Trusted Peer to Peer Communications Software Package

Product Overview

Trusted® Peer to Peer Communications is provided by the Trusted Communications Interface module (T8150/T8151/T8151B) for the interchange of safety and non-safety information between Trusted Controllers. Up to four Trusted Communications Interface modules may be fitted in each Trusted Controller.

Features:

- Supports up to forty Trusted Controllers per Peer to Peer Network
- Automatic redundancy routing.
- High density data transactions.
- Up to eight Peer to Peer Networks per Trusted Controller
- Safety related data interchange support (TÜV certified for SIL 3 applications)

There are two types of Peer to Peer network, Basic and Enhanced. The Enhanced is described in the main document below and Basic Peer to Peer is described in appendices of this document.

PREFACE

In no event will Rockwell Automation be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment. The examples given in this manual are included solely for illustrative purposes. Because of the many variables and requirements related to any particular installation, Rockwell Automation does not assume responsibility or reliability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, with respect to use of information, circuits, equipment, or software described in this manual.

All trademarks are acknowledged.

DISCLAIMER

It is not intended that the information in this publication covers every possible detail about the construction, operation, or maintenance of a control system installation. You should also refer to your own local (or supplied) system safety manual, installation and operator/maintenance manuals.

REVISION AND UPDATING POLICY

This document is based on information available at the time of its publication. The document contents are subject to change from time to time. The latest versions of the manuals are available at the Rockwell Automation Literature Library under "Product Information" information "Critical Process Control & Safety Systems".

TRUSTED RELEASE

This technical manual applies to **Trusted Release: 3.6.1**.

LATEST PRODUCT INFORMATION

For the latest information about this product review the Product Notifications and Technical Notes issued by technical support. Product Notifications and product support are available at the Rockwell Automation Support Centre at
http://rockwellautomation.custhelp.com

At the Search Knowledgebase tab select the option "By Product" then scroll down and select the Trusted product.

Some of the Answer ID’s in the Knowledge Base require a TechConnect Support Contract. For more information about TechConnect Support Contract Access Level and Features please click on the following link:

https://rockwellautomation.custhelp.com/app/answers/detail/a_id/50871

This will get you to the login page where you must enter your login details.

IMPORTANT	A login is required to access the link. If you do not have an account then you can create one using the "Sign Up" link at the top right of the web page.

DOCUMENTATION FEEDBACK

Your comments help us to write better user documentation. If you discover an error, or have a suggestion on how to make this publication better, send your comment to our technical support group at http://rockwellautomation.custhelp.com

SCOPE

This manual specifies the maintenance requirements and describes the procedures to assist troubleshooting and maintenance of a Trusted system.

WHO SHOULD USE THIS MANUAL

This manual is for plant maintenance personnel who are experienced in the operation and maintenance of electronic equipment and are trained to work with safety systems.

SYMBOLS

In this manual we will use these notices to tell you about safety considerations.

	SHOCK HAZARD: Identifies an electrical shock hazard. If a warning label is fitted, it can be on or inside the equipment.
	WARNING: Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which can cause injury or death, property damage or economic loss.
	ATTENTION: Identifies information about practices or circumstances that can cause injury or death.
	CAUTION: Identifies information about practices or circumstances that can cause property damage or economic loss.
	BURN HAZARD: Identifies where a surface can reach dangerous temperatures. If a warning label is fitted, it can be on or inside the equipment.
	This symbol identifies items which must be thought about and put in place when designing and assembling a Trusted controller for use in a Safety Instrumented Function (SIF). It appears extensively in the Trusted Safety Manual.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.
NOTE	Provides key information about the product or service.
TIP	Tips give helpful information about using or setting up the equipment.

WARNINGS AND CAUTIONS

WARNING: EXPLOSION RISK

Do not connect or disconnect equipment while the circuit is live or unless the area is known to be free of ignitable concentrations or equivalent

AVERTISSEMENT - RISQUE D'EXPLOSION

Ne pas connecter ou déconnecter l'équipement alors qu'il est sous tension, sauf si l'environnement est exempt de concentrations inflammables ou équivalente

MAINTENANCE

Maintenance must be carried out only by qualified personnel. Failure to follow these instructions may result in personal injury.

CAUTION: RADIO FREQUENCY INTERFERENCE

Most electronic equipment is influenced by Radio Frequency Interference. Caution should be exercised with regard to the use of portable communications equipment around such equipment. Signs should be posted in the vicinity of the equipment cautioning against the use of portable communications equipment.

CAUTION:

The module PCBs contains static sensitive components. Static handling precautions must be observed. DO NOT touch exposed connector pins or attempt to dismantle a module.

ISSUE RECORD

Issue					
Number	Date	Revised by	Technical Check	Authorised by	Modification
6	Oct 05	J W Clark			Format
7	Jan 06	N Owens			Release 3.5
8	Aug 06	N Owens	I Vince	P Stock	Corrections to examples
9	Nov 06	N Owens	I Vince	P Stock	Rewritten descriptions
10	Mar 08	N Owens	A Holgate	P Stock	Input Status advice
11	Jun 16	J McDonald	J Gonsalves	D Watley	Rebrand, merge Basic Peer to Peer Network into appendices of this document and correct typographical errors.

This page is intentionally blank

Table of Contents, Figures & List of Tables

Table of Contents

Figures

Tables

1. Enhanced Peer Network

The Peer Network provides communication of safety data between up to forty Trusted systems per peer network. The data can be transferred between individual systems or from one system to several systems at the same time using multicasting.

A peer network consists of one or more Ethernet networks connecting together a set of Trusted systems to enable safety data to be passed between them. A network can use up to eight physical Ethernet networks (referred to as subnets) to provide redundant data paths via up to eight separate physical routes.

Each Trusted system must be fitted with a T812x processor interface adapter for the system to participate in peer communication. Any T812x series adapter may be used, but adapters in use before TÜV release 3.5 require an update.

A single Trusted system can support up to four communications interfaces using peer communication and both Ethernet ports on the communications interface can be used for peer communication at the same time. This provides a maximum of eight physical peer ports per controller, each of which connects to a subnet. These can be divided between different peer networks or all assigned to one network as required.

Communications interaction via the peer network is on a master/slave basis with a single master per subnet. Each communications interface Ethernet port may be configured as master or slave. Each subnet is capable of supporting forty peers.

Simplex, dual or multiple redundant networks are supported. Eight peer networks are the maximum number that may be supported by a single Trusted system. Where a redundant network is employed, the most recent information received is used. Data integrity is checked via a CRC of the packet data sent between systems.

Network subnets may be assigned to modules and ports as desired. Normally, subnets of the same redundant network would use separate communication modules to achieve the highest level of hardware fault tolerance.

The information to be transferred between Trusted systems is defined within the application programs using input and output boards in the standard form. The boards configure data blocks of 16 or 128 Boolean points, 16 or 128 analogue points and relevant status information. Boolean and analogue boards are ‘complex equipment’ within the IEC 61131 toolset.

Each peer data block must have a unique identity on the peer network. The output board sets up a block of data which includes the network ID number (1 to 8), the ID number of the peer that is sending the data (1 to 40) and an index number that uniquely defines that block of data within the sending peer’s list of output data blocks (1 to 64). These identities are described later in this document. The data block is sent to the destination peer, chosen with another ID number. The receiving input board is given these identities to enable it to recognize the data.

This mechanism enables data to be passed between one output board and one input board and also allows an output to be multicast to several input boards on different controllers using multicasting. Multicasting is a part of TCP/IP communications. A separate IP address is chosen as a multicast destination address. This is configured as if it were another destination peer. Each receiving peer is configured to accept data from this multicast address, as well as its true IP address. At the receiving end, the data is presented as if it were on a private point to point link.

Each Peer to Peer point (both Boolean and analogue) is equivalent to an external I/O point. All Peer to Peer points and boards must therefore be included in the total number of external points and boards. The I/O point count and boards must remain within the constraints of the IEC 61131 toolset.

Note: The Trusted communications interface will also support external communications using Modbus over serial and Ethernet links. Using the module to support both external Modbus communications and peer networks may slow the performance of peer communications.

1.1. Theory of Operation

Peer communications interaction is Master/Slave which provides deterministic behaviour. Each peer communications subnet requires one Trusted system to act as the master for the subnet and up to thirty-nine Trusted systems participating as slaves. If redundant masters are required so that a subnet remains operational if the master peer goes offline, then another peer may be permanently set as master. The two masters will arbitrate their control.

Peer communications is configured by defining peer subnet control boards and I/O boards within the application program in the normal way. Each peer subnet control board defines the systems' view of one subnet of a network. Two control variables are provided on the peer subnet control board to define the board as a master or slave and to give the application program control over the starting and stopping of the peer to peer communications.

1.1.1. Communications Cycle

At start of the communications cycle, the peer master issues an enquiry command to the first slave. If the master receives a response from the slave, it registers that slave as being active and then repeats the process with the next slave. This sequence continues until all the slaves have been polled.

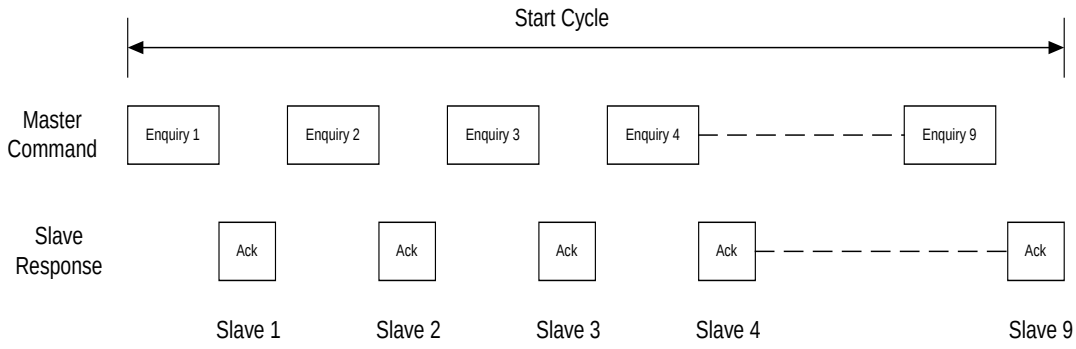

Figure 1 Peer Communications Start Cycle

The master then sends a transmit data command (token) to the first slave to instruct it to send its output data to its configured peers. When the slave has completed this, it returns the token to the master and the master repeats the process with the next slave. Once all the slaves have been polled, the master transmits its output data. The transmit data cycle starts again with the first slave. The master repeats this communications cycle continuously.

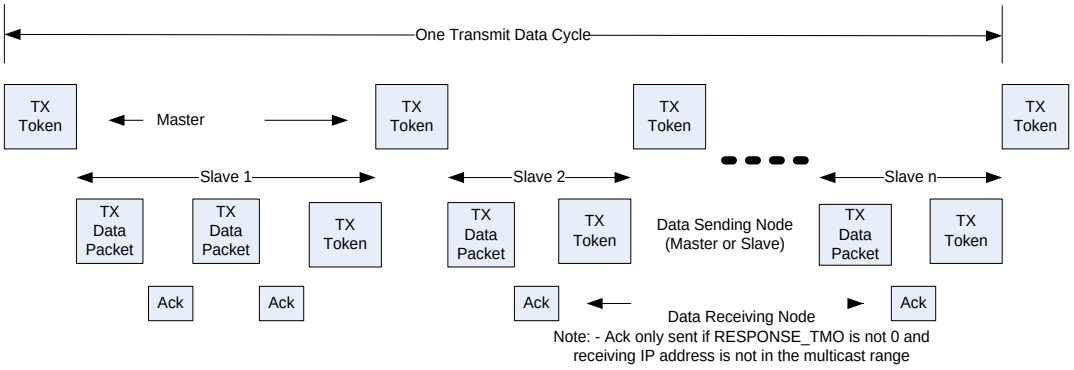

Figure 2 Peer Communications Transmit Data Cycle

1.1.1. Input Data

When the system receives peer input data, it is validated before it is passed on to the application program for use.

The system monitors the refreshing of input data. If fresh input data is received within the time-out period, the input refresh status bit on the input board is set to true. If fresh input data is not received, this status bit is set to false and the input data will either hold last state or go to the fail safe value depending on CONTROL rack variable state set by the application. The system always uses the latest data received (determined by a data sequence number) from all of the subnet links to update the application. The refresh timer is not updated if data older than the current data is received.

The length of time the system waits for fresh input data is configurable via the refresh time-out parameter on the input boards.

1.1.2. Output Data

When peer output data is changed by the application program, it is sent to the Trusted communications interface ready for transmission over the peer subnet. Only the latest output data for a particular peer system is stored on the communications interface. If fresh output data is received before the previous values have been transmitted, they will be overwritten by the new data.

If the application program has not changed output data within a time-out period, the current values are sent to the communications interface. This ensures the corresponding input board on the Peer system expecting the data is kept refreshed.

The length of time the system waits for fresh output data from the application program is configurable via the refresh time-out parameter on the Peer to Peer output boards.

2. Programming Information

The Trusted communications interface modules are selected and assigned to peer communications using the I/O Configuration Editor at the Engineering Workstation (EWS) as described in PD-T8082. It should be noted that the (OEM) parameters set up on all board / rack definitions cannot be changed online. General information relating to configuring the modules is detailed below.

2.1. Peer Subnet Control

This board definition configures and controls a peer controller for one subnet within a peer network. The definition also provides status for up to forty possible peer controllers (including itself).

A peer controller must be allocated to a communication interface. No more than one controller should be active at any one time for each physical Ethernet port of a communication interface.

Each peer controller may have up to forty peer controllers configured including itself. These may represent either actual or multicast IP addresses representing one peer or a group of peer controllers, respectively.

Peer controllers can only communicate with other peer controllers that share the same network and subnet identity. Each set of communicating controllers represents one subnet of a peer network which may consist of up to 8 subnets that provide redundant routing for I/O board data.

Each peer subnet control board defines the IP addresses of all the peer controllers on the subnet. Each peer controller has a peer ID, allocated according to the position of its IP address in the peer subnet control board parameters. The configuration of IP addresses must be the same across all peer subnet control boards sharing the same network because the configuration is used to set the Peer ID number.

A Multicast peer address must be in the range 239.255.0.0 to 239.255.255.255 for a local site. This range prevents the messages from being forwarded by a router outside the immediate network. Other addresses may be used, but these will be forwarded outside the immediate network. A limit may be set of the number of routers that will forward the data.

Note that Multicast operation must be configured in the System INI configurator. Refer to PD-T8151B for details.

Peer subnet control boards must be defined before their respective input/output boards in the I/O connection editor.

Figure 3 shows the display associated with the Peer Subnet Control board CONTROL rack.

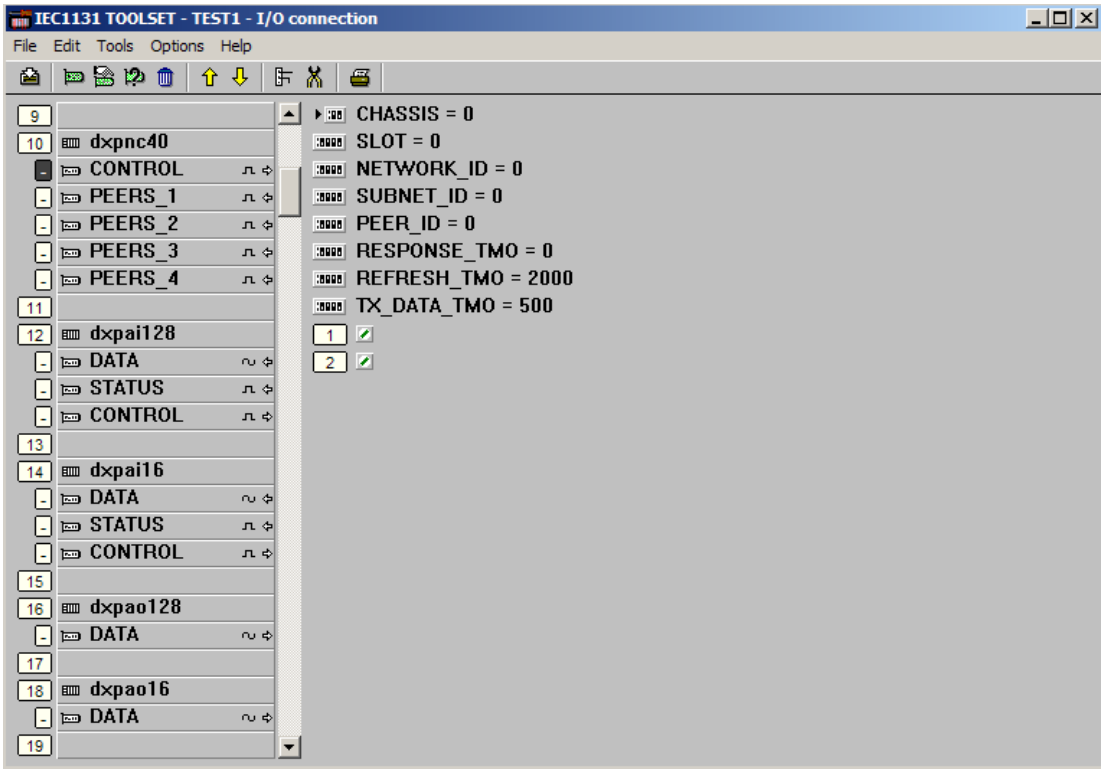

Figure 3 Peer Subnet Control board CONTROL rack

The user must enter data as detailed below:

1. CHASSIS – Logical chassis where the communication interface is installed. Range 1 - 29.
2. SLOT – this is the slot where the communications interface is installed. Range 1 – 12.
3. NETWORK_ID - Peer network number supported by this controller. Range 1 – 8.
4. SUBNET_ID - Subnet number within peer network supported by this controller. Range 1 – 8.
5. PEER_ID - Peer identity of this controller. Range 1 – 40.
6. RESPONSE_TMO – Milliseconds allowed for a peer to acknowledge a data packet. If this field is set to zero, no acknowledgement is required. This field need only be specified as non-zero to avoid network packet sequence errors in networks where the propagation delay between any two nodes could exceed 1 ms. Range 0 – 10000.
7. REFRESH_TMO - This represents the milliseconds a network controller will wait for a token from the master before declaring the network inoperable and discarding any data awaiting transmission. This time must be configured for both master and slave modes. Range 1 – 10000.
8. TX_DATA_TMO – This represents the milliseconds a network master controller will wait for a slave to complete transmission of its data and return the token before declaring the slave absent. This parameter will be ignored during slave mode. Range 1 – 10000.
9. Boolean output variable 1 – Peer Communications using this controller is started/stopped by this Boolean output. TRUE = Controller enabled.
10. Boolean output variable 2 – Master / Slave setting for the controller. TRUE = Master, FALSE = Slave.
11. Figure 4 shows a display of one of the four peer IP and status racks on the Peer Subnet Control board.

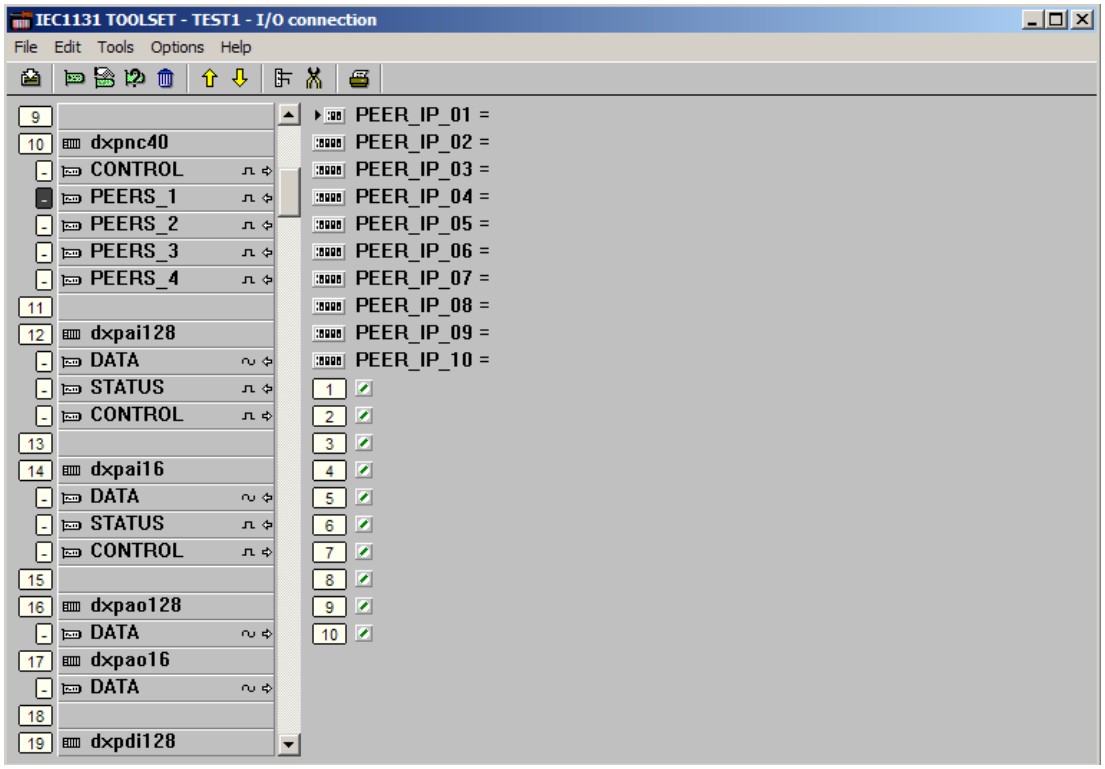

Figure 4 Peer Subnet Control board PEERS rack

The status rack contains ten IP addresses and ten status bits which indicate the status of the peers on the network.

PEER_IP_01 to 10 – IP address of peers with PEER_IDs of 1 to 10 in the subnet.

Boolean Inputs 1 to 10 - Each bit is set to TRUE when the peer associated with the IP address (PEER_IP_01 to 10) is active and FALSE when inactive.

E.g. Point 1 is the status of the peer configured as PEER_IP_01.

Boards PEERS_2 to PEERS_4 are for peers 11 to 40 in groups of ten.

2.2. Peer to Peer Data Boards

There are four different peer input boards (two analogue and two digital) that can be selected to ensure that the optimum communication packet size can be used for the application. Each input board has a corresponding output board that must be of the same type and channel quantity.

There are two versions of the analogue data boards, a 16 channel version and a 128 channel version. Both are configured the same. They only differ in the number of data channels supported. Similarly there are 16 and 128 channel versions of the digital channel boards.

Each output board delivers data to one or more input boards across one peer network. Note that the subnet of the peer network used to send the data is transparent to the input and output boards. More than one subnet may be defined using Peer Subnet Control boards to provide redundant communications. Peer subnet control boards must be defined before their respective input/output boards in the I/O connection editor.

Note that for a Peer output to communicate with a Peer input, they must share the same network number (NETWORK_ID), reference each others' peer numbers (TARGET_PEER_ID and SOURCE_PEER_ID) and have the same data block number (SOURCE_DATA_ID). The combination of these three identities should be considered as a global data identifier which must be uniquely defined across the entire peer network for each I/O board pair. The SOURCE_DATA_ID must be unique for all peer traffic between any two peers. It is recommended to set different SOURCE_DATA_IDs for each output block within each network in each system; this will ensure that they are unique at all destinations.

2.2.1. Analogue Input Boards

Figure 5 shows the data rack display associated with an IEC 61131 Toolset 16 channel analogue input board selected for incoming data to a Trusted controller.

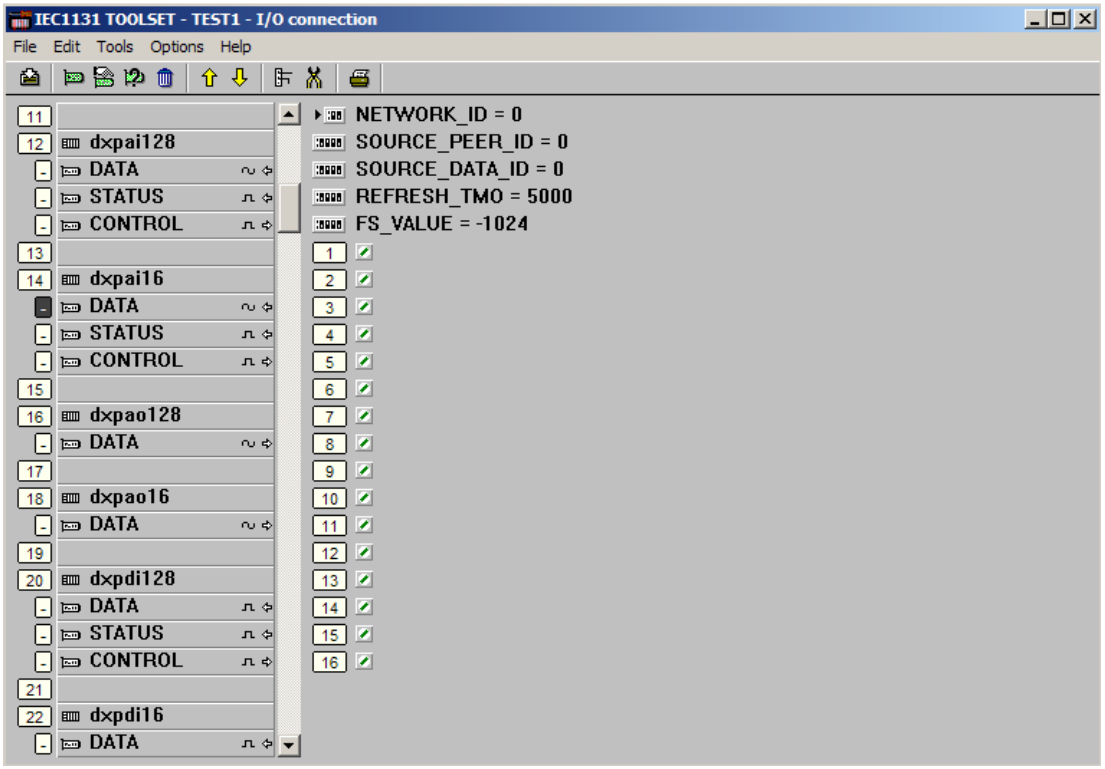

Figure 5 Peer to Peer Input Board Display

The user must enter data as detailed below.

1. NETWORK_ID – The network that is carrying the data. Data will be received via all peer controllers that share this network identity. Range 1 – 8.
2. SOURCE_PEER_ID – The peer that is sending the data. Range 1 – 40.
3. SOURCE_DATA_ID - Unique data block number defined at the output board. Range 1-64.
4. REFRESH_TMO - The maximum number of milliseconds allowed between successive refreshes of input data before the data is declared invalid. Note that following this time the input data will either retain the last received values or revert to a fail-safe condition according to the state of control rack variable 1. Range 1-10000.
5. FS_VALUE - Control value adopted by inputs when input is status has failed. Where input corresponds to an integer, fractional part is truncated. This value is always adopted at application start-up, though it will not be used again while RACK 3:Variable 1 is set TRUE. Range -9.999999e+38 to +9.999999e+38.

6. Analogue variable inputs 1 to 16 – Analogue values received from the corresponding channel of the selected output board in the sending system. The values are 32 bit and will assume either a 32 bit signed integer format or 32 bit real format depending on the variable to which it is connected. Both the specific input channel and its corresponding output channel must be connected to the same variable type. Different channels on a rack can use different variable types.
7. The 128 input peer board supports 128 analogue inputs instead of 16 but is otherwise identical. Note that safety related data using 128 analogue channel blocks must be sent via two different input/output block pairs and compared at the receiving input end in the application to ensure safety integrity. Alternatively it may be broken into 16 channel blocks.

Figure 6 shows a display of the refresh status rack of the associated analogue input board.

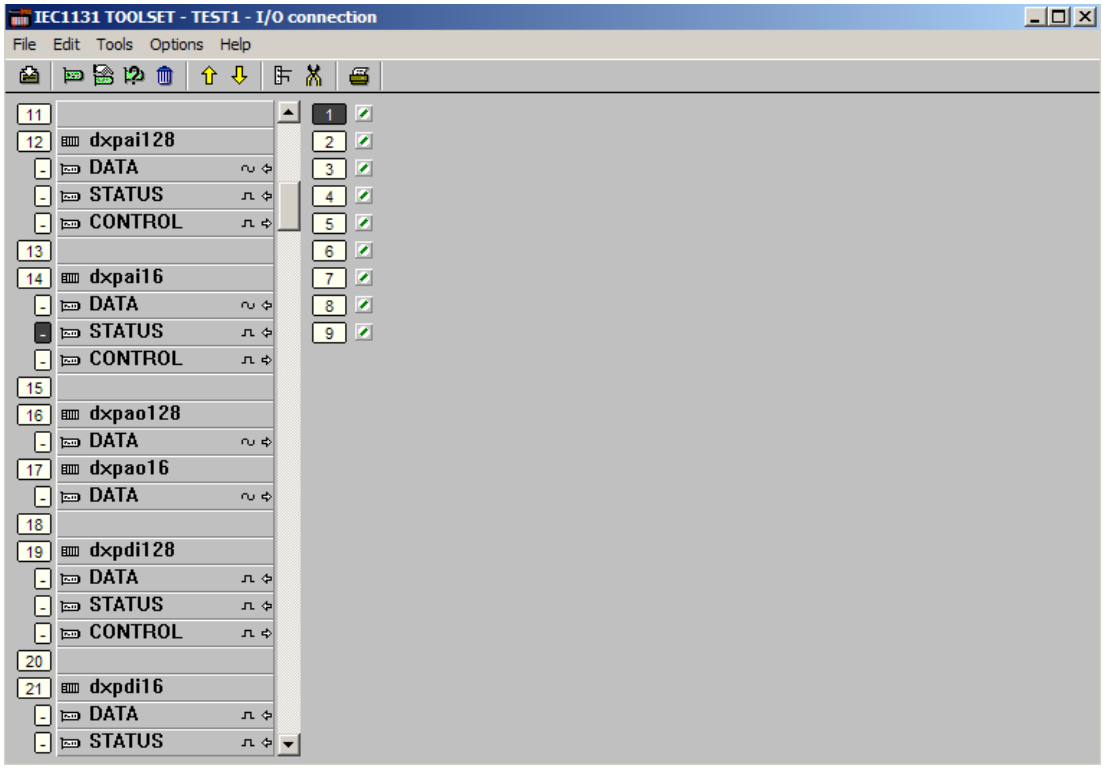

Figure 6 Input Board Status Display

Variable 1: TRUE = Input data is valid, i.e. refreshed within REFRESH_TMO

Variable 2-9: TRUE = Data has been refreshed within REFRESH_TMO by subnet 1-8, respectively. This status is intended for detection of latent faults within a redundant network. The data is delivered over all available programmed subnets simultaneously. If any of these variables goes FALSE for a programmed subnet, then data has failed to arrive on that subnet within the REFRESH_TMO. The variables for programmed subnets may be combined through an AND gate to provide an indication of full redundancy on that particular data path.

Figure 7 shows a display of the control rack of the associated analogue input board.

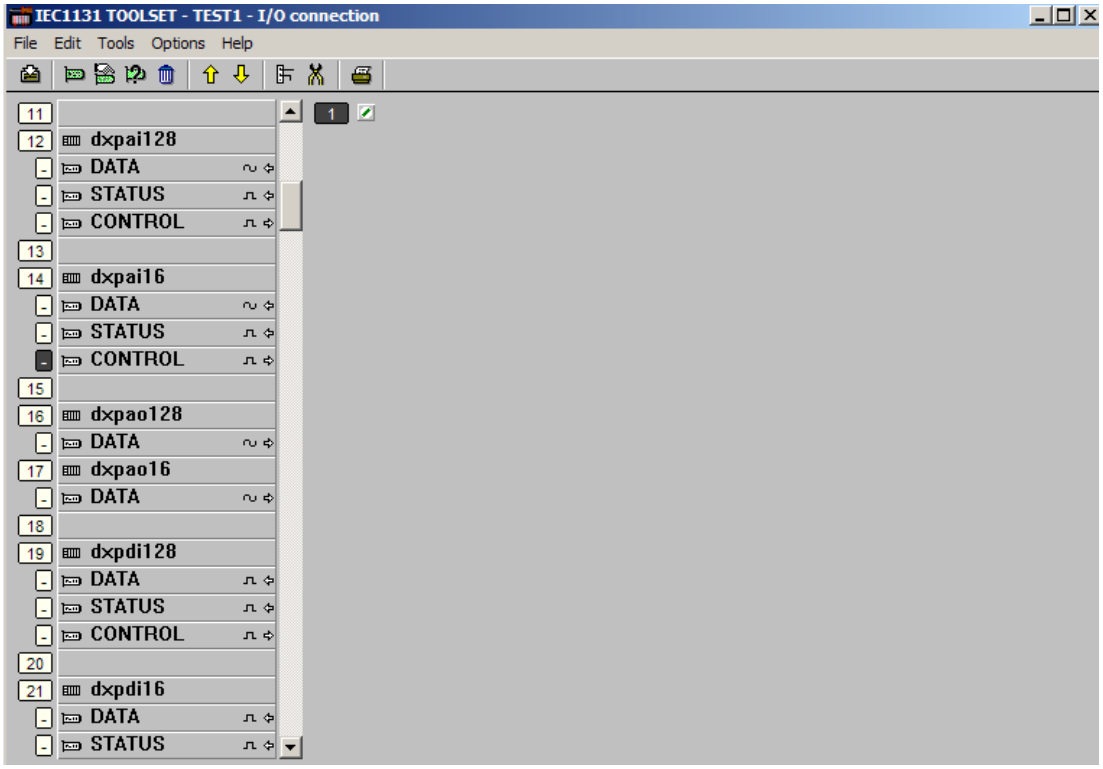

Figure 7 Input Board Control Display

This rack controls the whether the input values hold last state if refresh timer expires or go to 0.

Variable 1: FALSE = Force data to the fail safe state when data is invalid. TRUE = Allow previous data to persist when data is invalid.

2.2.2. Digital Input Boards

Figure 8 shows the data rack display associated with an IEC 61131 Toolset 16 channel digital input board selected for incoming data to a Trusted controller.

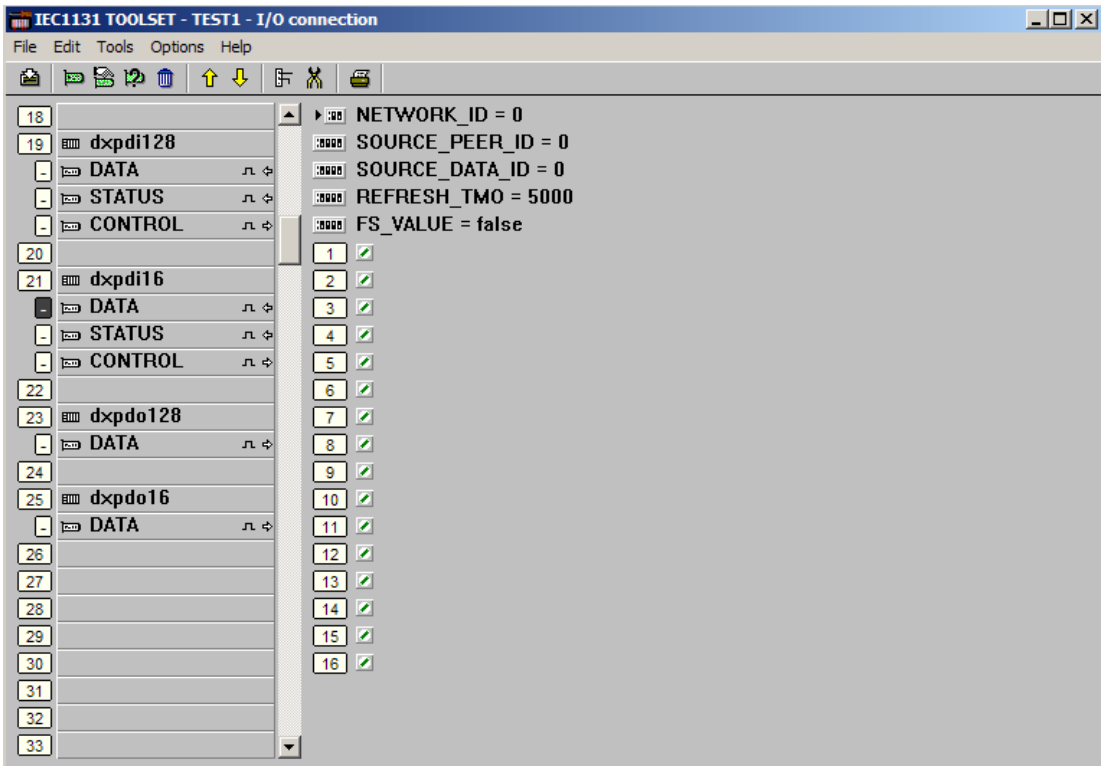

Figure 8 Peer to Peer Input Data Rack Display

The user must enter data as detailed below:

1. NETWORK_ID – The network that is carrying the data. Data will be received via all peer controllers that share this network identity. Range 1 – 8.
2. SOURCE_PEER_ID – The peer that is sending the data. Range 1 – 40.
3. SOURCE_DATA_ID - Unique data block number defined at the output board. Range 1-64.
4. REFRESH_TMO - The maximum number of milliseconds allowed between successive refreshes of input data before the data is declared invalid. Note that following this time the input data will either retain the last received values or revert to a fail-safe condition according to the state of control rack variable 1. Range 1-10000.
5. FS_VALUE - Control value adopted by inputs when input is status has failed. This value is always adopted at application start-up, though it will not be used again while RACK 3:Variable 1 is set TRUE. Range FALSE/TRUE.
6. Boolean variable inputs 1 to 16 – Boolean values received from the corresponding channel of the selected output board in the sending system.
7. The 128 input peer board supports 128 Boolean inputs instead of 16 but is otherwise identical.

Figure 9 shows a display of the refresh status rack of the associated digital input board.

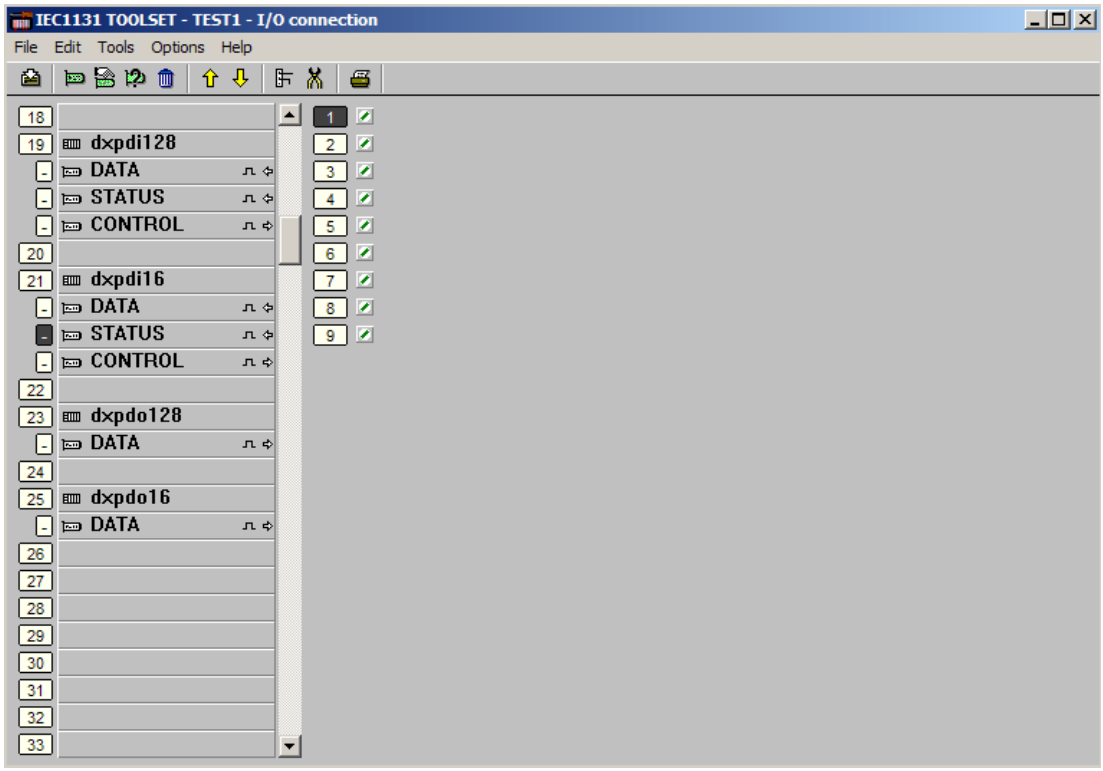

Figure 9 Input Board Status Display

Variable 1: TRUE = Input data is valid, i.e. refreshed within REFRESH_TMO

Variable 2-9: TRUE = Data has been refreshed within REFRESH_TMO by subnet 1-8, respectively. This status is intended for detection of latent faults within a redundant network. The data is delivered over all available programmed subnets simultaneously. If any of these variables goes FALSE for a programmed subnet, then data has failed to arrive on that subnet within the REFRESH_TMO. The variables for programmed subnets may be combined through an AND gate to provide an indication of full redundancy on that particular data path.

Figure 10 shows a display of the control rack of the associated digital input board.

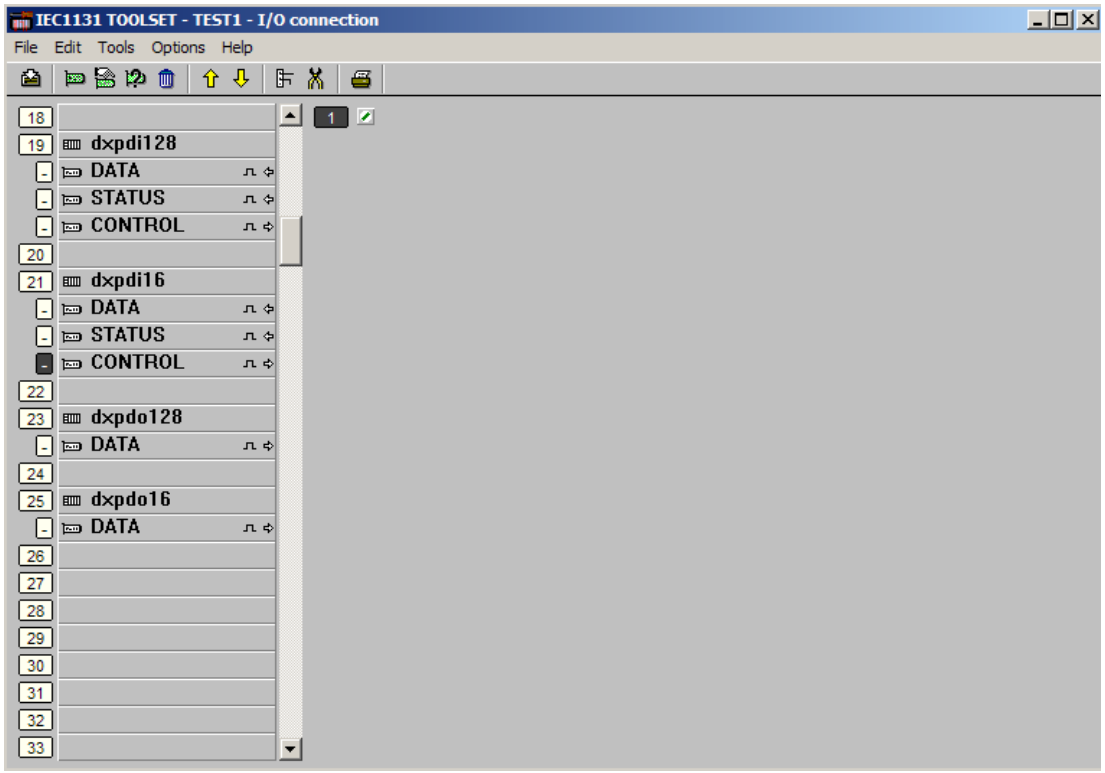

Figure 10 Input Board Control Display

This rack controls whether the input values hold last state if refresh timer expires or go to FALSE.

Variable 1: FALSE = Force data to RACK 1:FS_VALUE when data is invalid. TRUE = Allow previous data to persist when data is invalid.

2.2.3. Analogue Output Boards

Figure 11 shows the display associated with an IEC 61131 Toolset 16 channel analogue output board selected for outgoing data to a Trusted controller.

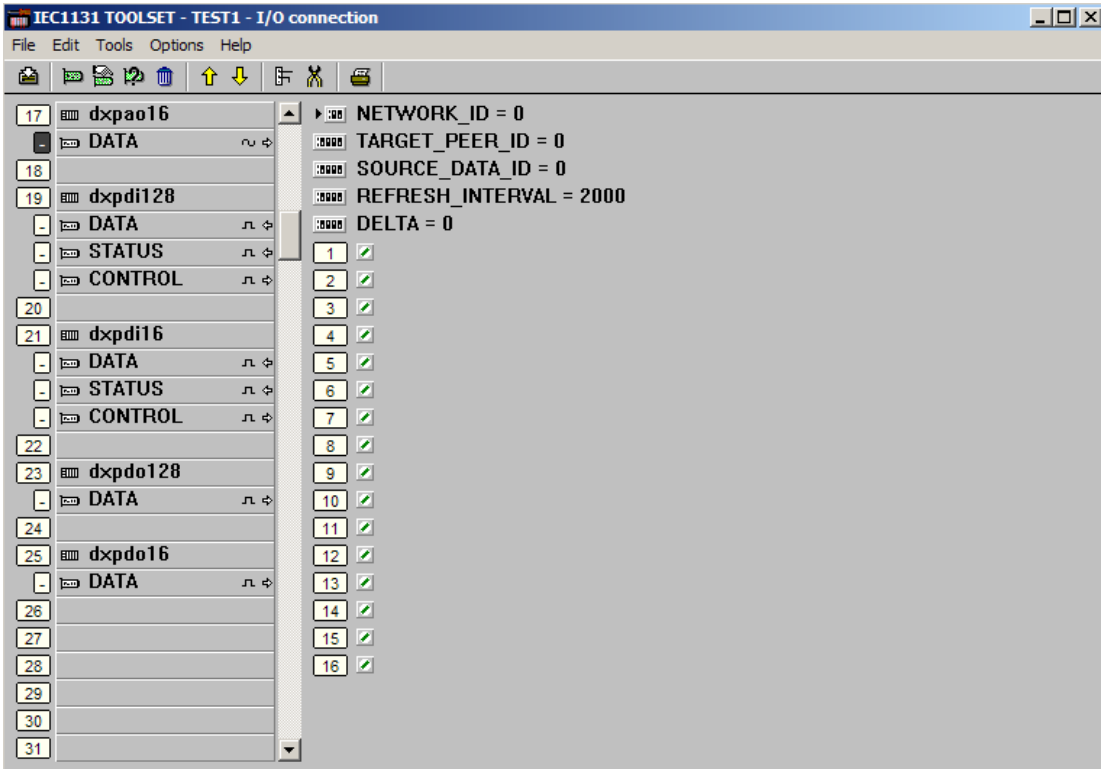

Figure 11 Peer to Peer Analogue Output Board Display

The user must enter data as detailed below:

1. NETWORK_ID – The network that is carrying the data. Data will be received via all peer controllers that share this network identity. Range 1 – 8.
2. TARGET_PEER_ID - The peer that is receiving the data, or the multicast 'peer'. Range 1 – 40.
3. SOURCE_DATA_ID - Unique data block number to allow input boards to distinguish the data. Range 1-64.
4. REFRESH_INTERVAL - The maximum number of milliseconds allowed between successive transmissions of the output data. Note that data will be sent immediately following any change of output state. If a value of zero is specified in this field then data will be refreshed every application scan regardless of output state change. Range 0-10000.
5. DELTA - Minimum change in any output variable required before update is sent to Peer, not withstanding refresh interval. When applied to integers, fractional part is truncated. Range 0 to 9.999999e+038.
6. Analogue variable outputs 1 to 16 – 32 bit integer or real analogue outputs. Note that no conversion will be applied when transferring real or integer data and therefore it is required that each input data variable matches its respective output variable type.
7. The 128 output peer board supports 128 analogue outputs instead of 16 but is otherwise identical. Note that safety related data using 128 analogue channel blocks must be sent via two different input/output block pairs and compared at the receiving input end in the application to ensure safety integrity. Alternatively it may be broken into 16 channel blocks.

2.2.4. Digital Output Boards

Figure 12 shows the display associated with an IEC 61131 Toolset 16 channel digital output board selected for outgoing data to a Trusted controller.

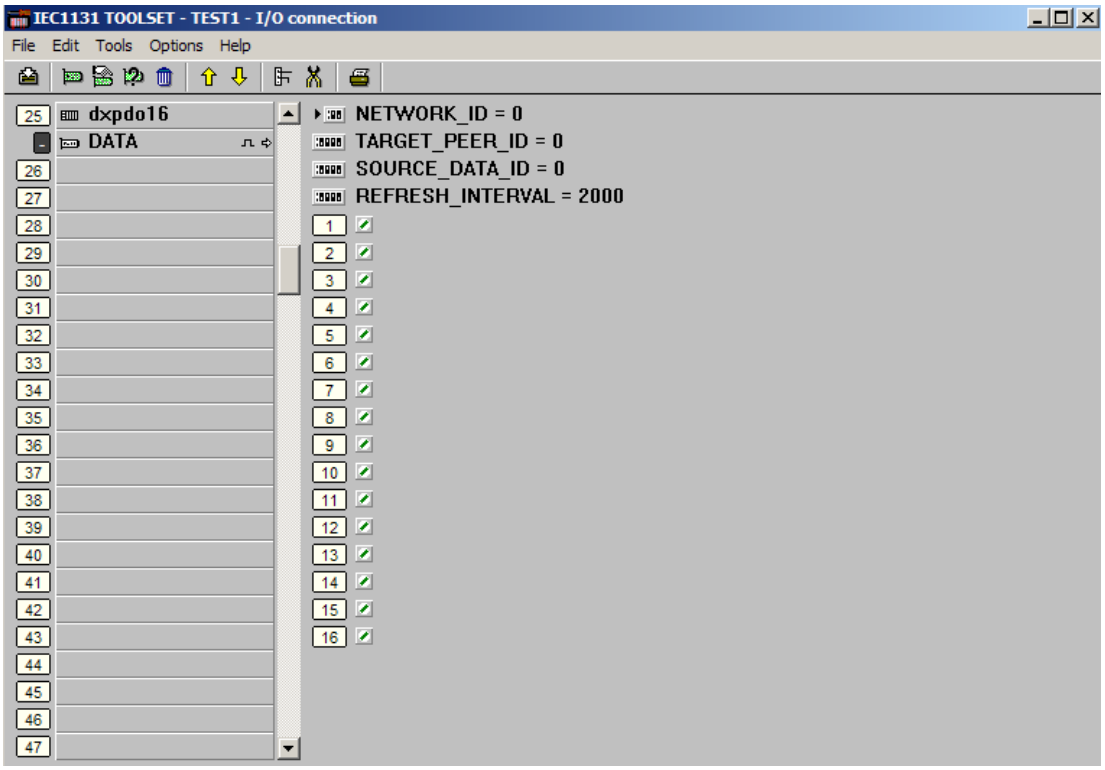

Figure 12 Peer to Peer Digital Output Board Display

The user must enter data as detailed below:

1. NETWORK_ID – The network that is carrying the data. Data will be received via all peer controllers that share this network identity. Range 1 – 8.
2. TARGET_PEER_ID - The peer that is receiving the data, or the multicast 'peer'. Range 1 – 40.
3. SOURCE_DATA_ID - Unique data block number to allow input boards to distinguish the data. Range 1-64.
4. REFRESH_INTERVAL - The maximum number of milliseconds allowed between successive transmissions of the output data. Note that data will be sent immediately following any change of output state. If a value of zero is specified in this field then data will be refreshed every application scan regardless of output state change. Range 0-10000.
5. Boolean variable outputs 1 to 16 – Boolean outputs.
6. The 128 output peer board supports 128 Boolean outputs instead of 16.

2.3. Peer to Peer Configuration Example 1

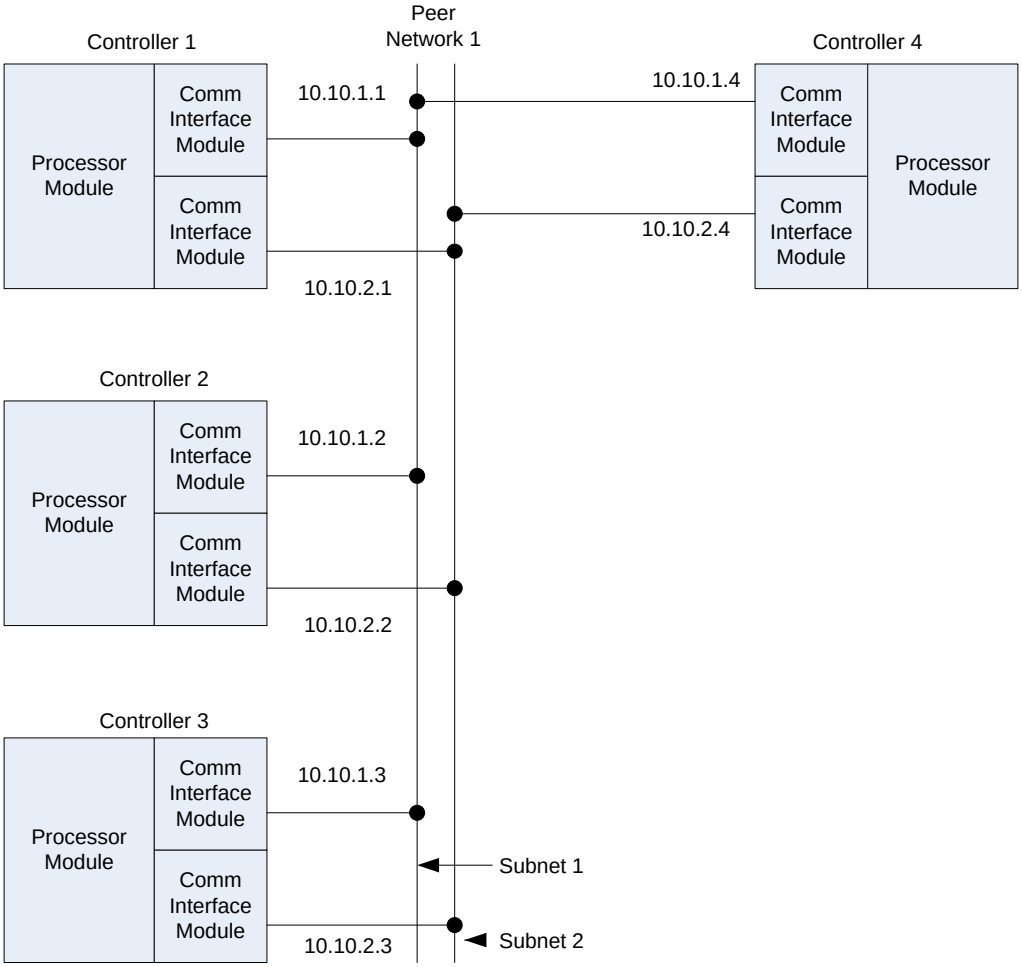

Figure 13 Example 1 & 2 Peer to Peer Configuration.

1. Figure 13 shows an example configuration for a system using 4 controllers connected together using one peer to peer network with dual physical network paths.
2. In this example, Controller 4 will be the master of network 1 subnet 1. Controller 1 will be the master of network 1 subnet 2.
3.

- 16 analogue points will be sent from controller 1 to controller 2.
- A separate set of 16 analogue values will be sent from controller 1 to controller 3.
- 16 digital values will be sent from controller 2 to controller 4.

2.3.1. Controller 1 settings

Dual Peer to Peer Net Control, network 1 subnet 1.

dxpnc40 – CONTROL rack	Value	Comment
CHASSIS	1	Communication module located in chassis 1.
SLOT	7	Communication module is located in slot 7.
NETWORK_ID	1	Network 1
SUBNET_ID	1	Subnet 1
PEER_ID	1	Identity of this controller.
RESPONSE_TMO	0	Default
REFRESH_TMO	2000	Default
TX_DATA_TMO	500	Default
Variable 1	TRUE	Enable Peer on this subnet.
Variable 2	FALSE	This is a slave connection.
PEERS_1 rack		
PEER_IP_01	10.10.1.1	Controller 1, network 1, subnet 1
PEER_IP_02	10.10.1.2	Controller 2, network 1, subnet 1
PEER_IP_03	10.10.1.3	Controller 3, network 1, subnet 1
PEER_IP_04	10.10.1.4	Controller 4, network 1, subnet 1
PEER_IP_05		
PEER_IP_06		
PEER_IP_07		

Table 1 Example 1 - Controller 1 Net Control, network 1 subnet 1.

Dual Peer to Peer Net Control, network 1 subnet 2.

dxpnc40 – CONTROL rack	Value	Comment
CHASSIS	1	Communication module located in chassis 1.
SLOT	8	Communication module is located in slot 8.
NETWORK_ID	1	Network 1
SUBNET_ID	2	Subnet 2
PEER_ID	1	Identity of this controller.
RESPONSE_TMO	0	Default
REFRESH_TMO	2000	Default
TX_DATA_TMO	500	Default
Variable 1	TRUE	Enable peer on this subnet.
Variable 2	TRUE	This is the master of the subnet.
PEERS_1 rack		
PEER_IP_01	10.10.2.1	Controller 1, network 1, subnet 2
PEER_IP_02	10.10.2.2	Controller 2, network 1, subnet 2
PEER_IP_03	10.10.2.3	Controller 3, network 1, subnet 2
PEER_IP_04	10.10.2.4	Controller 4, network 1, subnet 2
PEER_IP_05		
PEER_IP_06		
PEER_IP_07		

Table 2 Example 1 - Controller 1 Net Control, network 1 subnet 2.

2.3.2. Controller Setting Summary

Dual Peer to Peer Net Control, network 1 subnet 1.

dxpnc40 – CONTROL rack	Controller 1	Controller 2	Controller 3	Controller 4
CHASSIS	1	1	1	1
SLOT	7	7	7	7
NETWORK_ID	1	1	1	1
SUBNET_ID	1	1	1	1
PEER_ID	1	2	3	4
RESPONSE_TMO	0	0	0	0
REFRESH_TMO	2000	2000	2000	2000
TX_DATA_TMO	500	500	500	500
Variable 1	TRUE	TRUE	TRUE	TRUE
Variable 2	FALSE	FALSE	FALSE	TRUE
PEERS_1 rack				
PEER_IP_01	10.10.1.1	10.10.1.1	10.10.1.1	10.10.1.1
PEER_IP_02	10.10.1.2	10.10.1.2	10.10.1.2	10.10.1.2
PEER_IP_03	10.10.1.3	10.10.1.3	10.10.1.3	10.10.1.3
PEER_IP_04	10.10.1.4	10.10.1.4	10.10.1.4	10.10.1.4
PEER_IP_05				

Table 3 Example 1 - Controller Setting Summary Net Control, network 1 subnet 1.

Dual Peer to Peer Net Control, network 1 subnet 2.

dxpnc40 – CONTROL rack	Controller 1	Controller 2	Controller 3	Controller 4
CHASSIS	1	1	1	1
SLOT	8	8	8	8
NETWORK_ID	1	1	1	1
SUBNET_ID	2	2	2	2
PEER_ID	1	2	3	4
RESPONSE_TMO	0	0	0	0
REFRESH_TMO	2000	2000	2000	2000
TX_DATA_TMO	500	500	500	500
Variable 1	TRUE	TRUE	TRUE	TRUE
Variable 2	TRUE	FALSE	FALSE	FALSE
PEERS_1 rack				
PEER_IP_01	10.10.2.1	10.10.2.1	10.10.2.1	10.10.2.1
PEER_IP_02	10.10.2.2	10.10.2.2	10.10.2.2	10.10.2.2
PEER_IP_03	10.10.2.3	10.10.2.3	10.10.2.3	10.10.2.3
PEER_IP_04	10.10.2.4	10.10.2.4	10.10.2.4	10.10.2.4
PEER_IP_05				

Table 4 Example 1 - Controller Setting Summary Net Control, network 1 subnet 2.

2.3.3. Data Summary

Output data summary

	Controller 1		Controller 2
DATA rack	dxpao	dxpao	dxpdo
NETWORK_ID	1	1	1
TARGET_PEER_ID	2	3	4
SOURCE_DATA_ID	1	2	1
REFRESH_TMO	2000	2000	2000
MIN_DELTA	20	20	
Variable 1 - 16	Analogue Data Output	Analogue Data Output	Digital Data Output

Table 5 Example 1 - Output data summary

Input data summary

	Controller 2	Controller 3	Controller 4
DATA rack	dxpai	dxpai	dxpdi
NETWORK_ID	1	1	1
SOURCE_PEER_ID	1	1	2
SOURCE_DATA_ID	1	2	1
REFRESH_TMO	5000	5000	5000
FS_VALUE	-1024	-1024	FALSE
Variable 1 - 16	Analogue Data Input	Analogue Data Input	Boolean Data Input
STATUS rack			
Variable 1	Input data valid	Input data valid	Input data valid
Variable 2 - 9	Refreshed on subnet 1…8	Refreshed on subnet 1…8	Refreshed on subnet 1…8
CONTROL rack			
Variable 1	Failure action	Failure action	Failure action

Table 6 Example 1 - Input data summary

2.4. Peer to Peer Configuration Example 2

1. Figure 13 shows an example configuration for a system using 4 controllers connected together using one peer to peer network with dual physical network paths, but this time with multicast data.
2. In this example, Controller 4 will be the master of network 1 subnet 1. Controller 1 will be the master of network 1 subnet 2.
    - 16 digital points will be sent from controller 3 to controllers 1, 2 & 4 via a multicast configuration.
    - 16 analogue points will be sent from controller 1 to controller 2.
    - A separate set of 16 analogue values will be sent from controller 1 to controller 3.
    - 16 digital values will be sent from controller 2 to controller 4.

2.4.1. Controller 1 settings

Dual Peer to Peer Net Control, network 1 subnet 1.

dxpnc40 – CONTROL rack	Value	Comment
CHASSIS	1	Communication module located in chassis 1.
SLOT	7	Communication module is located in slot 7.
NETWORK_ID	1	Network 1
SUBNET_ID	1	Subnet 1
PEER_ID	1	Identity of this controller.
RESPONSE_TMO	0	Default
REFRESH_TMO	2000	Default
TX_DATA_TMO	500	Default
Variable 1	TRUE	Enable Peer to on this subnet.
Variable 2	FALSE	This is a slave connection.
PEERS_1 rack		
PEER_IP_01	10.10.1.1	Controller 1, network 1, subnet 1
PEER_IP_02	10.10.1.2	Controller 2, network 1, subnet 1
PEER_IP_03	10.10.1.3	Controller 3, network 1, subnet 1
PEER_IP_04	10.10.1.4	Controller 4, network 1, subnet 1
PEER_IP_05	239.255.1.1	Multicast address

Table 7 Example 2 - Controller 1 Settings Control, network 1 subnet 1

Dual Peer to Peer Net Control, network 1 subnet 2.

dxpnc40 – CONTROL rack	Value	Comment
CHASSIS	1	Communication module located in chassis 1.
SLOT	8	Communication module is located in slot 8.
NETWORK_ID	1	Network 1
SUBNET_ID	2	Subnet 2
PEER_ID	1	Identity of this controller.
RESPONSE_TMO	0	Default
REFRESH_TMO	2000	Default
TX_DATA_TMO	500	Default
Variable 1	TRUE	Enable peer on this subnet.
Variable 2	TRUE	This is the master of the subnet.
PEERS_1 rack		
PEER_IP_01	10.10.2.1	Controller 1, network 1, subnet 2
PEER_IP_02	10.10.2.2	Controller 2, network 1, subnet 2
PEER_IP_03	10.10.2.3	Controller 3, network 1, subnet 2
PEER_IP_04	10.10.2.4	Controller 4, network 1, subnet 2
PEER_IP_05	239.255.2.1	Multicast address

Table 8 Example 2 - Controller 1 Settings Control network 1 subnet 2

Dual Peer to Peer Digital Input (data is received via both subnets automatically).

dxpdi – DATA rack	Value	Comment
NETWORK	1	Network 1
SOURCE_PEER	3	This data must originate from the controller with IP specified in PEER_IP_03.
SOURCE_DATA_ID	1	Will receive data ID 1. This is a unique packet ID to enable the system to distinguish between different data packets routed between the same source and destination.
REFRESH_TMO	5000	Maximum time allowed before data is declared invalid.
FS_VALUE	FALSE	Fail safe state.
DATA rack		
Variable 1 - 16	Boolean	Digital Input points. Directly mapped to the points on the output board in controller 3.
STATUS rack		
Variable 1	Boolean Input	TRUE = data is valid. Will go to FALSE if the REFRESH_TMO times out.
Variable 2 - 9	Boolean Input	Data has been refreshed within the REFRESH_TMO by subnets 1-8 respectively.
CONTROL rack		
Variable 1	Boolean Output	FALSE = Force data to FALSE when invalid. TRUE = Allow previous value to persist when data is invalid.

Table 9 Example 2 - Digital Input (data received automatically from subnets)

Dual Peer to Peer Analogue Output (data is sent via both subnets automatically).

dxpao – DATA rack	Value	Comment
NETWORK_ID	1	Network 1
TARGET_PEER_ID	2	This output is going to PEER_IP_02.
SOURCE_DATA_ID	1	Will transmit data ID 1. This is a unique packet ID to enable the system to distinguish between different data packets routed between the same source and destination.
REFRESH_TMO	2000	Maximum time peer data is sent if no change of application values above the MIN_DELTA has occurred.
MIN_DELTA	20	The value change that is required before the data will be transmitted. If the value change is less than this, the value will be transmitted based on the REFRESH_TMO setting.
Variable 1 - 16	Analogue Output	Analogue output points.

Table 10 Example 2 - PEER_IP_02 Analogue Output (data sent automatically)

Dual Peer to Peer Analogue Output (data is sent via both subnets automatically).

dxpao – DATA rack	Value	Comment
NETWORK_ID	1	Network 1
TARGET_PEER_ID	3	This output is going to PEER_IP_03.
DATA_ID	2	Will transmit data ID 1. This is a unique packet ID to enable the system to distinguish between different data packets routed between the same source and destination.
REFRESH_TMO	2000	Maximum time peer data is sent if no change of application values above the MIN_DELTA has occurred.
MIN_DELTA	20	The value change that is required before the data will be transmitted. If the value change is less than this, the value will be transmitted based on the REFRESH_TMO setting.
Variable 1 - 16	Analogue Output	Analogue output points.

Table 11 Example 2 - PEER_IP_03 Analogue Output (data sent automatically)

2.4.2. Controller setting summary

Dual Peer to Peer Net Control, network 1 subnet 1.

dxpnc40 – CONTROL rack	Controller 1	Controller 2	Controller 3	Controller 4
CHASSIS	1	1	1	1
SLOT	7	7	7	7
NETWORK_ID	1	1	1	1
SUBNET_ID	1	1	1	1
PEER_ID	1	2	3	4
RESPONSE_TMO	0	0	0	0
REFRESH_TMO	2000	2000	2000	2000
TX_DATA_TMO	500	500	500	500
Variable 1	TRUE	TRUE	TRUE	TRUE
Variable 2	FALSE	FALSE	FALSE	TRUE
PEERS_1 rack				
PEER_IP_01	10.10.1.1	10.10.1.1	10.10.1.1	10.10.1.1
PEER_IP_02	10.10.1.2	10.10.1.2	10.10.1.2	10.10.1.2
PEER_IP_03	10.10.1.3	10.10.1.3	10.10.1.3	10.10.1.3
PEER_IP_04	10.10.1.4	10.10.1.4	10.10.1.4	10.10.1.4
PEER_IP_05	239.255.1.1	239.255.1.1	239.255.1.1	239.255.1.1

Table 12 Example 2 - Dual Peer to Peer Control network 1 subnet 1

Dual Peer to Peer Net Control, network 1 subnet 2.

dxpnc40 – CONTROL rack	Controller 1	Controller 2	Controller 3	Controller 4
CHASSIS	1	1	1	1
SLOT	8	8	8	8
NETWORK_ID	1	1	1	1
SUBNET_ID	2	2	2	2
PEER_ID	1	2	3	4
RESPONSE_TMO	0	0	0	0
REFRESH_TMO	2000	2000	2000	2000
TX_DATA_TMO	500	500	500	500
Variable 1	TRUE	TRUE	TRUE	TRUE
Variable 2	TRUE	FALSE	FALSE	FALSE
PEERS_1 rack				
PEER_IP_01	10.10.2.1	10.10.2.1	10.10.2.1	10.10.2.1
PEER_IP_02	10.10.2.2	10.10.2.2	10.10.2.2	10.10.2.2
PEER_IP_03	10.10.2.3	10.10.2.3	10.10.2.3	10.10.2.3
PEER_IP_04	10.10.2.4	10.10.2.4	10.10.2.4	10.10.2.4
PEER_IP_05	239.255.2.1	239.255.2.1	239.255.2.1	239.255.2.1

Table 13 Example 2 - Dual Peer to Peer Net control network 1 subnet 2

2.4.3. Data Summary

Output data summary

	Controller 1		Controller 2	Controller 3
DATA rack	dxpao	dxpao	dxpdo	dxpdo
NETWORK_ID	1	1	1	1
TARGET_PEER_ID	2	3	4	5
SOURCE_DATA_ID	1	2	1	1
REFRESH_TMO	2000	2000	2000	2000
MIN_DELTA	20	20		
Variable 1 - 16	Analogue Data Output	Analogue Data Output	Digital Data Output	Digital Data Output

Table 14 Example 2 - Output Data Summary

Input data summary

	Controller 1	Controller 2		Controller 3	Controller 4	
DATA rack	dxpdi	dxpdi	dxpai	dxpai	dxpdi	dxpdi
NETWORK_ID	1	1	1	1	1	1
SOURCE_PEER	3*	3*	1	1	3*	2
SOURCE_DATA_ID	1	1	1	2	1	1
REFRESH_TMO	5000	5000	5000	5000	5000	5000
FS_VALUE	FALSE	FALSE	-1024	-1024	FALSE	FALSE
Variable 1 - 16	Boolean Data Input	Boolean Data Input	Analogue Data Input	Analogue Data Input	Boolean Data Input	Boolean Data Input
STATUS rack						
Variable 1	Input data valid	Input data valid	Input data valid	Input data valid	Input data valid	Input data valid
Variable 2 - 9	Refreshed on subnet 1…8	Refreshed on subnet 1…8	Refreshed on subnet 1…8	Refreshed on subnet 1…8	Refreshed on subnet 1…8	Refreshed on subnet 1…8
CONTROL rack						
Variable 1	Failure action	Failure action	Failure action	Failure action	Failure action	Failure action

Table 15 Example 2 - Input data summary

* Multi cast data receive from controller 3. The communication modules for network 1 on controllers 1, 2 and 4 must have the multicast IP address added to the communication module multicast address list; refer to Multicast Configuration in PD-T8151B.

2.5. Peer to Peer Configuration Example 3

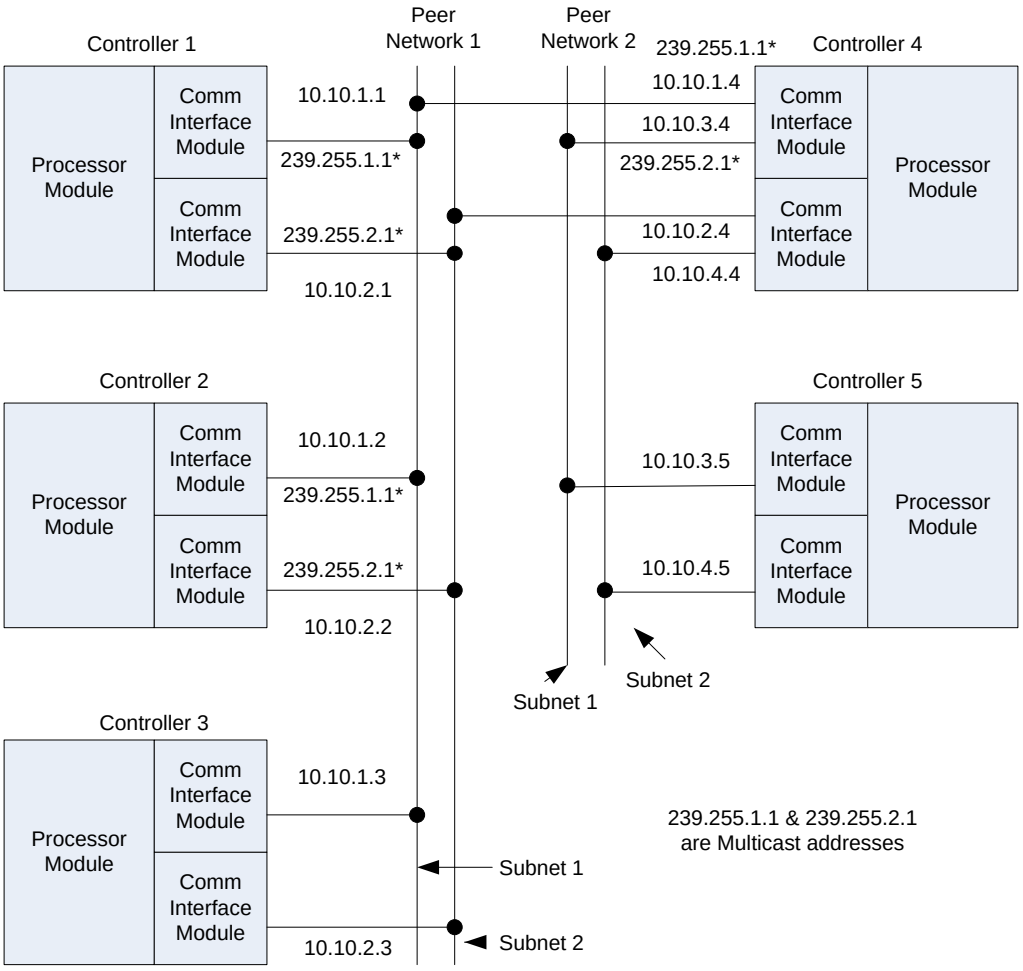

Figure 14 Example 3 Peer to Peer Configuration.

1. Figure 14 shows an example configuration for a system using 5 controllers connected together using two separate peer to peer networks, each having dual physical network paths.
2. In this example, Controller 4 will be the master of network 1 subnet 1 and network 2 subnet 1. Controller 1 will be the master of network 1 subnet 2 and Controller 5 will be the master of network 2 subnet 2.

- 16 digital points will be sent from controller 3 to controllers 1, 2 & 4 via a multicast configuration.
- 16 analogue points will be sent from controller 1 to controller 2.
- A separate set of 16 analogue values will be sent from controller 1 to controller 3.
- 16 digital values will be sent from controller 2 to controller 5. Controller 5 is on a different peer network than controller 2, therefore to achieve the data transfer 16 values will be sent from controller 2 to controller 4 and the application in controller 4 will connect the input signals to an output board which in turn will send the data to controller 5.

2.5.1. Controller setting summary

Dual Peer to Peer Net Control, network 1 subnet 1.

dxpnc40 – CONTROL rack	Controller 1	Controller 2	Controller 3	Controller 4
CHASSIS	**1**	**1**	**1**	**1**
SLOT	7	7	7	7
NETWORK_ID	1	1	1	1
SUBNET_ID	1	1	1	1
PEER_ID	1	2	3	4
RESPONSE_TMO	0	0	0	0
REFRESH_TMO	2000	2000	2000	2000
TX_DATA_TMO	500	500	500	500
Variable 1	TRUE	TRUE	TRUE	TRUE
Variable 2	FALSE	FALSE	FALSE	TRUE
PEERS_1 rack				
PEER_IP_01	10.10.1.1	10.10.1.1	10.10.1.1	10.10.1.1
PEER_IP_02	10.10.1.2	10.10.1.2	10.10.1.2	10.10.1.2
PEER_IP_03	10.10.1.3	10.10.1.3	10.10.1.3	10.10.1.3
PEER_IP_04	10.10.1.4	10.10.1.4	10.10.1.4	10.10.1.4
PEER_IP_05	239.255.1.1	239.255.1.1	239.255.1.1	239.255.1.1

Table 16 Example 3 - Controller Setting Control network 1 subnet 1

Dual Peer to Peer Net Control, network 1 subnet 2.

dxpnc40 – CONTROL rack	Controller 1	Controller 2	Controller 3	Controller 4
CHASSIS	1	1	1	1
SLOT	8	8	8	8
NETWORK_ID	1	1	1	1
SUBNET_ID	2	2	2	2
PEER_ID	1	2	3	4
RESPONSE_TMO	0	0	0	0
REFRESH_TMO	2000	2000	2000	2000
TX_DATA_TMO	500	500	500	500
Variable 1	TRUE	TRUE	TRUE	TRUE
Variable 2	TRUE	FALSE	FALSE	FALSE
PEERS_1 rack				
PEER_IP_01	10.10.2.1	10.10.2.1	10.10.2.1	10.10.2.1
PEER_IP_02	10.10.2.2	10.10.2.2	10.10.2.2	10.10.2.2
PEER_IP_03	10.10.2.3	10.10.2.3	10.10.2.3	10.10.2.3
PEER_IP_04	10.10.2.4	10.10.2.4	10.10.2.4	10.10.2.4
PEER_IP_05	239.255.2.1	239.255.2.1	239.255.2.1	239.255.2.1

Table 17 Example 3 - Controller Setting Control network1 subnet 2

Dual Peer to Peer Net Control, network 2 subnet 1.

dxpnc40 – CONTROL rack	Controller 4	Controller 5
CHASSIS	1	1
SLOT	7	7
NETWORK_ID	2	2
SUBNET_ID	1	1
PEER_ID	1	2
RESPONSE_TMO	0	0
REFRESH_TMO	2000	2000
TX_DATA_TMO	500	500
Variable 1	TRUE	TRUE
Variable 2	TRUE	FALSE
PEERS_1 rack		
PEER_IP_01	10.10.3.4	10.10.3.4
PEER_IP_02	10.10.3.5	10.10.3.5
PEER_IP_03		

Table 18 Example 3 - Dual Peer to Peer Net Control network 1 subnet 1

Dual Peer to Peer Net Control, network 2 subnet 2.

dxpnc40 – CONTROL rack	Controller 4	Controller 5
CHASSIS	1	1
SLOT	8	8
NETWORK_ID	2	2
SUBNET_ID	2	2
PEER_ID	1	2
RESPONSE_TMO	0	0
REFRESH_TMO	2000	2000
TX_DATA_TMO	500	500
Variable 1	TRUE	TRUE
Variable 2	FALSE	TRUE
PEERS_1 rack		
PEER_IP_01	10.10.4.4	10.10.4.4
PEER_IP_02	10.10.4.5	10.10.4.5
PEER_IP_03		

Table 19 Example 3 - Dual Peer to Peer Net Control network 2 subnet 2

2.5.2. Data Summary

Output data summary

	Controller 1		Controller 2	Controller 3	Controller 4
DATA rack	dxpao	dxpao	dxpdo	dxpdo	dxpdo
NETWORK_ID	1	1	1	1	2
TARGET_PEER_ID	2	3	4	5	2
SOURCE_DATA_ID	1	2	1	1	1
REFRESH_TMO	2000	2000	2000	2000	2000
MIN_DELTA	20	20			
Variable 1 - 16	Analogue Data Output	Analogue Data Output	Digital Data Output	Digital Data Output	Digital Data Output

Table 20 Example 3 - Output data summary

Input data summary

	Controller 1	Controller 2		Controller 3	Controller 4		Controller 5
DATA rack	dxpdi	dxpdi	dxpai	dxpai	dxpdi	dxpdi	dxpdi
NETWORK_ID	1	1	1	1	1	1	2
SOURCE_PEER_ID	3*	3*	1	1	3*	2	1
SOURCE_DATA_ID	1	1	1	2	1	1	1
REFRESH_TMO	5000	5000	5000	5000	5000	5000	5000
FS_VALUE	FALSE	FALSE	-1024	-1024	FALSE	FALSE	FALSE
Variable 1 - 16	Boolean Data Input	Boolean Data Input	Analogue Data Input	Analogue Data Input	Boolean Data Input	Boolean Data Input	Boolean Data Input
STATUS rack							
Variable 1	Input data valid	Input data valid	Input data valid	Input data valid	Input data valid	Input data valid	Input data valid
Variable 2 - 9	Refreshed on subnet 1…8	Refreshed on subnet 1…8	Refreshed on subnet 1…8	Refreshed on subnet 1…8	Refreshed on subnet 1…8	Refreshed on subnet 1…8	Refreshed on subnet 1…8
CONTROL rack							
Variable 1	Failure action	Failure action	Failure action	Failure action	Failure action	Failure action	Failure action

Table 21 Example 3 - Input data summary

* Multi cast data receive from controller 3. The communication modules for network 1 on controllers 1, 2 and 4 must have the multicast IP address added to the communication module multicast address list; refer to Multicast Configuration in PD-T8151B.

2.6. Suggested Configuration

The Peer to Peer I/O board definitions for timeout parameters should be set appropriate to the peer system as described below.

Equipment	Parameter	Description
dxpnc40		
	RESPONSE_TMO	0 ms is recommended on a local network.
	REFRESH_TMO	(Npeer x TX_DATA_TMO)
Master	TX_DATA_TMO	Set to RESPONSE_TMO or 2 ms, whichever is greater, multiplied by the maximum number of (dxpao + dxpdo) output boards in any single controller + 16 ms.
dxpdi & dxpai		
Input	REFRESH_TMO	Set to the longest acceptable time before stale data should cause a trip. (this time is used as Input REFRESH_TMO below)
dxpdo & dxpao		
Output	REFRESH_TMO	$\frac{\text{(Input REFRESH\_TMO) - ((Npeer x TX\_DATA\_TMO) + TSsource + TSdest + 50 ms)}}{2}$

Table 22 Peer to Peer I/O Board definitions for Timeouts Parameters

Where: -

Npeer = number of peer to peer controllers

TSsource = Maximum application scan time of controller with output board

TSdest = Maximum application scan time of controller with input board

Note that if the Output REFRESH_TMO calculation results in a negative number, then the Peer to Peer network is too complex for the Process Safety Time.

2.7. Peer Network Specification

No. of Peer Networks per System	≤ 8
Target Inter-application Response	
Single point change	nx15 ms + 2x(source + destination application scan)
All points change	nx15 ms(per 1000 digital points per node) + nx15 ms(per 60 analogue points per node) + 2x(source + destination application scan) n=no. of nodes/systems on the network
No. of Nodes per Network	$2 \leq n \leq 40$
Points per Node/System	Peer Communication points are to be included in the total number of external points. Each point is equivalent to a single I/O point. The total I/O point count must remain within the Trusted IEC 61131 TOOLSET constraints.
Analogue Accuracy	32 bit integer or real.

Appendices

There are two types of Peer to Peer network, Basic and Enhanced. The Enhanced Peer to Peer is described in the main part of this document, and describes the operation from TUV release 3.5. The Basic Peer to Peer network is described in these appendices.

Product Overview (Basic)

Trusted Peer to Peer Communications is provided by the Trusted Communications Interface module (T8150/T8151/T8151B) for the interchange of safety and non-safety information between Trusted Controllers. Up to four Trusted Communications Interface modules may be fitted in each Trusted Controller.

The Peer to Peer structure employs Ethernet and User Datagram Protocol (UDP) as its underlying transport mechanism. The Peer to Peer architecture is a multi-drop bus structure.

It is a simplex peer network between up to 10 Trusted controllers. Two (or more) networks can be configured to carry redundant data between the controllers. The application program has to be configured to put the data onto the networks and to handle the received redundant data together with the data voting.

Features:

- Supports up to ten Trusted Controllers per Peer to Peer Network
- Up to four Peer to Peer Networks per Trusted Controller
- Safety related data interchange support (TÜV certified for SIL 3 applications)

A.1. Basic Peer to Peer Network

Communications interaction via the Peer to Peer network is on a master/slave basis with a single master per network. The Trusted Communications Interface module may be configured as master, or slave but may not be operated in both roles simultaneously. Each network is capable of supporting up to a maximum of nine slaves.

Single or dual (redundant) networks are supported. Example configurations are shown in Figure 15 and Figure 16 below. Four logical networks are the maximum number of Peer to Peer networks that may be supported by a single Trusted Controller. Where a redundant network is employed, no voting of information takes place and the most recent information received is used. Data integrity is checked via a CRC of the packet data sent between systems.

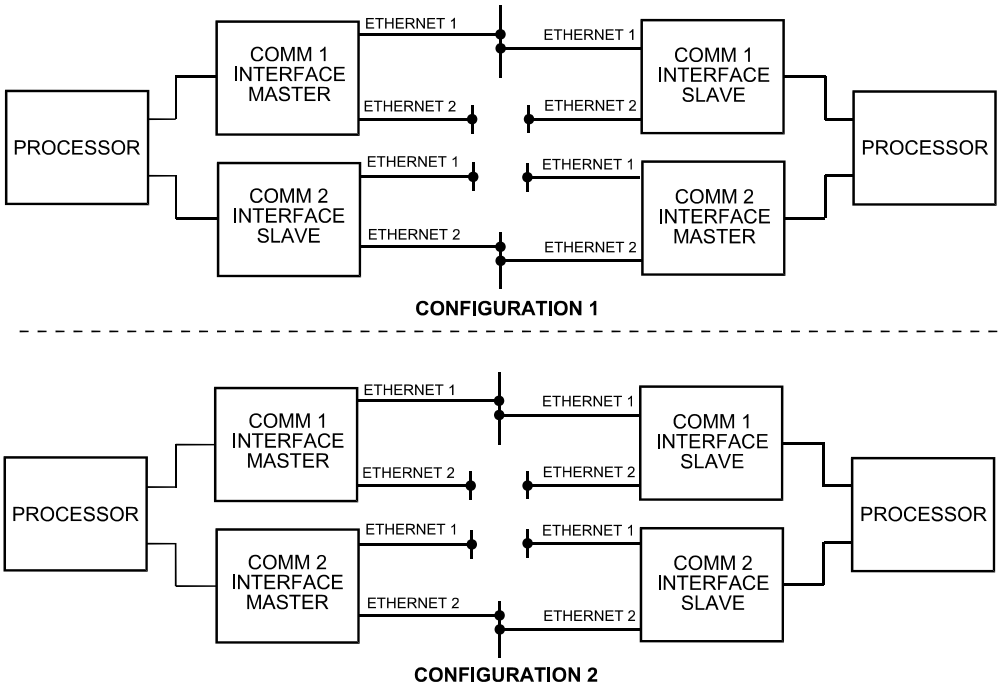

Figure 15 Dual Communications Module Networks

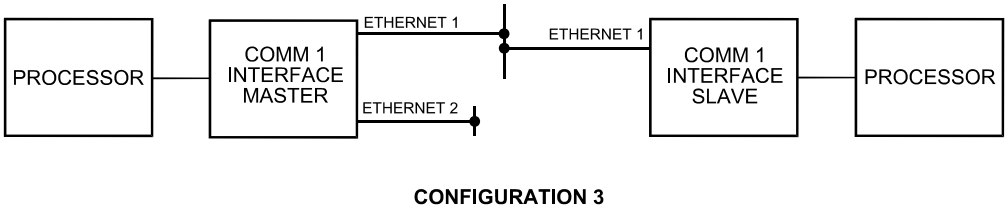

Figure 16 Single Communications Module Networks

Where only a single Trusted Communications Interface module is used in a Trusted Controller, as shown in Figure 16, the maximum number of slaves that may be supported is nine.

When two or more Trusted Communications Interface modules are installed within a controller, they may be configured to operate on independent Peer to Peer Communications Networks. Each of these networks may support up to ten Controllers, with data routed between the Peer to Peer Networks by the application program running in the Trusted TMR Processor. This approach is recommended where additional isolation is required between inter-operating controllers for safety or maintainability purposes.

Examples of configurations not supported by Trusted Controllers are shown in Figure 17 below. The first example shows the Trusted Communications Interface module operating in both master and slave roles simultaneously. The second shows a Trusted Communications Interface module being used as a 'Bridge' between two separate networks.

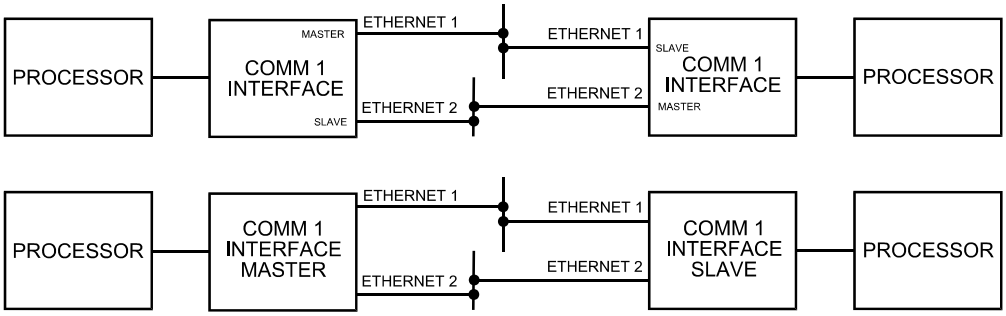

Figure 17 Unsupported Configurations

The information to be transferred between Trusted Systems is defined within the application programs as input and output boards in the standard form. The boards provide 64 Boolean points, 64 analogue points and relevant status information. Boolean and analogue boards are combined as 'complex equipment' within the IEC 61131 TOOLSET. The identity of the destination system for outgoing information and the source of incoming information is defined by the board parameters. Where information is to be transferred to more than one system, multiple boards must be used.

Each Peer to Peer point (both Boolean and analogue) is equivalent to an external I/O point. All Peer to Peer points and boards must therefore be included in the total number of external points and boards. The I/O point count and boards must remain within the constraints of the IEC 61131 TOOLSET.

Note: The Trusted Communications Interface module will also support external communications using Modbus over serial and Ethernet links. Using the module to support both external Modbus communications and Peer to Peer may slow the performance of Peer to Peer Communications.

A.1.1. Theory of Operation

Peer to Peer Communications interaction is Master/Slave which provides deterministic behavior. Each Peer to Peer Communications network requires one Trusted System to act as the Master for the network and up to nine Trusted Systems participating as Slaves.

Peer to Peer Communications is configured by defining Peer to Peer Master/Slave and I/O boards within the application program in the normal way. A control variable is provided on the Peer to Peer

Master and Slave boards to give the application program control over the starting and stopping of the communications cycle.

A.1.1.1. Communications Cycle

At start of the communications cycle, the Peer to Peer Master issues an enquiry command to the first Slave. If the Master receives a response from the Slave, it registers that Slave as being active and then repeats the process with the next Slave. This sequence continues until all the Slaves have been polled.

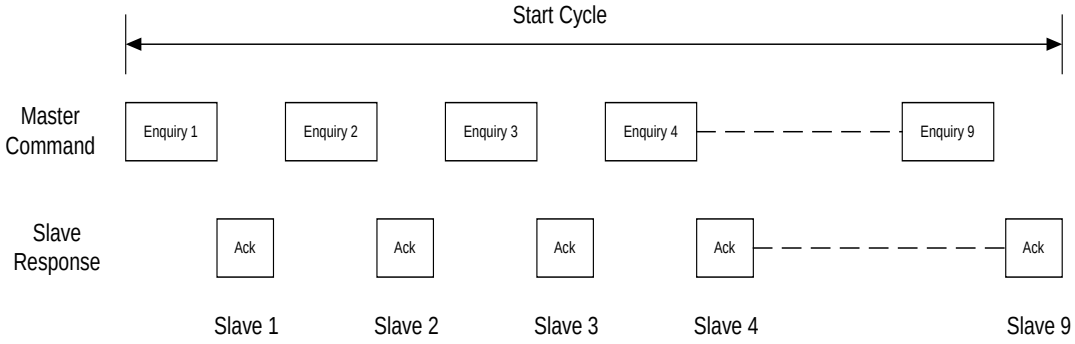

Figure 18 Peer Communications Start Cycle

The Master then sends a transmit data command to the first Slave to instruct it to send its output data to its configured Peers. When the Slave has completed this, it sends a transmit data complete response to the Master and the Master repeats the process with the next Slave. Once all the Slaves have been polled, the Master transmits its output data. The transmit data cycle starts again with the first Slave. The Master repeats this communications cycle continuously.

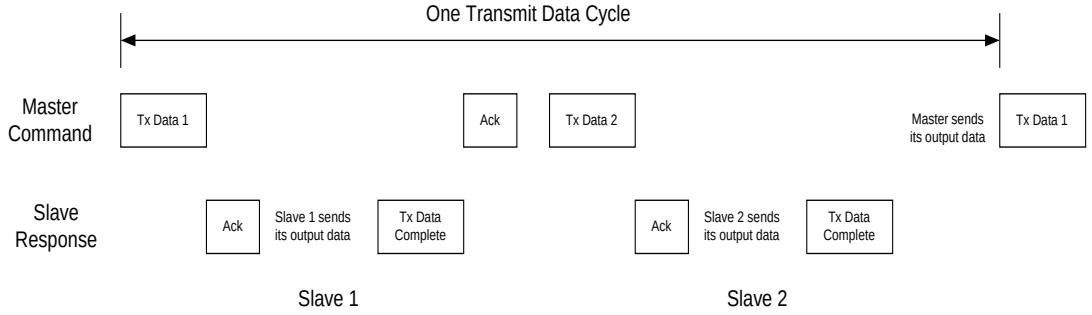

Figure 19 Peer Communications Transmit Data Cycle

All commands issued by a Master or a Slave are acknowledged immediately by the receiving Peer system. If the Master fails to receive a response from a Slave, it registers that Slave as inactive and on the next poll of the Slave, issues an enquiry command again. The Master will continue to send an enquiry command on each poll of the inactive Slave until it receives a response. When the Master receives a response to the enquiry, it will resume sending the transmit data command to the Slave as described above.

The length of time the system waits for a response from a Peer is configurable via the response time-out parameter on the Master or Slave board. Also, the length of time the Master will wait for a Slave to complete sending its output data can also be adjusted via the transmit data time-out parameter on the Master board.

A.1.1.2. Input Data

When the system receives Peer to Peer input data, it is validated before it is passed on to the application program for use.

The system monitors the refreshing of input data. If fresh input data is received within the time-out period, the input refresh status bit on the input board is set to true. If fresh input data is not received, this status bit is set to false.

The length of time the system waits for fresh input data is configurable via the refresh time-out parameter on the input boards.

A.1.1.3. Output Data

When Peer to Peer output data is changed by the application program, it is sent to the Trusted TMR Communications Interface module ready for transmission over the Peer to Peer network. Only the latest output data for a particular Peer system is stored on the Trusted TMR Communications Interface module. If fresh output data is received before the previous values have been transmitted, they will be overwritten by the new data.

If the application program has not changed output data, within a time-out period, the current values are sent to the Trusted TMR Communications Interface module. This ensures the corresponding input board on the Peer system expecting the data is kept refreshed.

The length of time the system waits for fresh output data from the application program is configurable via the refresh time-out parameter on the Peer to Peer output boards.

A.2. Programming Information

The Trusted Communications Interface modules are selected and assigned to Peer to Peer Communications using the I/O Connection Editor at the Engineering Workstation (EWS) as described in PD-T8082. It should be noted that the (OEM) parameters set up on all board / rack definitions cannot be changed online. General information relating to configuring the modules is detailed as follows:

A.2.1. Peer to Peer Master

Figure 20 shows the display associated with the Trusted Communications Interface module selected as Peer to Peer master.

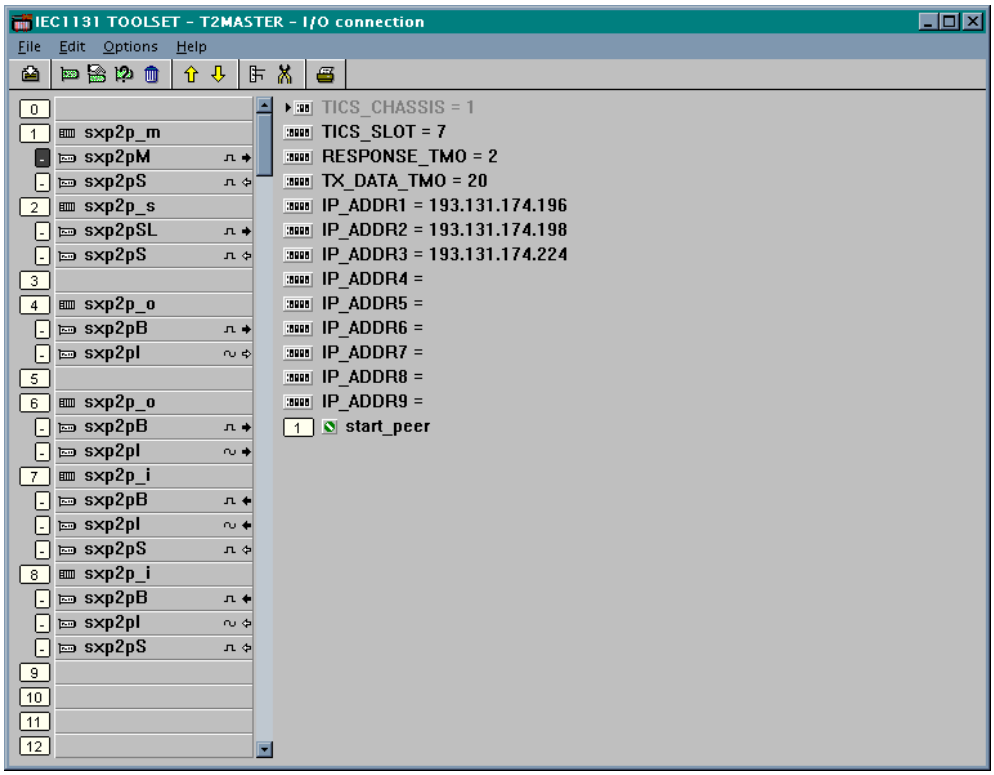

Figure 20 Peer to Peer Master Display

The user must enter data as detailed below:

1. TICS_CHASSIS – this will always be '1'.
2. TICS_SLOT – this must be assigned the slot number of the associated Trusted Communications Interface module.
3. RESPONSE_TMO – this is the time, in seconds, that the system will wait for a response from a peer. Values of 1 to 30 seconds are valid.
4. TX_DATA_TMO – this is the time, in seconds, that the master will wait for a peer to complete sending its data. Values of 1 to 60 seconds are valid.
5. IP_ADDR1 to IP_ADDR9 – each Peer to Peer master can communicate with up to a maximum of nine slaves on a single network. Each slave must have a unique IP (Internet Protocol) address assigned to it.
6. start_peer – Peer to Peer Communications is started/stopped by assigning a variable name to this field in the normal way.

Figure 21 shows a display of the status board associated with the Trusted Communications Interface module selected as Peer to Peer master.

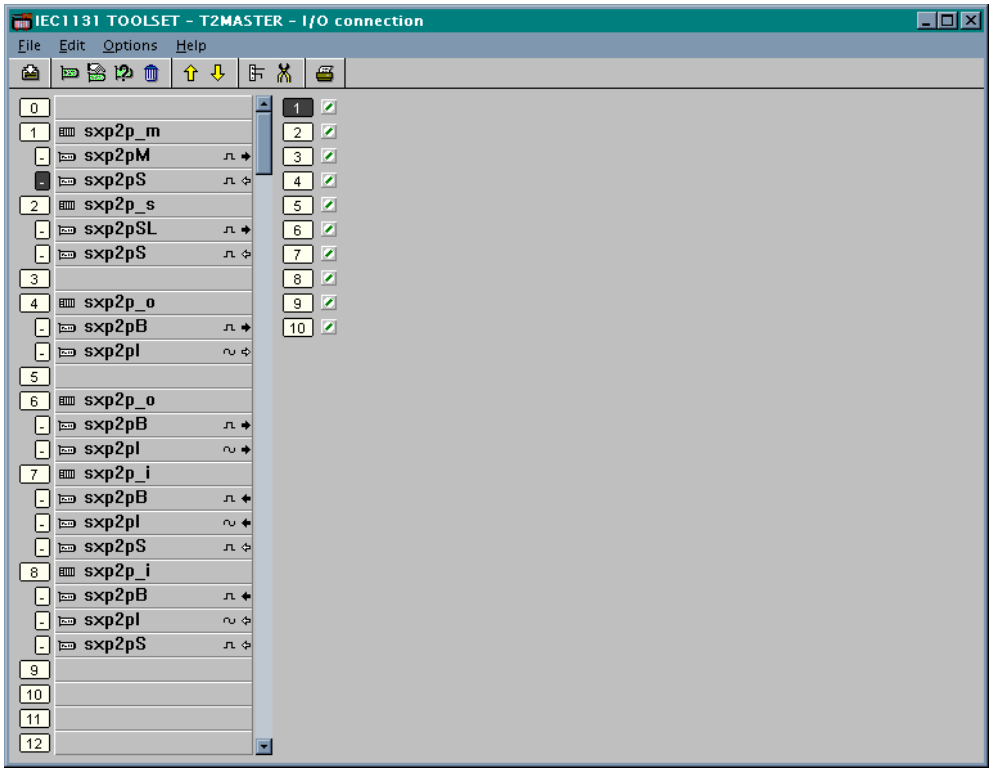

Figure 21 Peer to Peer Master Status Board Display

The status board contains 10 status bits which indicate the status of the peers on the network. Each bit is set to TRUE when active and FALSE when inactive.

Point 1 represents the status of the master.

Points 2 to 10 represents the status or the slaves. These are displayed in the same order that they have been entered in the “Peer to Peer Master Display” shown in Figure 20.

E.G.

Refer to Figure 20.

Point 2 is the status of the Slave configured as IP_ADDR1,

Point 3 is the status of the Slave configured as IP_ADDR2,

Point 4 is the status of the Slave configured as IP_ADDR3,

Point 5 is the status of the Slave configured as IP_ADDR4,

Point 6 is the status of the Slave configured as IP_ADDR5,

Point 7 is the status of the Slave configured as IP_ADDR6,

Point 8 is the status of the Slave configured as IP_ADDR7,

Point 9 is the status of the Slave configured as IP_ADDR8,

Point 10 is the status of the slave configured as IP_ADDR9

A.2.2. Peer to Peer Slave

Figure 22 shows the display associated with the Trusted Communications Interface module selected as Peer to Peer slave.

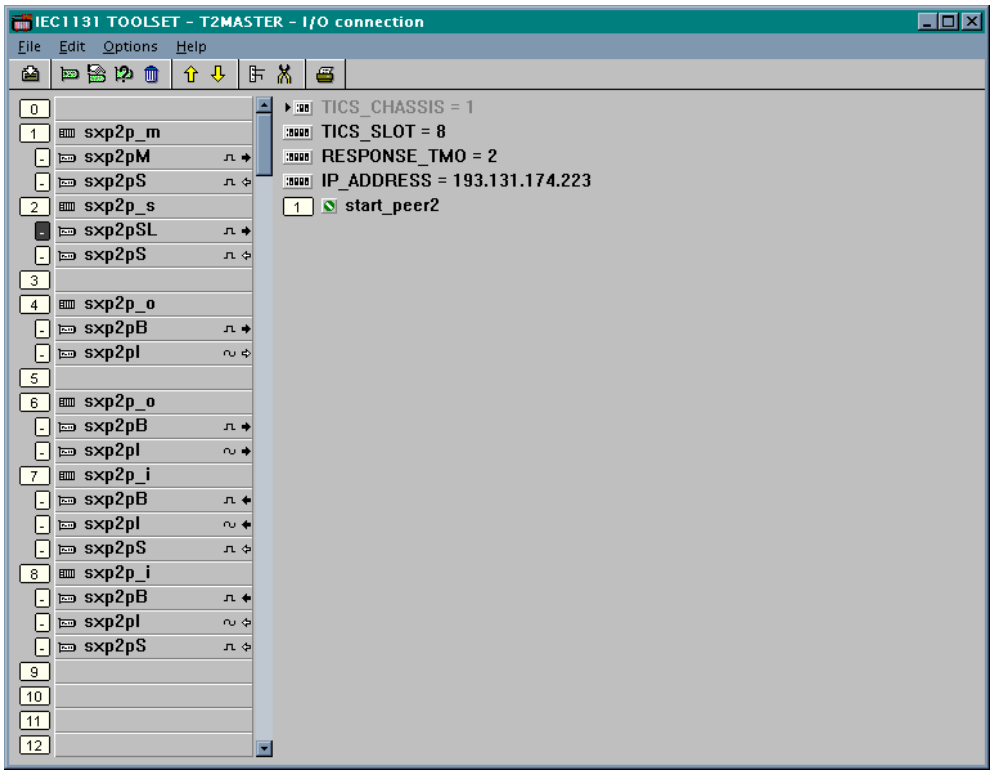

Figure 22 Peer to Peer Slave Display

The user must enter data as detailed below:

1. TICS_CHASSIS – this will always be '1'.
2. TICS_SLOT – this must be assigned the slot number of the associated Trusted Communications Interface module.
3. RESPONSE_TMO – this is the time, in seconds, that the system will wait for a response from a peer. Values of 1 to 30 seconds are valid.
4. IP_ADDRESS – this will be the IP address of the Peer to Peer Communications network master.
5. start_peer – Peer to Peer Communications is started/stopped by assigning a variable name to this field in the normal way.

Figure 23 shows a display of the status board associated with the Trusted Communications Interface module selected as Peer to Peer slave.

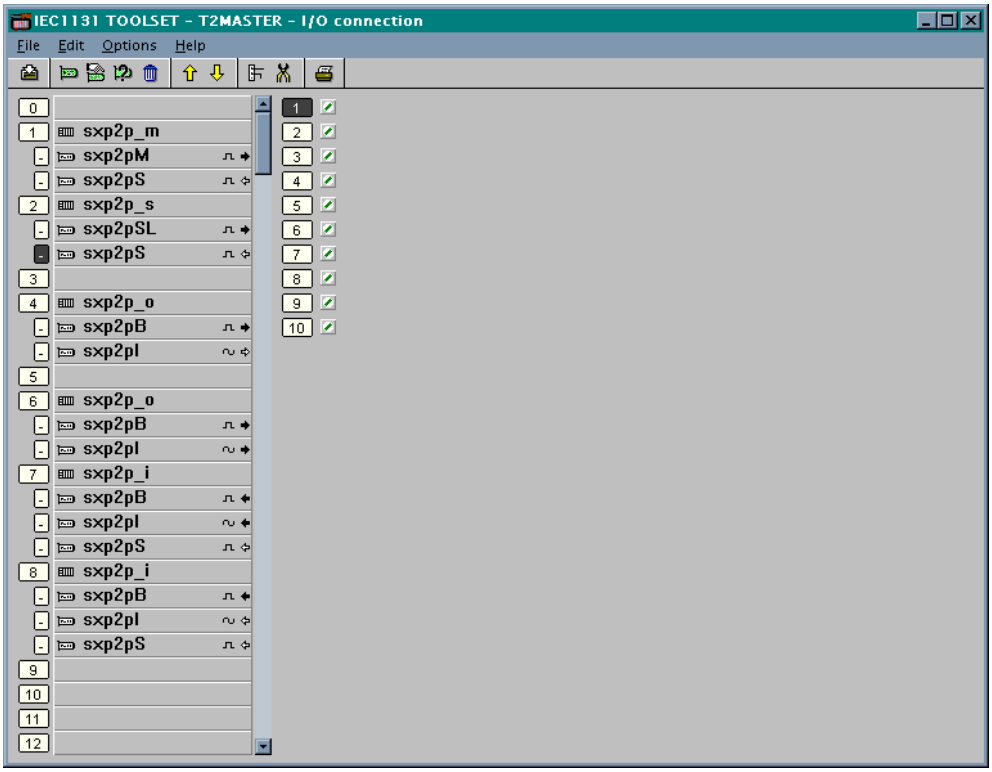

Figure 23 Peer to Peer Slave Status Board Display

The status board contains 10 status bits which indicate the status of the peer network

Point 1 represents the status of the slave, TRUE if active, otherwise FALSE.

Point 2 represents the status of the Master, TRUE if active, otherwise FALSE

Points 3 to 10 represent each of the remaining peers that this slave is communicating with and are displayed in ascending IP address order. Point 3 is the lowest IP address and point 10 is the highest IP address. Each is set to TRUE if active, otherwise FALSE.

Note that when the Master is not responding and Point 2 above is FALSE, then points 3 to 10 will then be invalid.

A.2.3. Peer to Peer Input Boards

Figure 24 shows the display associated with an IEC 61131 TOOLSET input board selected for incoming data to a Trusted Communications Interface module.

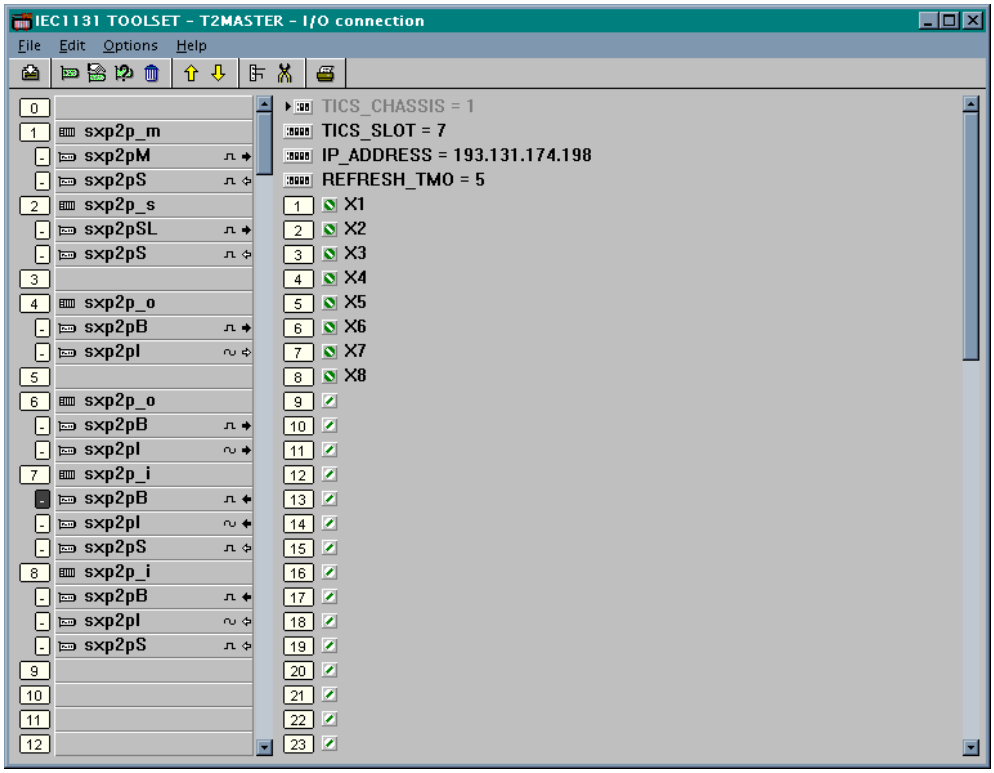

Figure 24 Peer to Peer Input Board Display

The user must enter data as detailed below:

1. TICS_CHASSIS – this will always be '1'.
2. TICS_SLOT – this must be assigned slot number of the associated Trusted Communications Interface module.
3. IP_ADDRESS – this will be the IP address of the source system.
4. REFRESH_TMO – this is the time, in seconds, that the system will wait for fresh input data from the peer network before setting the input refresh status bit to FALSE. Values of 1 to 60 seconds are valid.
5. The input identifiers for each of the inputs assigned to the input board, e.g. X1, X2, X3 etc. Each input board may have 64 Boolean and 64 analogue input points assigned. All inputs assigned to any given input board must originate from the same source. Separate input boards must be assigned if there is more than one source.

Note: Peer to Peer input boards must be allocated in the configuration after their associated Peer to Peer master or slave board

Figure 25 shows a display of the refresh status of the associated input board.

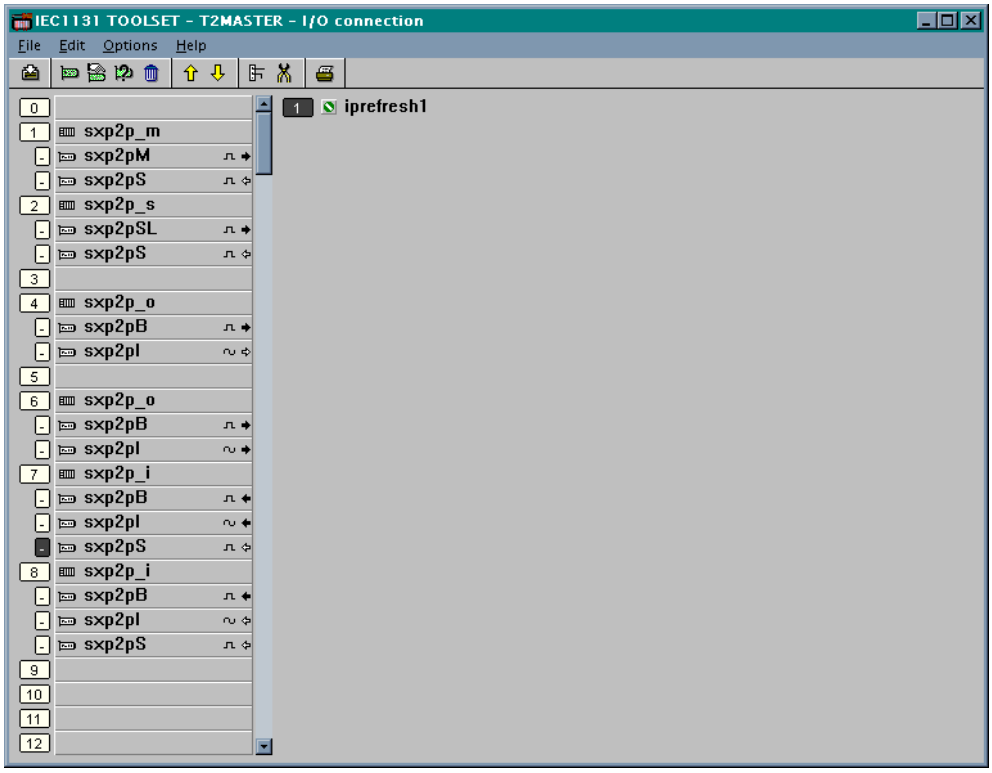

Figure 25 Input Board Refresh Display

The input refresh status is set TRUE if fresh input data is received, otherwise it is set FALSE.

A.2.4. Peer to Peer Output Boards

Figure 26 shows the display associated with an IEC 61131 TOOLSET output board selected for outgoing data to a Trusted Communications Interface module.

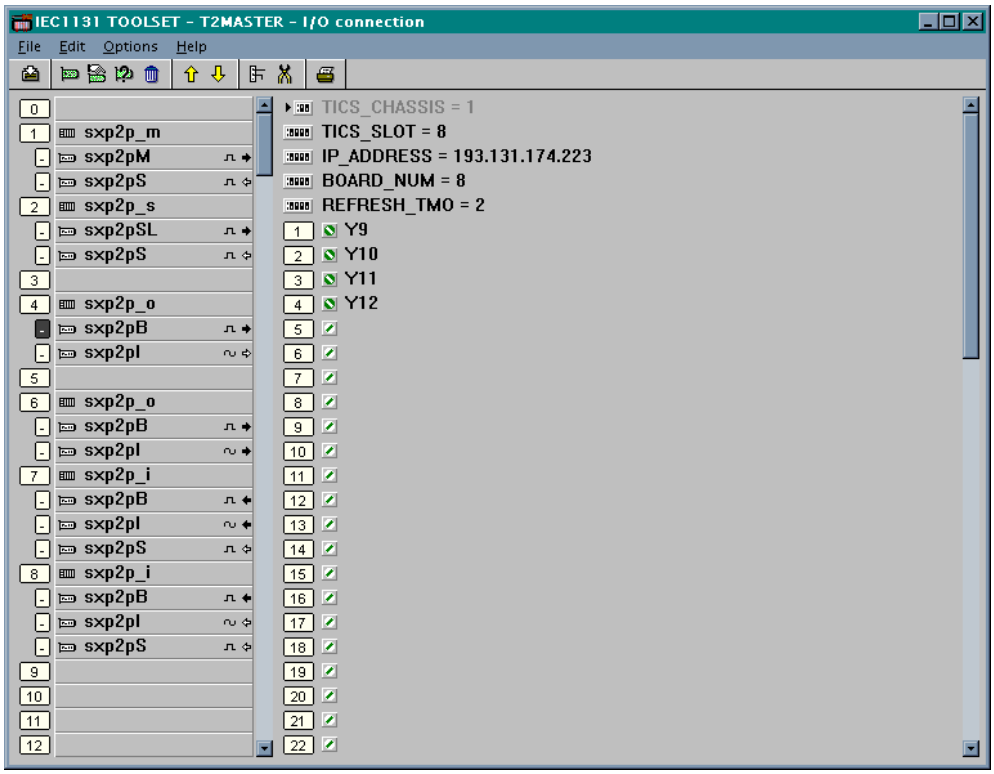

Figure 26 Peer to Peer Output Board Display

The user must enter data as detailed below:

1. TICS_CHASSIS – this will always be '1'.
2. TICS_SLOT – this must be assigned the slot number of the associated Trusted Communications Interface module.
3. IP_ADDRESS – this will be IP address of the destination system.
4. BOARD_NUM – the number of the input board at the destination system to which the outgoing data is addressed.
5. REFRESH_TMO this is the time, in seconds, that the system will wait for fresh output data from the application before sending the current output data to the peer system.
6. The output identifiers for each of the outputs assigned to the output board, e.g. Y1, Y2, Y3 etc. Each output board may have up to 64 Boolean and analogue points assigned. All outputs assigned to any given output board must be destined for the same destination system. Separate output boards must be assigned if there is more than one destination.

Note: Peer to Peer output boards must be allocated in the configuration after their associated Peer to Peer master or slave board.

A.2.5. Peer to Peer Analogue Data Transmission

Analogue data sent between an sxp2p_o board and an sxp2p_i board is transferred as a 16 bit unsigned integer. However, the application stores integers as 32 bit with sign. On transferring the data, only the lower 16 bits is sent across the peer to peer network. This means that values between 0 and 65535 will be transferred without change, but negative values will be shifted to above 32767. Values above 65535 will be truncated. It is essential to be aware of the truncation when choosing data ranges. If numbers between -32768 and +32767 are required, then the application receiving the data must subtract 65536 from any number greater than 32767.

A.2.6. Timeout Parameters and Data Integrity

The Peer to Peer I/O board definitions for timeout parameters should be set appropriate to the peer system as described in Table 23 below. Safety related input signals should then be gated with the Input Refresh flag, which is the single digital input on the sxp2pS board of the sxp2p_I peer to peer input equipment definition. The Refresh flag is set true until data has remained stale for longer than the refresh timeout REFRESH_TMO on the sxp2p_I equipment definition.

Integer seconds are entered as the number of seconds, e.g. 30 = 30 seconds.

Millisecond times may be entered by adding 32768 to the required milliseconds, e.g. 32 ms is entered as 32768+32 = 32800. Numbers below 32768 are interpreted as units of seconds.

The timing settings are limited by the recommendation of 32 ms for master Response_tmo, upon which the other timeouts depend. The maximum recommended setting of the Input Refresh_tmo is 60 seconds.

Notes:

- Entry of millisecond times is only recognised on Trusted release 3.3 or later (MP build 34 and CI build 19). Before these builds, the number is always interpreted as seconds.
- The requirement for the correction factor of 500 ms in the calculation of *sxp2p_O Refresh_tmo* in Table 23 below is only required for CI modules used in Trusted release 3.4.2 (CI build 105) or earlier.

The status rack in peer master and slave controller board definitions reflects the instantaneous status of communication between peer nodes. It is entirely possible for the controller status rack to indicate a temporary loss of communication to a peer node without impacting on the integrity of peer input board data received from that peer. It is therefore recommended that assessment of peer input board data integrity be based solely upon the associated input board refresh status and not upon any related controller status.

Board sxp2p_s, rack sxp2pS and board sxp2p_m, rack sxp2pS: These signals are the status bits for a peer node and will change state, as seen by a master controller, within a few seconds of removing or restoring a slave's Ethernet connection.

Board sxp2p_I, rack sxp2pS (Refresh_tmo): This is the P2P input signal refresh state and will remain true until the input refresh time has expired, i.e. input data will tolerate interruptions in communication between peers, independent of the peer status reported by sxp2pS.

It is recommended that a delay of 11 seconds (10 seconds timeout + 1 second tolerance) be added to any existing peer input refresh timeout to ensure continued operation of a redundant channel in the presence of a single CI fault. This only applies to systems containing MP builds prior to release 3.5 and revision B CI module hardware where the IMB is not isolated following watchdog failure.

Equipment	Parameters	Description
sxp2p_m		Master Response Timeout
Master	Response_tmo	32 ms is recommended on a local network.
sxp2p_m		Transmit data timeout
Master	Tx_data_tmo	Set to Master Response Timeout multiplied by the maximum number of sxp2p_O output boards in any single controller.
sxp2p_s		Slave Response Timeout
Slave	Response_tmo	Set the same as Master Response Timeout above.
sxp2p_I		Input Refresh Timeout
Input	Refresh_tmo	Set to the longest acceptable time before stale data should cause a trip.
sxp2p_O		Output Refresh Timeout
Output	Refresh_tmo	$\frac{\text{(Input Refresh Timeout) – ((Npeer x Transmit Data Timeout) + TSsource + TSdest + 500 ms)}}{2}$

Table 23 Timeout Parameters

Where Npeer = number of peer to peer controllers

TSsource = Maximum application scan time of controller with output board

TSdest = Maximum application scan time of controller with input board

Note: If the Output Refresh Timeout calculates as a negative number, then the Input Refresh Timeout is unrealistically low for the communications load.

A.2.7. Peer Network Specification

No. of Peer Networks per System	≤ 4
Target Inter-application Response	
Single point change	nx15 ms + 2x(source + destination application scan)
All points change	nx15 ms(per 1000 digital points per node) + nx15 ms(per 60 analogue points per node) + 2x(source + destination application scan) n=no. of nodes/systems on the network
No. of Nodes per Network	$2 \leq n \leq 10$
Points per Node/System	Peer Communication points are to be included in the total number of external points. Each point is equivalent to a single I/O point. The total I/O point count must remain within the Trusted IEC 61131 TOOLSET constraints.
Analogue Accuracy	Analogue values are transferred as 16 bit unsigned integers (0 to 65535). If signed values are to be transferred the receiving controller application must monitor the Peer to Peer value at the receiving end and if it is above 32767 then subtract 65536 from the incoming value. This will provide a range of -32768 to +32767.

Table 24 Peer Network Specification