module or by resetting the module via web page or **RESET** button (if either is enabled).

## 5.2 Module Startup

This section describes the sequence of events that occur during a power-on startup or after a module 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 module. This provides indication that the module is powered and attempting to decrypt and load the contents of the boot.bin file on the System 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 SYSTEM SD card must be formatted as FAT32 (only the USER SD card supports EXFAT)
- 2) If step 1 is successful, the module starts a ‘Secure boot’ process. Each component of the image file (boot manager, operating system, module 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/NETWORK SETTINGS web page.

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. This IP address, which is not routable, can be used as a temporary IP address until other IP assignment methods are configured.

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 CONFIGURATION/GENERAL SETTINGS web page Startup Options.

## 5.3 Reset Pushbutton Operation

When enabled, the **RESET** pushbutton provides a direct method to clear exceptions, reset module configuration values to default values, or restore factory defaults without requiring access to *Janus Workbench* or the module web server. In cases where the user selected password(s) for web server access is lost, this is the only method that can be 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 module event log. The **RESET** pushbutton will function only when Switch 3 is in the CLOSED (ON) position.

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

- **CLEAR EXCEPTION**

Pressing and holding the recessed pushbutton for greater than 5 seconds causes the Janus module 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 module 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 module reset.

If the module 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 module 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 module 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
- Module 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 module 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 module configuration settings (as reported on the module Configuration web pages) are restored to default values.

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

- **RESTORE FACTORY DEFAULTS**

Pressing and holding the recessed pushbutton for greater than 15 seconds causes the module to return to as-shipped factory defaults by pressing the button for greater than 15 seconds. This action will reset all JACP 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 System 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 module 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 JACP module includes an HTML Data Server that provides an embedded HMI function. Using the Data Server, you can access "live" 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 JACP 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 module 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 module web server **CONFIGURATION/NETWORK SETTINGS** page. If you wish to encrypt the communications between the web server and the JACP module, secure (https:) connections can optionally be selected (see [Section 4.3 Security Settings](#)).

---

## CHAPTER 6      **UPDATING FIRMWARE**

---

### 6.1 Overview

The JACP module stores the operating firmware on the System SD Card. 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 JACP module. 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 JACP module
- 2) Extraction of OS/firmware file,
- 3) Copy of the OS/firmware file to the root folder of the System 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 User SD Card Firmware Update

Firmware should normally be updated using the web server Configuration – Firmware Update page, as this method is much easier and can be performed without shutting down the module to access the User SD Card slot. The SD Card method outlined below is retained for compatibility with older installations.

The procedure requires the following steps:

- 1) Copy the new firmware file downloaded from CTI website to root directory of an SD card. The firmware file can be a compressed zip file or binary file (boot.bin) extracted from the zip file. NOTE: *ensure that only one .zip or boot.bin file exists on the root directory*
- 2) Turn off power to the chassis, remove the JACP module, set Module Switch 2 to CLOSED position, ensure Module Switch 4 is OPEN, and install the SD card into the User SD Card receptacle (See location [here](#)) Then re-install the module into the chassis, and restore power to the chassis.
- 3) On power-up, module attempts to find the firmware file in the root directory of the “User” SD card.
- 4) If any of the following errors occur, a **Firmware Update Error** occurs and the appropriate error code (see below) is displayed.
  - If a properly formatted SD card is not inserted into the user SD card receptacle, ‘UFEr’ is displayed and error Error 370 (**User SD Card Not Accessible**) is logged.
  - If file with ‘.zip’ extension or file named ‘boot.bin’ cannot be found in the SD card root folder, ‘UFEr’ is displayed and Error 250 (**User SD Card – Update File Not found**) is logged. Note: in firmware prior to V2.00, this error was also used to indicate SD card Ethernet Port Setup error.

- If the update file is found but not valid for the JACP product, 'UFEr' is displayed and Error 260 (**User SD Card -Invalid Update File**) is logged. Note: in firmware prior to V2.00, this error was also used to indicate SD card Ethernet Port Setup error.

If one of these errors exists, the firmware update procedure is terminated and you must correct the problem and repeat the firmware procedure.

- 5) If the firmware file is found and validated, **UFdn** is displayed on the front panel display to indicate success. This action is also reported in the Event Log.
- 6) When the firmware has been successfully updated, turn off power to the chassis, remove the module, and set Module Switch 2 to the OPEN position. You may also choose to remove the SD card from the user SD card receptacle at this time. Then re-install the module and re-apply power to the chassis to return to normal operation.

## 6.3 Remote Firmware Update

The **Remote Firmware Update** method allows the JACP firmware to be updated via network connection to web server. This procedure 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 JACP 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 module operational mode is checked. To update firmware, the module 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 JACP 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 module is ready for firmware update.

### NOTE

*The [Refresh] button can be pressed at any time to recheck JACP operational mode and update the module 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 Module operational state.*

- 4) Select the firmware file to download to the module by pressing the **[BROWSE]** button. The selected file can be a zip file – normally named CTI\_JANUS\_ACP\_Vnn\_nn.zip (where nn\_nn represents the version number) or an 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 module 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 module is rebooting**. This action is also reported in the Event Log.
- 9) The module then resets to complete the operation and restarts using the updated firmware.

During the module 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 module 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 module 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\_ACP\_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 module, and insert the SD card containing the boot.bin file into the System SD card slot (see [Section 3.2.2](#)).
- 4) Ensure Module Switch 2 and Switch 4 are in the OPEN position.
- 5) Reinstall the module and restore power to the base.
- 6) The module should start up as described in [Section 5.2](#).

---

## **CHAPTER 7      EMBEDDED WEB SERVER**

---

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

### **7.1 Product Information**

This page provides information about the module

- **Product Number**
- **Product Name**
- **Serial Number**
- **Manufacture Date**
- **Module Identifier:** Assigned by user in the GENERAL SETTINGS page
- **Hardware Configuration:** Designator that allows software to determine hardware compatibility
- **Module Firmware Version**
- **Module Firmware Date**
- **FPGA Version**
- **Build Information 1 & 2:** (CTI development and support information)
- **Clock Synchronization Mode:** Determines how the module clock is set)
- **Startup Mode:** Determines how the module starts up when reset or powered up
- **User SD Card Status:** If inserted, displays Utilization Percentage
- **Profinet Activated Status**
- **HTTPS Basic Authentication Enabled:** Authentication for webserver access
- **HTTPS Encryption Enabled:** Encryption of web server traffic
- **Internal Ethernet Switch Mode**
- **CPU Temperature (° C)**
- **Dipswitch Settings**
- **User Jumper Selections**
- **Network Settings for Port Groups 1 and 2**
  - **Port Group**
  - **MAC Address**
  - **IP Address**
  - **Subnet Mask**
  - **Default Gateway Address**
  - **IP Address Method**
  - **Data Cache Port Group**
  - **Ethernet/IP Port Group**

## 7.2 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 )
- **Project Run Time:** Days-Hours-Minutes-Seconds the project has been running
- **Active Error Codes:** See [Error Descriptions and Status](#) web page description for details.
- **System Resources:** Displays total memory, free memory, open files open TCP sockets, open UDP sockets for the operating system
- **Product Resources:** Displays used virtual memory, open files, open TCP sockets, and open UDP sockets 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).

## 7.3 Configuration

### 7.3.1 General Settings

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

- **Module Identifier** - Optional 16-character text field used to identify the JACP
- **Operation following Module Reset**
  - Restore Last State (Default)
  - Application Stop
  - Auto-Run Cold Start,
  - Auto-Run Warm 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

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

### 7.3.2 Network Settings

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

- **IP Address 1 Configuration** (configuration is required)
  - Display IP Address on Front Panel: checkbox to display the IP Address

- Automatic (DHCP): Designates that IP parameters will be assigned using DHCP (Dynamic Host Configuration Protocol)
- Static: IP v4 Address and CIDR for subnet mask setting
- Default Gateway
- **IP Address 2 Configuration** (optional)
  - Display IP Address on Front Panel: checkbox to display the IP Address
  - Static: IP v4 Address and CIDR for subnet mask setting
- **Internal Ethernet Switch Configuration.** Allows you to configure how the internal Ethernet Switch operates. See [ETHERNET PORT OPERATION](#) for additional information.
- **Fieldbus Port Group Assignments.** Configure which Port Group are used by Data Cache and Ethernet/IP.
  - **Data Cache** – Disabled, Port Group 1, Port Group 2
  - **Ethernet/IP** – Disabled, Port Group 1, Port Group 2

NOTE: the web page includes checks for valid IP addresses, switch configuration, and port group assignments. These checks are performed when the APPLY button is clicked, and any errors are displayed. If errors are found, the configuration changes are not saved.

If no errors are found, the new configuration goes into effect immediately after selecting the APPLY button and confirming the action.

### 7.3.3 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 selected, the updated configuration parameters are saved and a confirmation message is displayed.

### 7.3.4 Clock Settings

Determines how the module 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)
- **Sync with 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 following must be entered when ‘Remote NTP Server’ selected:

- Time Zone Region
- Time Zone City
- Sync Host IP Address

**NOTE:** you must have a default gateway set in [Network Settings](#) to use NTP time sync.

- **Sync with 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 selected, 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.

- **Sync with Block Transfer Host PLC**

The Block Transfer interface reads time from the Host PLC immediately upon configuring the SFIO interface and then once every 4 seconds.

### 7.3.5 File Management

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

- **Copy to User SD Card:** Copies selected user file(s) from the System SD card '/ctiplc' folder
- **Copy from User SD Card:** Copies selected user file(s) or folder to the System SD card '/ctiplc/user' or '/ctiplc/graphics' folder
- **Replicate the System:** Copies files from System SD card to User SD card necessary to replicate the OS and application on another JACP module
- **Download File to Computer:** Downloads a selected file from the System 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 System SD card
- **Import Public Certificates from Computer:** Saves the selected X.509 certificate file (\*.der) to the System SD card.
- **Import Private Key from Computer:** Saves the selected Private Key file to the System SD card.
- **Delete Files from System SD Card:** Deletes selected files from the '/user' or '/graphics' folder on the System SD card.
- **Copy Core Dump Files to User SD Card:** Creates a zip file of the selected Core Dump file and transfers it to the User SD card.
- **Download Core Dump Files to Computer:** Creates a zip file of the selected Core Dump file and transfers it to the computer.
- **Delete Core Dump Files:** Deletes selected Core Dump files on the System SD card.

#### NOTES:

- An error message will be displayed if the 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 User SD card, it must be inserted and detected by the system (via Status message) before SD card file transfer can start.
- The [IMPORT] button initiates the import operation.
- 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.

### 7.3.6 Firmware Update

This page provides a method to initiate a *Remote Firmware Update* for the JACP module. For more details, see [Section 6.3](#).

- [REFRESH] pushbutton is used to recheck the module operational status.
- [CHOOSE FILE] 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 (Switch 1 position, Warning Acknowledgement checkbox, and JACP 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.

### 7.3.7 Product Reset

This page provides a method to remotely the reset of the JACP module. 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 JACP web server will be lost after any of the above actions are taken. Any action other than 'Clear Exception' will force the JACP to lose its IP address.*

## 7.4 Event Log

The Event Log maintains a history of user actions, operational states, application settings, and system-level errors that affect the module 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 the Event (not shown)

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

| Event Log                                |                                                                                                              |                                                                                                                         |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| 0 Pending Events, Max Pending Events = 1 |                                                                                                              |                                                                                                                         |
| 9                                        | Category: Product Information Events (54)<br>Ethernet Link Status Change (15003)<br>Ethernet Ports Active: A | Created[2022-08-22 17:14:40] Session#6<br>Updated[2022-08-22 17:14:40] Reps:0<br>CDisplay.cpp InternalThreadEntry 347 0 |
| 8                                        | Category: Application Events (6)<br>Workbench Application Start (50017)<br>Project: PRTEST2 [V3] Warm Start  | Created[2022-08-22 17:14:39] Session#6<br>Updated[2022-08-22 17:14:39] Reps:0<br>AbramsFalls.cpp _StartVmThread 1340 0  |
| 7                                        | Category: Application Events (6)<br>Firmware Startup (50000)<br>Janus ACP Classic V1 v01.04 2022-06-20       | Created[2022-08-22 17:14:38] Session#6<br>Updated[2022-08-22 17:14:38] Reps:0<br>AbramsFalls.cpp main 447 0             |

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.

## 7.5 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:

- **Communications Sessions:**
  - 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:
  - Module scan
  - Binding Subscriber
  - I/O Exchange
  - Modbus Master and Slave
  - Binding Publisher
  - User Logic Programs
  - Ethernet/IP
  - I/O Exchange Details
- **Fieldbus Statistics:** Displays information regarding configured fieldbus drivers (except Modbus).
- **Net Statistics:** Displays information regarding the TCP/IP stack.
- **Serial Port Statistics:** Displays statistics related to serial port communications

## 7.6 Error Descriptions and Status

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

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

Active Errors are shown in red.

## 7.7 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.

## 7.8 Custom HTML (graphics)

Displays list of user-generated graphics pages that have been created and downloaded to the appropriate folder (ctiplc/graphics) on the System 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.

## 7.9 Acknowledgements

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

## 7.10 Product Support

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

---

## CHAPTER 8 ETHERNET PORT OPERATION

---

**IMPORTANT NOTE:** This chapter describes JACP Ethernet Port operation with Firmware V2.00 and later. If you have earlier firmware, please refer to Version 2.6 (or earlier) of this 2500P-JACP Installation and Operation Guide.

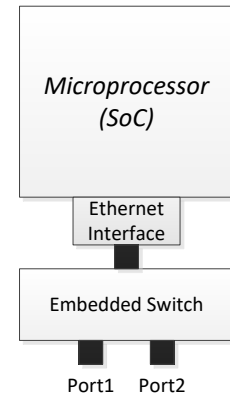
### 8.1 Ethernet Port Hardware Operation

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 JACP module 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 1 and 2) are not isolated from each other. Frames entering one port are forwarded to the other ports. In this default “non-isolated” mode, you must not plug cables into both Ports 1 and 2 unless the cables go to 2 physically separate networks.

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 port or when the destination address is a multicast or broadcast address. The switch does not forward frames to the microprocessor that do not meet these criteria, preventing them from consuming microprocessor resources.

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.



### 8.2 Overview

Version 2.00 firmware brings significant changes to networking using the 2500P-JACP. These changes were necessary to prepare the product for future inclusion of PROFINET as it requires a dedicated isolated port for the network communications.

This chapter outlines how V2.00 networking works and is a guide for changes that may be required for your JACP Workbench application when upgrading to V2.00 firmware.

The JACP is designed to operate as a co-processor in conjunction with the SIMATIC® 505 Series or CTI 2500 Series PLC acting as Host PLC to manage and control a process. The JACP enhances the Host PLC by providing drivers for

multiple Ethernet protocols and serial protocols for communicating with external devices. Two methods are available for high-speed data transfer to/from the Host PLC: Data Cache and Block Transfer.

The JACP can be used in the following configurations:

- As a co-processor and share data with a Simatic®/TI 545/555 or CTI 2500 Series® PLC using the Block Transfer driver over the local backplane
- As a co-processor and share data with a CTI 2500 Series® PLC using the Data Cache protocol over Ethernet
- As a co-processor and share data with a CTI Janus PAC using the binding protocol
- As a standalone controller with no need to share data with any other PLC

The JACP may be installed in a local or remote base. When installed in a remote base, the performance of the Block Transfer driver is degraded. When installed in a remote base with a Profibus RBC, the Block Transfer driver will not work, since the Profibus RBC does not support Special Function I/O.

## 8.3 New Network Design Overview

Beginning with Firmware V2.00, a new network design was implemented in conjunction with the introduction of an updated operating system and a new internal network switch driver. Below is a summary of features with the new network design.

- The internal Ethernet switch now has the capability to “group” the 2 physical ports together into logical “Port Groups” and forward packets between them, or completely isolate them from each other. This capability existed in previous firmware versions, but now the user has more explicit configuration control over the interface. There are 2 Port Groups available: Port Group 1 and Port Group 2.
- When the physical ports are grouped together and not isolated, they share a MAC address. When they are isolated, each port gets its own MAC address.
- Setup of the Port Groups is made by selecting the Ethernet Switch Configuration on the **Network Settings** web page. There are 2 pre-configured Switch settings: NONE (no isolation) and ALL (ports isolated)
- Up to 2 IP Addresses can be defined, and the Network Settings web page Ethernet Switch Configuration determines which IP Address(es) are available on each physical port.
- New settings on the module Network Configuration Web page allow selection of **Fieldbus Port Group Assignments**. This setting controls which Port Group is used for Data Cache, Ethernet/IP (Scanner, Adapter, Flex IO, Tag Client), and PROFINET (future)
- Ethernet/IP Tag Server, CAMP Server, Modbus Server, and Workbench connections will work over any configured IP Address or physical port.

### 8.3.1 Operational Notes for V2.00 Networking

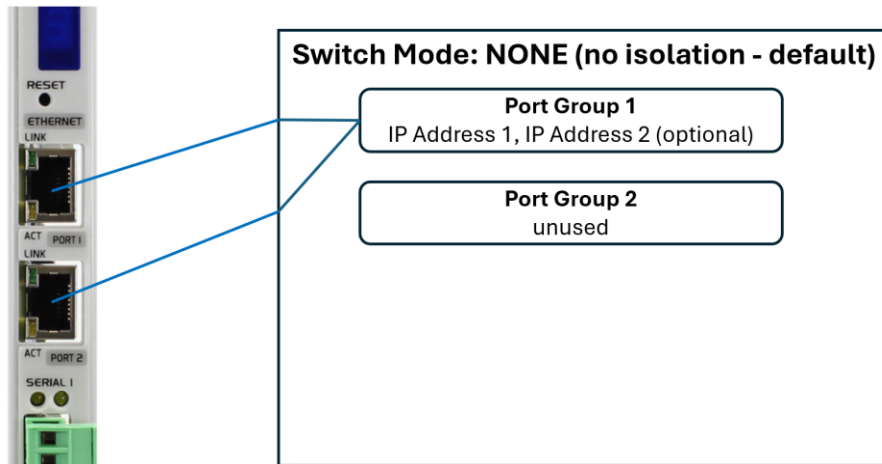
- A total of 2 IP addresses can be configured on the JACP. Each address must be on a unique and separate subnet, and the subnets cannot overlap. This requirement is unchanged from previous JACP firmware versions. For example, if the first IP address is 172.18.69.10/20 (255.255.240.0)

then that network consists of all the addresses 172.18.64.1 - 172.18.79.254 inclusive. So, for this example you could not configure a second IP address as 172.18.75.10/24 (255.255.255.0) since that second network includes the addresses 172.18.75.1 - 172.18.75.254. This configuration would give you an overlap between the 2 subnets. The web page will check configured IP addresses for validity when you click the “Apply” button and will notify if any errors are present.

- Be aware that in future firmware releases that include PROFINET, the PROFINET Device or Controller address will count as the second of the 2 allowed IP addresses above.
- Only IP Address 1 is allowed to be configured as DHCP. IP Address 2, if used, must be configured as Static. DHCP is rarely, if ever, used since the address can change each time the product restarts. It is useful for initial startup “out of the box” only.
- IP Address 1 and IP Address 2 are automatically assigned to Port Groups. This setting is not user-configurable. IP Address 1 is always assigned to Port Group 1. IP Address 2 is assigned to Port Group 1 when Switch Mode is NONE. IP Address 2 is assigned to Port Group 2 when Switch Mode is ALL.
- The network configuration web page also allows selecting which Port Group is used for Ethernet/IP and DataCache.
  - For both Ethernet/IP and Data Cache, the choices are Disabled, Port Group 1, Port Group 2. The default (after firmware upgrade to V2.00) is “Disabled”. **IMPORTANT NOTE:** since this setting comes up as “Disabled” after firmware upgrade to V2.00, you will need to edit the Port Group configuration on the Network Settings web page if your application uses Ethernet/IP or Data Cache.
- Other protocols such as CAMP, Modbus, MQTT, Binding, and Workbench connections are automatically handled using the appropriate IP address and Port Group.
  - For example, if the JACP IP Address 1 is 192.168.1.10/24 and IP Address 2 is 192.168.2.10/24, then either address can be used for these protocols (ie CAMP Client or Modbus Client could communicate on either network). This is true whether the Ethernet Switch is in NONE or ALL.
- Ethernet/IP Tag Server, CAMP Server, Modbus Server, and Workbench connections will work over any configured IP Address or physical port
- Other notes:
  - Ethernet/IP and OPC get their IP Address assignment in the corresponding Fieldbus I/O configuration in Workbench.
  - Since a gateway is used when sending packets *outside* of your network, if you wish to isolate a port, then you are likely most interested in NOT configuring a gateway address because you do NOT wish any packets to be forwarded to another network.

### 8.3.2 Ethernet Switch Configuration: NONE

The diagram below shows the port operation when Ethernet Switch Configuration is NONE.

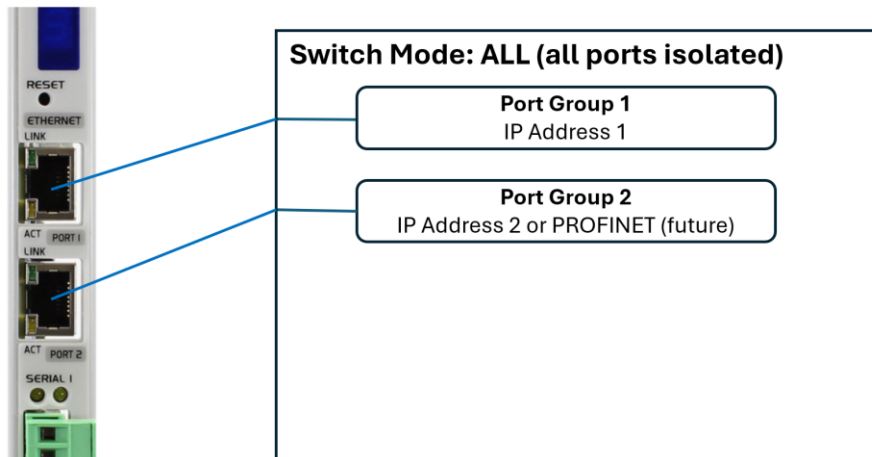


- Emulates the way the JACP worked previously in most applications
- Ports 1 and 2 on the front panel share a MAC address
- IP Address 1 and (optional) IP Address 2 are available on both physical ports. These two IP Addresses must be on different subnets.
- Packets are forwarded between Ports 1 and 2
- Example Use Case 1 (most common):
  - Only one IP Address is configured.
  - Port 1 is plugged into your factory network.
  - Port 2 is not used.
  - IP Address 1 is used by all protocols: Workbench, CAMP, OPC-UA, Modbus, MQTT, Ethernet/IP, Binding, Data Cache.
- Example Use Case 2:
  - Only one IP Address is configured.
  - Port 1 is plugged into your factory network.
  - Port 2 is cabled directly to your 2500-Cxxx Host PLC.
  - IP Address 1 is used by all protocols: Workbench, CAMP, OPC-UA, Modbus, MQTT, Ethernet/IP, Binding, Data Cache.
  - Packets are forwarded between Ports 1 and 2, allowing Data Cache communication and connection of 505 Workshop to your 2500-Cxxx Host PLC on Port 2.
- Example Use Case 3:
  - Two IP Addresses are configured.
  - Port 1 is plugged into your factory network.
  - Port 2 is not used.

- IP Address 1 is used for Workbench, CAMP, Modbus, MQTT, Binding, Data Cache and these communications occur on Port 1
- IP Address 2 is used for Ethernet/IP and/or OPC-UA, and these communications occur on Port 1.
- Example Use Case 4:
  - Two IP Addresses are configured.
  - Port 1 is plugged into your factory network.
  - Port 2 is cabled directly to your 2500-Cxxx Host PLC.
  - IP Address 1 is used for Workbench, CAMP, Modbus, MQTT, Binding.
  - IP Address 2 is used for Ethernet/IP and/or OPC-UA, and these communications occur on Port 1.
  - Packets are forwarded between Ports 1 and 2, allowing Data Cache communication and connection of 505 Workshop to your 2500-Cxxx Host PLC on Port 2.
  - Data Cache communications can use IP Address 1 or IP Address 2.
- **IMPORTANT:** When the switch mode is NONE, to prevent creating a network “storm”, you **must not** plug cables into both ports unless
  - The cables go to 2 physically separate networks OR
  - You are “daisy chaining” to another device which is not connected to a network (as in Use Case 2 or 4 above).

### 8.3.3 Ethernet Switch Configuration ALL

The diagram below shows the port operation when Ethernet Switch Configuration is ALL.



- Provides full isolation between Ports 1 and 2
- Ports 1 and 2 each get a MAC address
- IP Address 1 is available only on Port 1 and must be on a different subnet than IP Address 2
- IP Address 2 is available only on Port 2 and must be on a different subnet than IP Address 1
- No packets are forwarded between Ports 1 and 2
- Example Use Case 1:
  - Two IP Addresses are configured.
  - Port 1 is plugged into your factory network. IP Address 1 is used for Workbench, CAMP, Modbus, MQTT, Binding.
  - Port 2 is plugged into your factory network OR a physically separate network. IP Address 2 is used for Ethernet/IP and/or OPC-UA.
  - Data Cache communications, if used, can be configured to occur on Port Group 1 (Port 1) or Port Group 2 (Port 2). If configured for Port Group 2, your 2500-Cxxx PLC must have an IP Address on the same network as IP Address 2.
- In this configuration, you must plug cables into both Ports 1 and 2. These cables can go to separate networks or to the same physical network.

## 8.4 Existing Use Cases in 2500P-JACP Networking

This section summarizes existing use cases for networking on 2500P-JACP (prior to V2.00 firmware) and shows how to support these use cases with V2.00 networking.

1. Single cable in Port 1. Switch set in “All Ports Isolated [Default]”. One IP address assigned. **See diagram in Section 8.5.2.** For example:
  - a. Primary subnet 192.168.1.10/24 used for Workbench, CAMP, OPC-UA, Modbus, MQTT, Ethernet/IP, Data Cache and Binding.

*After firmware update, this use case is handled with the default Switch Mode NONE (and will also work with Switch Mode ALL). IP Address 1 is defined the same as the “Primary Subnet” from before. Ethernet/IP and Data Cache, if used, must be set to “Port Group 1”. The Ethernet/IP and OPC IP addresses must be set in Workbench to IP Address 1.*

2. Single cable in Port 1. Switch set in “All Ports Isolated [Default]”. Two IP addresses assigned (required to be different subnets), but running on the same network infrastructure, so running out of Port 1. **See diagram in Section 8.5.2.** For example:
  - a. Primary subnet 192.168.1.10/24 used for Workbench, CAMP, Modbus, MQTT, Data Cache and Binding.
  - b. Alternate Subnet 1 – 192.168.2.10/24 used for Ethernet/IP and/or OPC-UA. In this case, the user wants the Ethernet/IP and OPC-UA on a different logical network from other traffic, but still running on the same physical network.

*After firmware update, this use case is handled with the default Switch Mode NONE. IP Address 1 is defined the same as the “Primary Subnet” from before. IP Address 2 is defined the same as “Alternate Subnet 1” from before. EIP and DataCache must be set to “Port Group 1”. The Ethernet/IP and OPC-UA addresses must be set in Workbench to the desired values – IP Address 1 or IP Address 2.*

3. Network 1 cable in port 1. Network 2 cable in port 2. Networks are “galvanically isolated”, ie separate infrastructure. Switch set in “All Ports Isolated [Default]”. Two IP addresses assigned (required to be different subnets). **See diagram in Section 8.5.4.** For example:
  - a. Primary subnet 192.168.1.10/24 used for Workbench, CAMP, Modbus, MQTT, Data Cache and Binding.
  - b. Alternate Subnet 1 – 192.168.2.10/24 used for Ethernet/IP and/or OPC-UA.

*After firmware update, this use case is handled with Switch Mode ALL. IP Address 1 is defined the same as the “Primary Subnet” from before. IP Address 2 is defined the same as “Alternate Subnet 1” from before.*

Ethernet/IP must be set to Port Group 2. Data Cache must be set to the desired Port Group 1 or 2 based on the IP address of the Data Cache target. The Ethernet/IP and OPC-UA IP addresses must be set in Workbench to the desired values – IP Address 1 or IP Address 2.

4. Same as in #3 above, except switch set to “Forwarding between 1 & 2”. Another cable in port 2 is connected to a downstream CTI 2500-Cxxx PLC. **See diagram in Section 8.5.3.**

*After firmware update, this use case is handled with the default Switch Mode NONE. IP Address 1 defined the same as the “Primary Subnet” from before. IP Address 2, if it exists, is defined the same as “Alternate Subnet 1” from before. Ethernet/IP and Data Cache must be set to “Port Group 1”. The Ethernet/IP and OPC-UA IP addresses must be set in Workbench to the desired values – IP Address 1 or IP Address 2. **The downstream cable to the 2500-Cxxx must be inserted directly into Port 2. NOTE: this Port 2 cannot go to a switch on the same physical network as Port 1.***

## 8.5 Networking V2.00 Setup Guide

Networking configuration is done using the Network Settings web page in the module and by using Workbench Fieldbus Configuration for some protocols like Ethernet/IP, as outlined in the 4 steps below. Some of these steps are done automatically during the firmware upgrade process.

1. Configuring “Our IP Address” in Workbench if certain Ethernet/IP protocols are used
2. Configuring IP Address(es) – done automatically by the firmware upgrade process
3. Configuring the Internal Switch Mode – NONE or ALL – automatically set to NONE by the firmware upgrade process
4. Configuring Port Groups for Ethernet/IP and Data Cache – **must be done manually.**

**IMPORTANT NOTE:** After you upgrade from a previous firmware version to V2.00, the following settings are made automatically:

- Your previous “Primary Subnet” address becomes IP Address 1
- Your previous “Alternate Subnet 1” address (if used) becomes IP Address 2
- Ethernet Switch Configuration is set to NONE
- Ethernet/IP and Data Cache Port Groups are set to “Disabled”

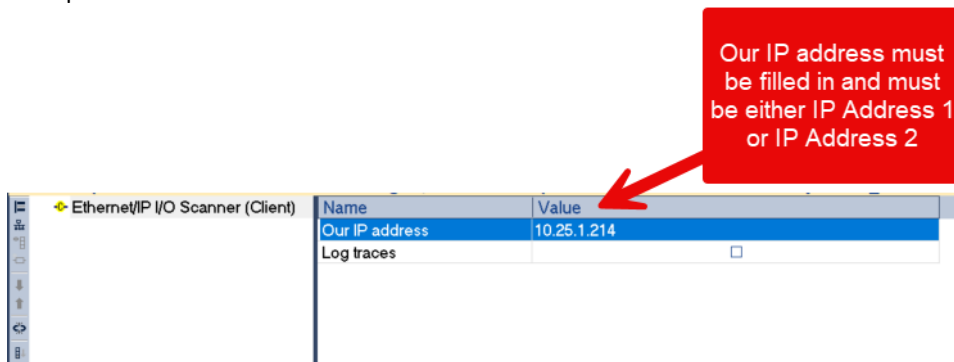
Networking setup after upgrade to V2.00 firmware depends on:

- a. How many network cables are used in the existing installation: 1 cable or 2 cables?
- b. Does Cable 2 (if used) connect to a downstream 2500-Cxxx (or Ethernet/IP device) or to a physically separate network?
- c. How was the Ethernet Switch set previously: “All Ports Isolated” or “Forwarding between 1 & 2”?

Detailed setup instructions for each of these cases are included in the sections below.

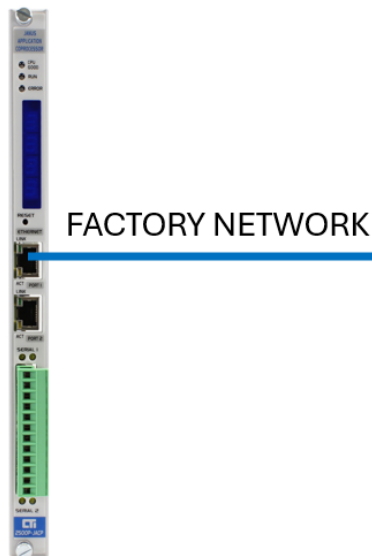
### 8.5.1 All Installations

For all JACP installations which use the protocols Ethernet/IP Adapter, Ethernet/IP FlexIO, Ethernet/IP I/O Scanner, or Ethernet/IP Tag Client, you **MUST** ensure that the “Our IP Address” set in the Workbench Fieldbus Configuration contains a valid IP address which must be either IP Address 1 or IP Address 2 (if configured). Example:



Previous versions of JACP firmware would default to the Primary Subnet address if this field was left blank, but now this field **MUST** have a valid IP address - IP Address 1 or IP Address 2, depending on which address you plan to use for Ethernet/IP communications. This is necessary so the firmware can configure these protocols to use the desired port.

## 8.5.2 Installation with 1 cable connected to JACP



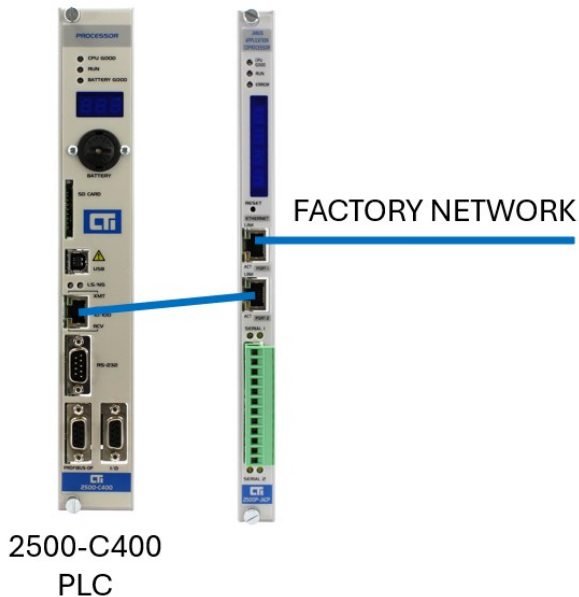
### Ethernet Switch was previously set to “All Ports Isolated”

- Ensure the network cable is plugged into Port 1
- On the Network Settings web page, set the **Internal Ethernet Switch Configuration** to **NONE**. This should have been automatically done by the firmware upgrade process.
- In the Network Settings web page, set “IP Address 1 Configuration” to the “Primary Subnet” address. Set “IP Address 2 Configuration” to the “Alternate Subnet 1” address. This should have been automatically done by the firmware upgrade process.
- In the Network Settings web page, set **Fieldbus Port Group Assignments** for Ethernet/IP and Data Cache (if these protocols are used) to Port Group 1. This step must be done manually, as it is not performed automatically by the firmware upgrade process.

### Ethernet Switch was previously set to Forwarding between 1 & 2

This would not be a valid configuration since the installation has only 1 cable.

### 8.5.3 Installation with 2 cables connected to JACP, where Port 2 connects to a single downstream device (2500-Cxxx PLC or Ethernet/IP device)



#### **Ethernet Switch was previously set to “All Ports Isolated”**

This configuration would not be very useful since the JACP port isolation would prevent connecting to this PLC or Ethernet/IP device from the Factory Network with Workshop, SCADA, or Ethernet/IP device management software. However, the JACP could still communicate over Port 2 with the 2500-Cxxx PLC using Data Cache or with the Ethernet/IP device.

- Set Internal Ethernet Switch Configuration to ALL.** NOTE: the firmware upgrade process sets this to NONE, so this setting will need to be manually changed in the Network Settings webpage.
- On the Network Settings web page, set “IP Address 1 Configuration” to the “Primary Subnet” address. Set “IP Address 2 Configuration” to the “Alternate Subnet 1” address. This should have been automatically done by the firmware upgrade process.
- In the Network Settings web page, set **Fieldbus Port Group Assignment** for Ethernet/IP (if used) to Port Group 2 OR, if Port 2 connects to a 2500-Cxxx PLC, set the **Fieldbus Port Group Assignment** for Data Cache to Port Group 2. This step must be done manually, as it is not performed automatically by the firmware upgrade process.

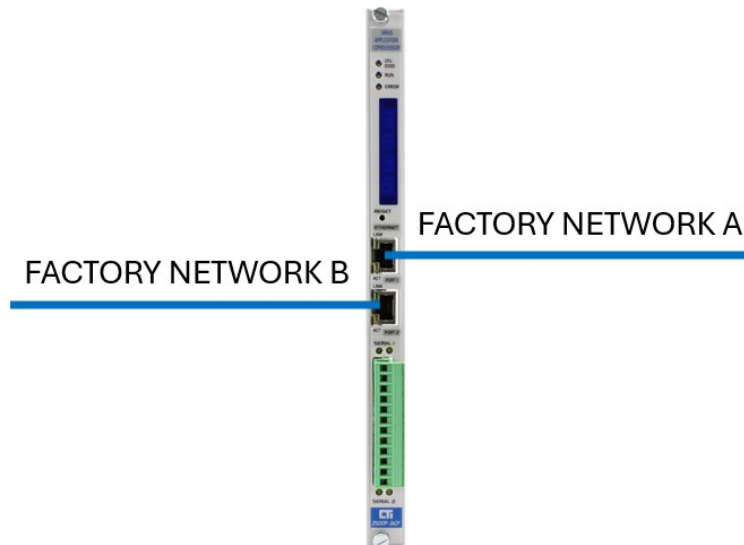
#### **Ethernet Switch was previously set to “Forwarding between 1 & 2”**

This configuration would be useful since the JACP port forwarding allows connecting to a PLC (as shown in the diagram above) or Ethernet/IP device from the Factory Network with Workshop, SCADA, or Ethernet/IP device management software.

- Set **Internal Ethernet Switch Configuration** to **NONE**. This should have been automatically done by the firmware upgrade process.

- b. On the Network Settings web page, set “IP Address 1 Configuration” to the “Primary Subnet” address. Set “IP Address 2 Configuration” to the “Alternate Subnet 1” address. This should have been automatically done by the firmware upgrade process.
- c. In the Network Settings web page, set **Fieldbus Port Group Assignment** for Ethernet/IP and/or Data Cache (if used) to Port Group 1. This step must be done manually, as it is not performed automatically by the firmware upgrade process.

#### 8.5.4 Installation with 2 cables connected to JACP, where Port 2 connects to physically separate network with Ethernet/IP devices and/or SCADA communicating with OPC-UA



##### **Ethernet Switch was previously set to “All Ports Isolated”**

This would be the typical configuration where the 2 networks need to remain isolated from each other.

- Set **Internal Ethernet Switch Configuration** to **ALL**. This should have been automatically done by the firmware upgrade process.
- In the Network Settings web page, set “IP Address 1 Configuration” to the “Primary Subnet” address. Set “IP Address 2 Configuration” to the “Alternate Subnet 1” address. This should have been automatically done by the firmware upgrade process.
- In the Network Settings web page, set **Fieldbus Port Group Assignment** for Ethernet/IP to Port Group 1 or Port Group 2, depending on which network the Ethernet/IP devices reside on. This step must be done manually, as it is not performed automatically by the firmware upgrade process.
- In the Network Settings web page, set **Fieldbus Port Group Assignment** for Data Cache to Port Group 1 or Port Group 2, depending on which network the Data Cache host resides on. This step must be done manually, as it is not performed automatically by the firmware upgrade process

##### **Ethernet Switch was previously set to Forwarding between 1 & 2**

This configuration would be very unusual since the JACP forwards packets between the 2 networks – thereby defeating the purpose of using 2 physically separate networks. This is not a recommended configuration.

- Set **Internal Ethernet Switch Configuration** to **NONE**. This should have been automatically done by the firmware upgrade process.

- b. In the Network Settings web page, set “IP Address 1 Configuration” to the “Primary Subnet” address. Set “IP Address 2 Configuration” to the “Alternate Subnet 1” address. This should have been automatically done by the firmware upgrade process.
- c. In the Network Settings web page, set **Fieldbus Port Group Assignment** for Ethernet/IP and/or Data Cache (if used) to Port Group 2. This step must be done manually, as it is not performed automatically by the firmware upgrade process.

## 8.6 New IP Address Display

NOTE: See [CIDR Notation](#) for description of CIDR notation.

- When Switch Mode = NONE (no ports isolated)
  - IP - xxx.xxx.xxx.xxx – CIDR (for IP Address 1)
  - IP - xxx.xxx.xxx.xxx – CIDR (for IP Address 2)
  - NOTE: the user can set whether a particular address is displayed on the [Network Settings](#) web page.
- When Switch Mode = ALL (all ports isolated)
  - P1 - xxx.xxx.xxx.xxx - CIDR
  - P2 - xxx.xxx.xxx.xxx – CIDR
  - NOTE: the user can set whether a particular address is displayed on the [Network Settings](#) web page.

NOTES:

- The user can tell the switch mode, All or None, by looking at how the IP addresses are displayed on the front panel. If switch mode = NONE, the IP address is preceded by “IP”. If switch mode = ALL, the IP address is preceded by “P1” or “P2”.
- When NO IP Addresses are selected for display, the module will display “NoIPDISP”



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

### **CPU Startup Errors**

| <b>Error Code</b> | <b>Description</b>                                                                           | <b>Operation</b> | <b>Error Recovery</b>                                                                                                                                                                          |
|-------------------|----------------------------------------------------------------------------------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 010               | No Network Configuration                                                                     | Module stopped.  | Configure JACP via Web Server or use User SD Card Ethernet Port Setup to specify Module IP Address.<br><b>NOTE: User SD Card Ethernet Port setup is removed beginning with Firmware V2.00.</b> |
| 011               | Two IP Addresses are on overlapping subnets                                                  | Module stopped.  | Check DHCP address and all configured IP addresses for overlaps and correct                                                                                                                    |
| 020               | Ethernet Port Switch Configuration error (not set for 'Full Duplex' or '10/100mb' operation) | Module stopped.  | Cycle power to Module. Contact CTI.                                                                                                                                                            |
| 023               | Ethernet/IP configured but Port Group is Disabled                                            | Module stopped.  | Ethernet/IP configured but Port Group is Disabled                                                                                                                                              |
| 024               | Ethernet/IP "Our IP Address" not found in Ethernet/IP Port Group Addresses                   | Module stopped.  | Correct error by changing the Port Group and/or IP Address setup in the web page or Workbench                                                                                                  |
| 025               | OPC IP Address in User Application does match an IP Address configured                       | Module stopped.  | Correct error from by by changing IP Address setup in the web page or Workbench                                                                                                                |
| 026               | Data Cache configured but Port Group is Disabled                                             | Module stopped.  | Data Cache configured but Port Group is Disabled                                                                                                                                               |
| 027               | Data Cache Host PLC IP Address not in Data Cache Port Group subnet                           | Module stopped.  | Data Cache Host PLC IP Address not in Data Cache Port Group subnet                                                                                                                             |
| 030               | Manufacturing Data Checksum Error                                                            | Module stopped.  | Cycle power to Module. Contact CTI.                                                                                                                                                            |

| Error Code | Description                                                                                                           | Operation                  | Error Recovery                                                                                                                                                                                                                         |
|------------|-----------------------------------------------------------------------------------------------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 031        | MRAM failure on startup.<br>NOTE: This is shown in front panel only; it does not appear on the Error Status web page. | Module stopped.            | Cycle power to Module. If error persists, Contact CTI.                                                                                                                                                                                 |
| 032        | Serial Port Initialization Failure                                                                                    | Module stopped.            | Cycle power to Module. If error persists, Contact CTI.                                                                                                                                                                                 |
| 050        | Duplicate IP Address detected on network<br>NOTE: This condition is checked every minute while module is active.      | Module state is unchanged. | Check Event Log for details. Resolve IP address on conflicting devices. Error is cleared after 2 consecutive probes report no duplicate IP Address (3 minutes max).<br>Note: duplicate IP addresses can cause random control problems. |
| 070        | Configuration Settings Missing or Invalid                                                                             | Module stopped.            | Configure JACP via Web Server. Download program from Janus Workbench.                                                                                                                                                                  |

## Module Run Mode Startup Errors

| Error Code | Description                                                                                                                          | Operation       | Error Recovery                                                                                                                                                           |
|------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 080        | No Application Program Found                                                                                                         | Module stopped. | Download program from Janus Workbench.                                                                                                                                   |
| 085        | Specified Startup Mode Unavailable<br>(Application cannot start as configured due to abnormal shutdown, unsupported program version. | Module stopped. | JACP could not complete an orderly shutdown due to loss of power. Connect Workbench to start application or press <i>Clear Exception</i> button to trigger "Cold Start". |

| Error Code | Description                                   | Operation       | Error Recovery                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------|-----------------------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 090        | Incompatible Application Program              | Module Stopped  | Recompile Program with correct module model/firmware version or update firmware. This error can also occur if the user program has a function block in a POU or a field I/O configuration that is not applicable for the target product. The "Execution" window in Workbench will detail this type of runtime error. This error may also occur if the product does not have the manufacturing "Profinet Activated" bit set and the program that was downloaded includes Profinet field I/O. The product must be returned to CTI for this feature upgrade or make use of a product that shipped with the Profinet feature. Profinet activation status can be viewed on the module "Product Information" web page. |
| 150        | CTI Data Cache Client driver failed to start  | Module stopped. | Reset Module.<br>Contact CTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 160        | CAMP Client driver failed to start            | Module stopped. | Reset Module.<br>Contact CTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 165        | CAMP Server driver failed to start            | Module stopped. | Reset Module<br>Contact CTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 170        | MODBUS Client driver failed to start          | Module stopped. | Reset Module.<br>Contact CTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 175        | MODBUS Server driver failed to start          | Module stopped. | Reset Module.<br>Contact CTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 180        | Ethernet/IP Scanner driver failed to start    | Module stopped. | Reset Module.<br>Contact CTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 185        | Ethernet/IP Adapter driver failed to start    | Module stopped. | Reset Module.<br>Contact CTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 187        | Ethernet/IP FlexIO driver failed to start     | Module Stopped  | Reset Module.<br>Contact CTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 190        | Ethernet/IP Tag Client driver failed to start | Module stopped. | Reset Module.<br>Contact CTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 195        | Ethernet/IP Tag Server failed to start        | Module stopped. | Reset Module.<br>Contact CTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 210        | MQTT Client driver failed to start            | Module stopped. | Reset Module.<br>Contact CTI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Error Code | Description                              | Operation       | Error Recovery                |
|------------|------------------------------------------|-----------------|-------------------------------|
| 215        | OPCUA Server failed to start             | Module Stopped  | Reset Module.<br>Contact CTI  |
| 220        | HTML5 Data Server driver failed to start | Module stopped. | Reset Module.<br>Contact CTI. |
| 225        | Block Transfer Start Error               | Module stopped. | Reset Module.<br>Contact CTI. |

## Firmware/Configuration Update Errors

| Error Code | Description                 | Operation                                                                                                                                                                                                                                                                          | Error Recovery                                                                                                                                                                                                                                                                                                                                            |
|------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 250        | File Not Found              | Occurs when file download fails during 'Remote Firmware Update' or expected file is not found on user SD card during 'User SD Card Firmware Update' or 'User SD Card Ethernet Port Setup'. <b>NOTE: User SD Card Ethernet Port setup is removed beginning with Firmware V2.00.</b> | Ensure that module switches 1,2 and 4 are in the proper position for desired firmware update process. Retry download, or copy appropriate file to root directory of User SD card and re-insert card into User SD Card receptacle.                                                                                                                         |
| 260        | User SD Card – Invalid File | Occurs when no valid firmware update file is found during 'User SD Card Firmware Update' or 'User SD Card Ethernet Port Setup' operations) <b>NOTE: User SD Card Ethernet Port setup is removed beginning with Firmware V2.00.</b>                                                 | 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 'User SD Card Firmware Update'. If condition persists, contact CTI. |

## Execution Errors

| Error Code | Description                                                                                       | Operation                                              | Error Recovery                                                                                            |
|------------|---------------------------------------------------------------------------------------------------|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| 310        | System Exception Error (Detected after JACP reset following Segmentation Fault or Firmware Error) | System restarts. Module remains stopped after restart. | Connect Workbench and transfer to RUN or use CLEAR EXCEPTION button to restart JACP. Contact CTI Support. |

| Error Code | Description                                                                                        | Operation                                                                      | Error Recovery                                                                                                                                                                             |
|------------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 320        | System Watchdog Timeout (Detected after JACP reset following Segmentation Fault or Firmware Error) | System restarts. Module remains stopped after restart.                         | Connect Workbench and transfer to RUN or use Reset button to restart JACP.<br>Contact CTI Support.                                                                                         |
| 330        | Program Logic Error                                                                                | Module 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 JACP. |

## SD Card Errors

| Error Code | Description                                                                                                                                            | Operation                                                                                                    | Error Recovery                                                                                                                                                    |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 350        | System SD Card Disk Full (no further writes to System SD card)                                                                                         | Module 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        | System SD Card Free Space Limit (disk > 90% full)                                                                                                      | Module 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        | System SD Card Free Space Warning (disk > 80% full)                                                                                                    | Module continues to run normally.                                                                            | Use Web Server 'SD Card File Management' page to transfer or delete user files                                                                                    |
| 370        | User SD Card Not Accessible (Missing, Incompatible, Unformatted or Write-Protected). NOTE: Error 250 will also be returned if switch 2 or 4 is closed. | Module continues to run normally                                                                             | Cancel function that is using User SD Card, or correct problem with SD card. If Error 250 is returned and switch 2 or 4 is inadvertently closed, open the switch. |

## Client Communication Errors

| Error Code | Description                                        | Operation                        | Error Recovery                                                                                  |
|------------|----------------------------------------------------|----------------------------------|-------------------------------------------------------------------------------------------------|
| 470        | CTI Data Cache Client: Host TCP Connection Failure | Module continues to run normally | Correct connection and/or Host settings                                                         |
| 475        | CTI Data Cache Client has non-CTI MAC Address      | Module continues to run normally | Remove DC Client from application or force creation of new 'cti.ini' file to update MAC Address |

| Error Code | Description                                                                                                                       | Operation                                                               | Error Recovery                                                                                                                                                                          |
|------------|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 480        | CTI Data Cache Client Incompatible Host PLC Firmware                                                                              | Module continues to run normally                                        | Update Host PLC firmware                                                                                                                                                                |
| 485        | CTI Data Cache Client: Host PLC Registration Failed (PLC already has max number of connections)                                   | Module continues to run normally                                        | If replacing an existing Data Cache module, remove old module before connecting new one.                                                                                                |
| 490        | CTI Data Cache Client: Host PLC Link Inactive                                                                                     | Module continues to run normally                                        | Correct connection to Host PLC. Ensure Host PLC is online.                                                                                                                              |
| 510        | CTI Data Cache Client: Host PLC Fatal Error                                                                                       | Module continues to run normally                                        | Clear Host PLC Fatal Error                                                                                                                                                              |
| 515        | CTI Data Cache Client: Host PLC in Program Mode                                                                                   | Module continues to run normally                                        | Change Host PLC mode to RUN                                                                                                                                                             |
| 520        | CTI Data Cache Client: Inaccessible PLC Address                                                                                   | Module 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). | Module continues to run normally. Error clears next scan cycle.         | Increase Host PLC time slice for CTI Data Cache interface. Set "fixed" IEC PLC cycle time.                                                                                              |
| 530        | Block Transfer: Host PLC does not support SFIO                                                                                    | Module continues to run normally                                        | Choose a CTI 2500 Series® / Simatic®/TI 505 PLC with Special Function (SFIO) support or choose a different data transfer protocol. Note: The Janus PAC does not currently support SFIO. |
| 531        | Block Transfer: Unable to Issue Request to SFIO                                                                                   | Module continues to run normally                                        | Ensure that the Block Transfer configuration matches the PLC memory configuration                                                                                                       |
| 532        | Block Transfer: Timeout Error                                                                                                     | Module continues to run normally                                        |                                                                                                                                                                                         |
| 534        | Block Transfer: Host PLC Fatal Error                                                                                              | Module continues to run normally                                        | Clear Host PLC Fatal Error                                                                                                                                                              |
| 536        | Block Transfer: Host PLC in Program Mode                                                                                          | Module continues to run normally                                        | Change Host PLC mode to RUN                                                                                                                                                             |
| 538        | Block Transfer: Inaccessible Host PLC Memory Address                                                                              | Module continues to run normally                                        | Ensure that the Block Transfer configuration matches the PLC memory configuration                                                                                                       |
| 539        | Block Transfer: SFIO Message queue full                                                                                           | Module continues to run normally. Error clears on next controller cycle | Since the error clears once the queue has space, there is no need for user intervention to recover from the error.                                                                      |

| Error Code | Description                                                                         | Operation                        | Error Recovery                                                                       |
|------------|-------------------------------------------------------------------------------------|----------------------------------|--------------------------------------------------------------------------------------|
| 540        | CAMP Client Error<br>(Connection to servers or communication failed)                | Module continues to run normally | Check configuration and connection to CAMP Server(s).                                |
| 550        | MODBUS Client Error<br>(Connection to servers or communication failed)              | Module continues to run normally | Check configuration and connection to Modbus Server(s).                              |
| 560        | Data Exchange Error<br>(Subscriber not receiving data from one or more Publishers). | Module continues to run normally | Check Global Binding configuration and connection to Data Exchange Publisher device. |
| 570        | Ethernet/IP Scanner Error<br>(Connection to servers or communication failed)        | Module continues to run normally | Check configuration and connection to EIP Adapter(s).                                |
| 575        | Ethernet/IP FlexIO Error<br>(Connection to Adapters or I/O communications failed)   | Module continues to run normally |                                                                                      |
| 580        | Ethernet/IP Tag Client Error<br>(Error is default at startup when configured)       | Module continues to run normally | Check configuration and connection to EIP Server.                                    |
| 590        | MQTT Client Error<br>(Connection to broker or communication failed)                 | Module continues to run normally | Check configuration and connection to MQTT broker.                                   |

\* Not displayed on Alphanumeric Display

## Hardware Errors

| Error Code | Description                                                         | Operation                        | Error Recovery                                                                                                                                                      |
|------------|---------------------------------------------------------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 620        | Real-Time Clock Access Error (firmware unable to read or write RTC) | Module 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                                  | Module continues to run normally | This indicates a serious issue with JACP internal temperature. User should lower ambient temperature and/or shutdown JACP 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 (11111111111101110000000000000000) 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     |                       |                       |                       |
|-------------------------|----------------|-----------------------|-----------------------|-----------------------|-----------------------|
|                         |                | 1 <sup>st</sup> Octet | 2 <sup>nd</sup> Octet | 3 <sup>rd</sup> Octet | 4 <sup>th</sup> Octet |
| IP Address              | 127.18.40.3    | 01111111              | 00010010              | 00101000              | 00000011              |
| Subnet Mask             | 255.255.240.0  | 11111111              | 11111111              | 11110000              | 00000000              |
| Derived Network Address | 127.18.32.0    | 01111111              | 00010010              | 00100000              | 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 JACP module 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 JACP module 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/](http://www.iana.org/assignments/multicast-addresses/)



---

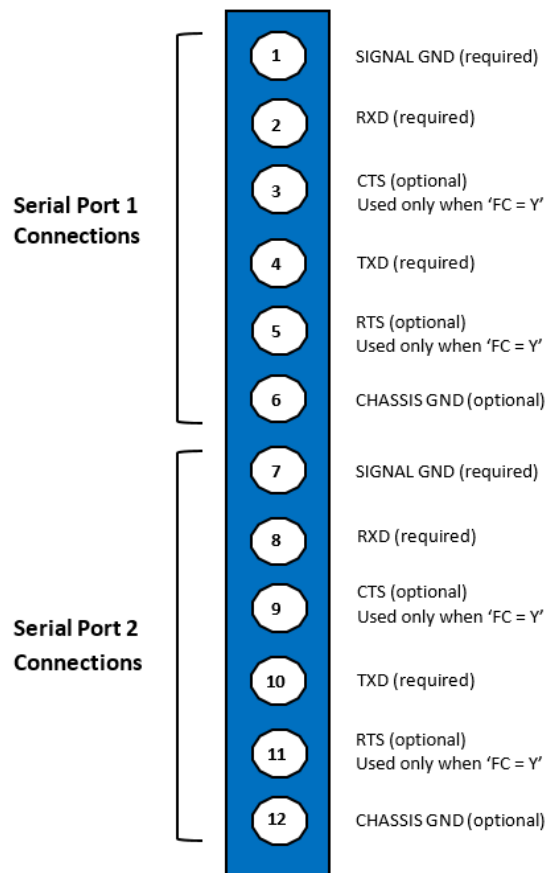
## ***APPENDIX C: Serial Port Wiring***

---

### **RS232 Wiring**

RS232 is the original single-ended serial interface (usually implemented as RS423 using 5V signals in modern devices) used for short-length connections in low-noise environments.

The following diagram shows the pin-out for wiring connections when RS232 is specified as the 'Interface' in the serial port parameter setup:



#### **NOTES:**

SIGNAL GND (Pin 1 or Pin 7) connects to Male DB9 connector SIGNAL GND (usually Pin 5).

RXD (Pin 2 or Pin 8) connects to Male DB9 connector (usually Pin 2).

TXD (Pin 4 or Pin 10) connects to Male DB9 connector (usually Pin 3).

When Hardware Flow Control is specified:

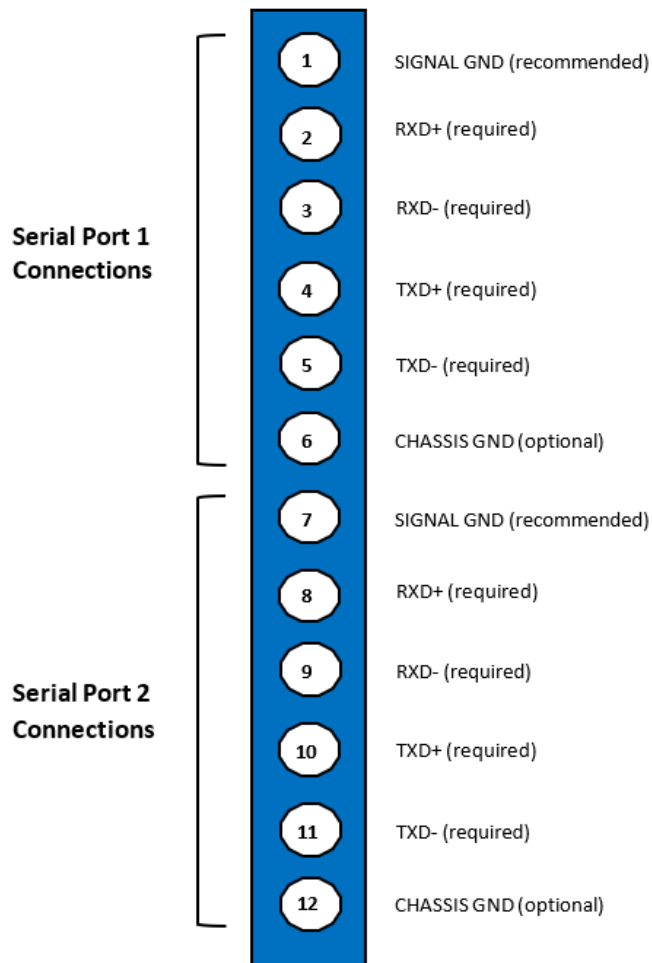
CTS (Pin 3 or Pin 9) connects to Male DB9 connector RTS (usually Pin 7).

RTS (Pin 5 or Pin 11) connects to Male DB9 connector CTS (usually Pin 8).

## RS422 Wiring

RS422 is a 4-wire differential-signal serial interface that can be used in a multi-drop network. RS422 works over longer distances and has superior noise-immunity compared to RS232.

The following diagram shows the pin-out for wiring connections when RS422 is specified as the 'Interface' in the serial port parameter setup:



### NOTES:

SIGNAL GND (Pin 1 or Pin 7) connects to Male DB9 connector (usually Pin 5).

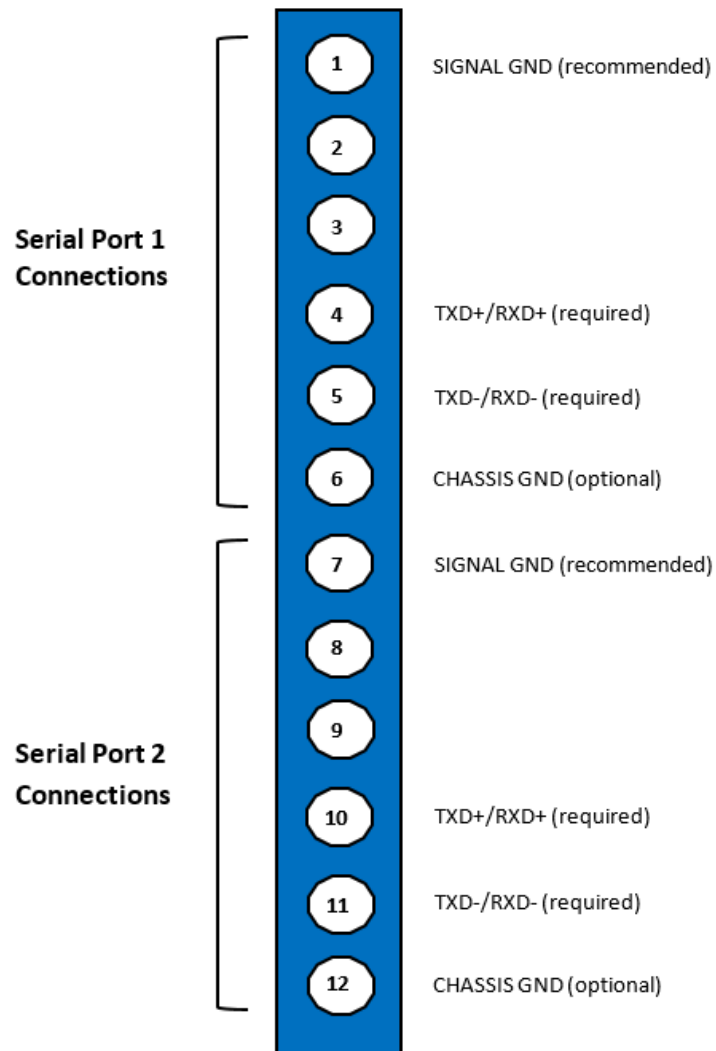
TXD+/RXD+ (Pin 4 or Pin 10) connects to Male DB9 connector TXD+ (usually Pin 1).

TXD-/RXD- (Pin 5 or Pin 11) connects to Male DB9 connector TXD- (usually Pin 2).

## RS485 Wiring

RS485 is a 2-wire differential-signal serial interface that can be used in a multi-drop network. RS485 has the same properties as RS422 with the advantage of requiring less expensive signal wiring.

The following diagram shows the pin-out for wiring connections when RS485 is specified as the 'Interface' in the serial port parameter setup:



### NOTES:

SIGNAL GND (Pin 1 or Pin 7) connects to Male DB9 connector (usually Pin 5).

TXD+/RXD+ (Pin 4 or Pin 10) connects to Male DB9 connector TXD+ (usually Pin 1).

TXD-/RXD- (Pin 5 or Pin 11) connects to Male DB9 connector TXD- (usually Pin 2).

---

## ***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<br>Sinusoidal<br><br>Random                                                           | IEC 68-2-6 Test Fc<br>0.15 peak to peak, 10 – 57 Hz<br>1.0g. 57 – 150 Hz<br><br>IEC 68-2-34 or NAVMAT p-9492<br>Test Fdc with 0.04 g <sup>2</sup> /Hz, 80 – 350 Hz and<br>3db/Octave roll off, 80 -20 Hz and<br>350 – 2000Hz at 10 min/Axis                   |
| Impact Shock                                                                                    | IEC 68-2-27, Test Ea. Half Sine 15g, 11ms                                                                                                                                                                                                                     |
| Isolation, Inputs to Module                                                                     | 1500 VRMS except where specified                                                                                                                                                                                                                              |
| Corrosion Protection                                                                            | All parts of corrosion resistant material or plated/painted as corrosion protection                                                                                                                                                                           |
| Electric Noise Immunity<br>Conducted Noise<br><br>Radiated Noise<br><br>Electrostatic Discharge | IEC 801 Part 4 Level 3<br>MIL-STD-461B, Part 4:CS01, CS02, CS06<br>IEC 255-4, Appendix C<br>IEC 4517/79 Com(78) 766 Final, Part 4<br>IEC 472, 2.5 KV<br><br>IEC 801 Part 3, Level 3<br>MIL-STD-461B, Part 4 RS01, RS02<br><br>IEC 801. Part 2, Level 4 (15kV) |

### **Agency Approvals (pending)**

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-JACP Janus Application Coprocessor                                                 |                       |
|------------------------------------------------------------------------------------------|-----------------------|
| <b>Built-in display for IP address and errors</b>                                        | yes                   |
| <b>Ethernet</b>                                                                          |                       |
| Number of IP/Subnet Configurations                                                       | 2                     |
| Number of connections                                                                    | 64                    |
| <b>User Memory</b>                                                                       |                       |
| Code (Programs + Fieldbus)                                                               | 3MB                   |
| Data                                                                                     | 4MB                   |
| <b>Web Server</b>                                                                        | yes                   |
| Web Visualization (variables)                                                            | unlimited             |
| <b>Enhanced On-line change</b>                                                           | yes                   |
| <b>Communication Protocols</b>                                                           |                       |
| Binding (peer-peer)                                                                      | yes                   |
| CAMP Server                                                                              | yes                   |
| Camp Client                                                                              | yes                   |
| Modbus UDP/TCP Client                                                                    | choose 2*             |
| Modbus UDP/TCP Server                                                                    | yes                   |
| Ethernet/IP Scanner & Flex I/O                                                           | choose 2*             |
| Ethernet/IP Adapter                                                                      | yes                   |
| Ethernet/IP Tag Server                                                                   | yes                   |
| Ethernet/IP Tag Client                                                                   | choose 2*             |
| Ethernet/IP Explicit Message Server                                                      | yes                   |
| MQTT Client (communicates with broker)                                                   | yes                   |
| OPC-UA Server                                                                            | yes (max 10 sessions) |
| Profinet Controller & Device                                                             | future                |
| <b>Host PLC Interfaces</b>                                                               |                       |
| CTI Enhanced Data Cache<br>( 1 Host PLC Connections / 6144 of variables)                 | choose 1*             |
| CTI Block Transfer (Backplane data transfer)<br>(1 Host PLC Connection / 4096 Variables) | choose 1*             |
| <b>Serial Communications</b>                                                             |                       |
| Electrical Interfaces (2 ports)                                                          | RS232 / RS422 / RS485 |
| Modbus-RTU Master/Slave                                                                  | yes                   |
| General ASCII                                                                            | yes                   |

## NOTES

Choose 1\*      Project may include one Host PLC interface: CTI Enhanced Data Cache or CTI Block Transfer

Choose 2\*\*     Project may include two of these protocols: Open Modbus Client, Ethernet/IP Scanner, Ethernet/IP Tag Client, Ethernet/IP Explicit Message Client

### ETHERNET CONNECTION LIMIT

The 2500P-JACP 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/](http://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.