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.

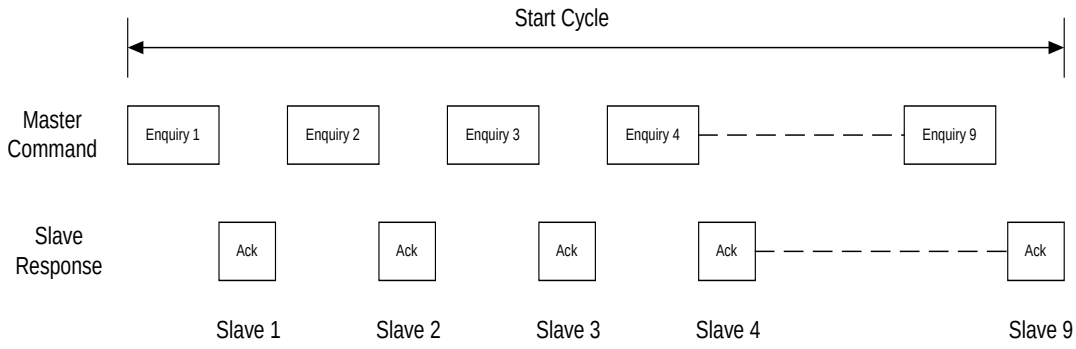

Figure 1 Peer Communications Start Cycle

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.

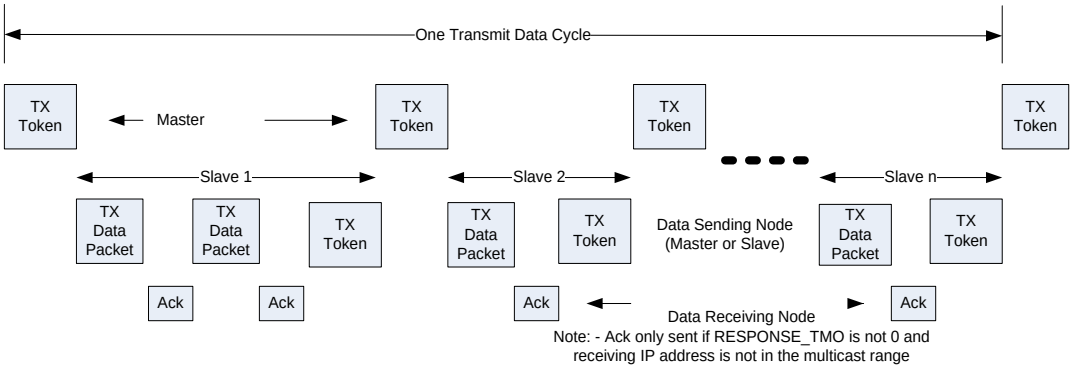

Figure 2 Peer Communications Transmit Data Cycle

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.

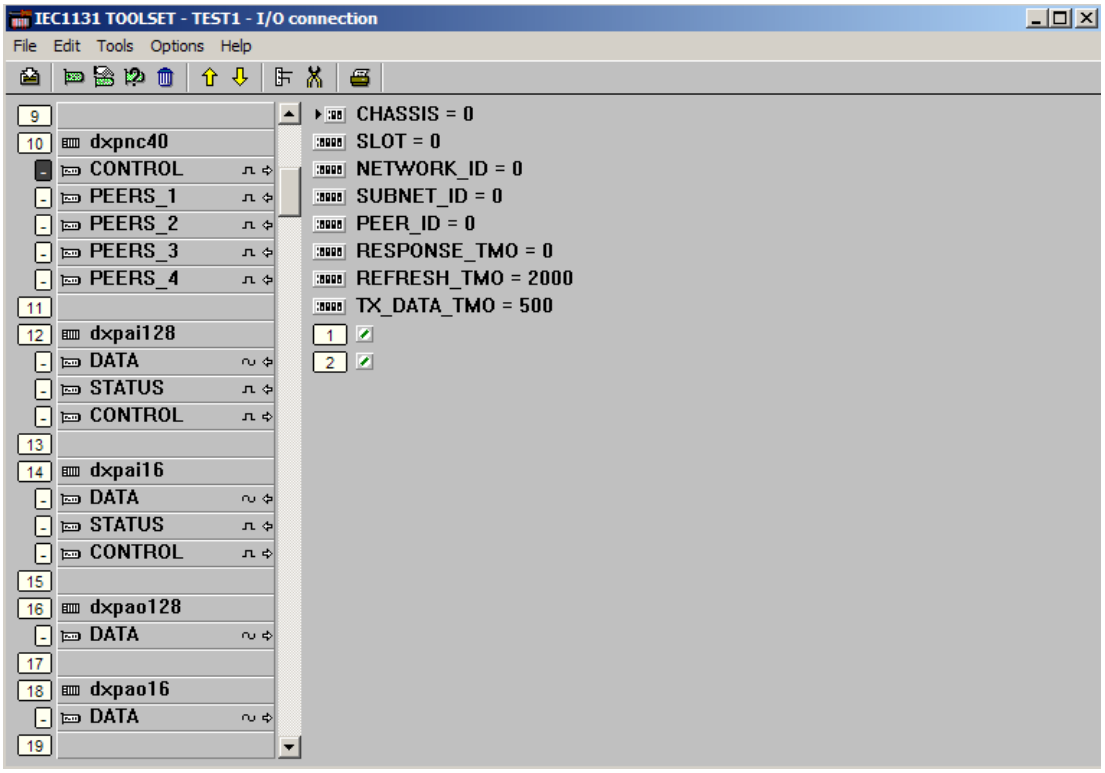

Figure 3 Peer Subnet Control board CONTROL rack

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.

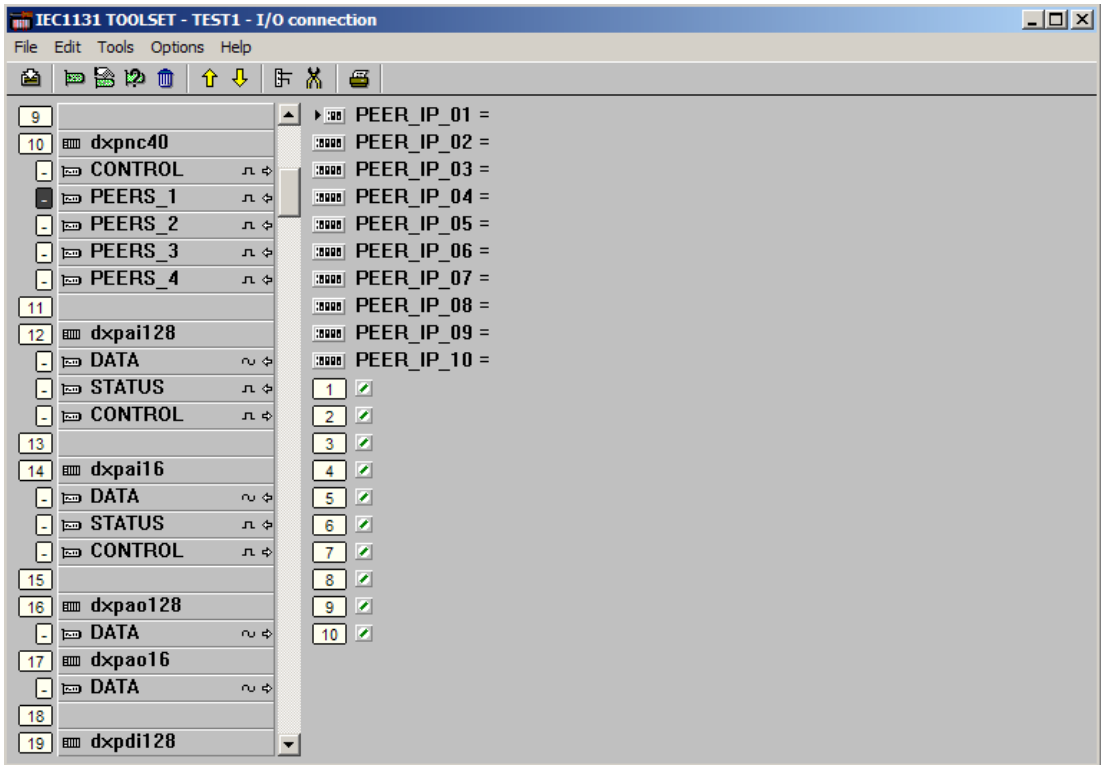

Figure 4 Peer Subnet Control board PEERS rack

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.

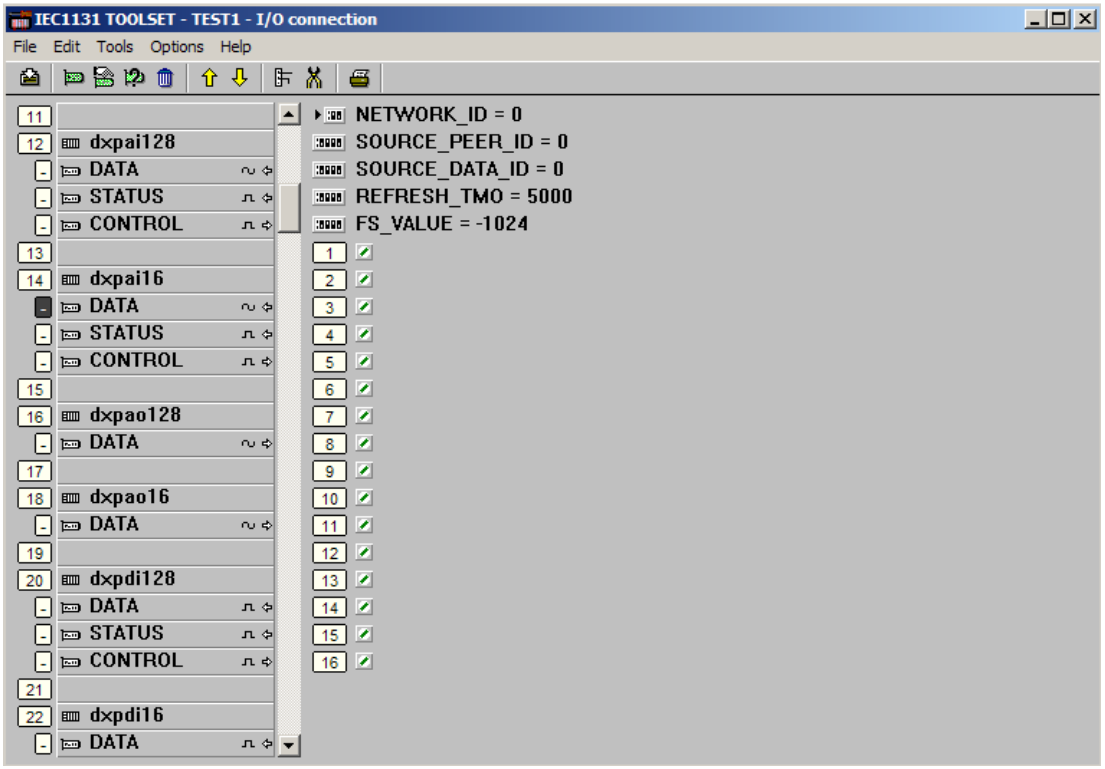

Figure 5 Peer to Peer Input Board Display

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.

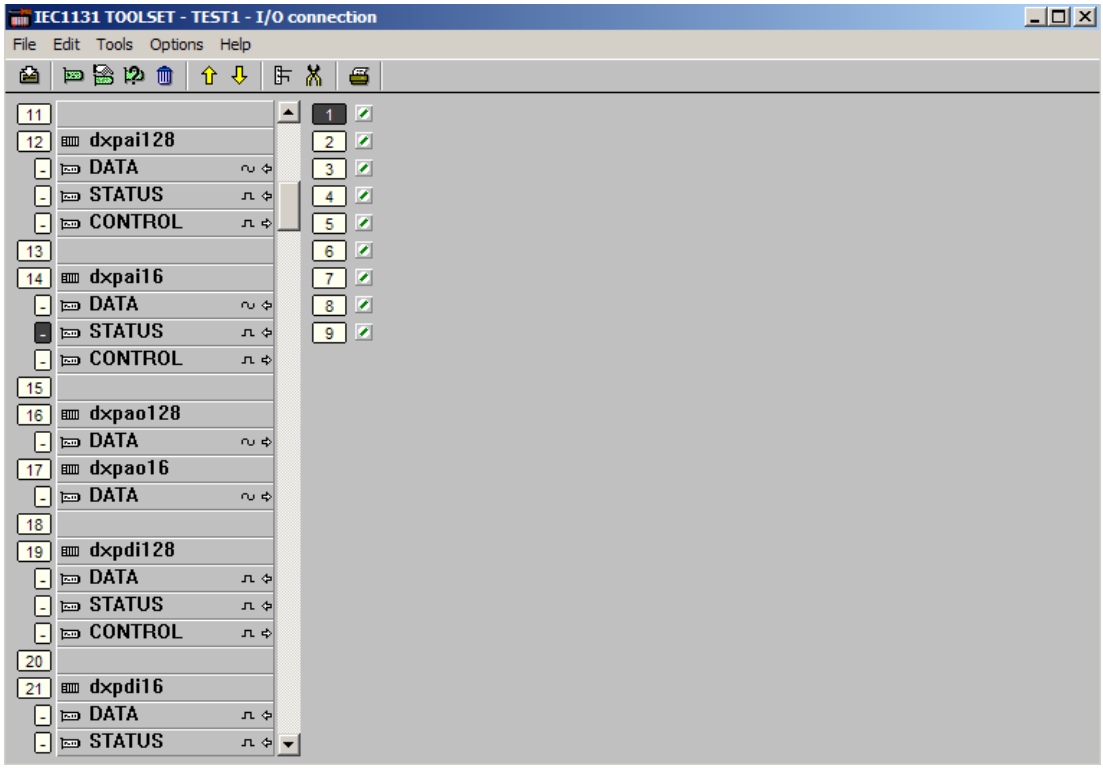

Figure 6 Input Board Status Display

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.

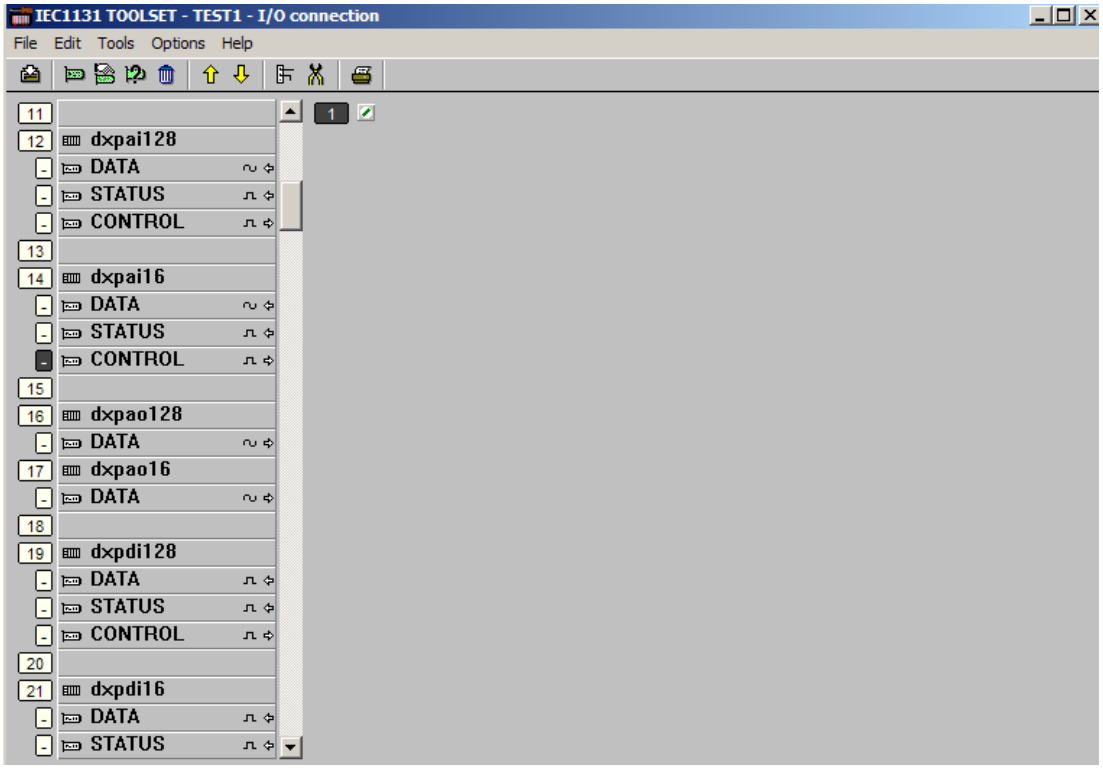

Figure 7 Input Board Control Display

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.

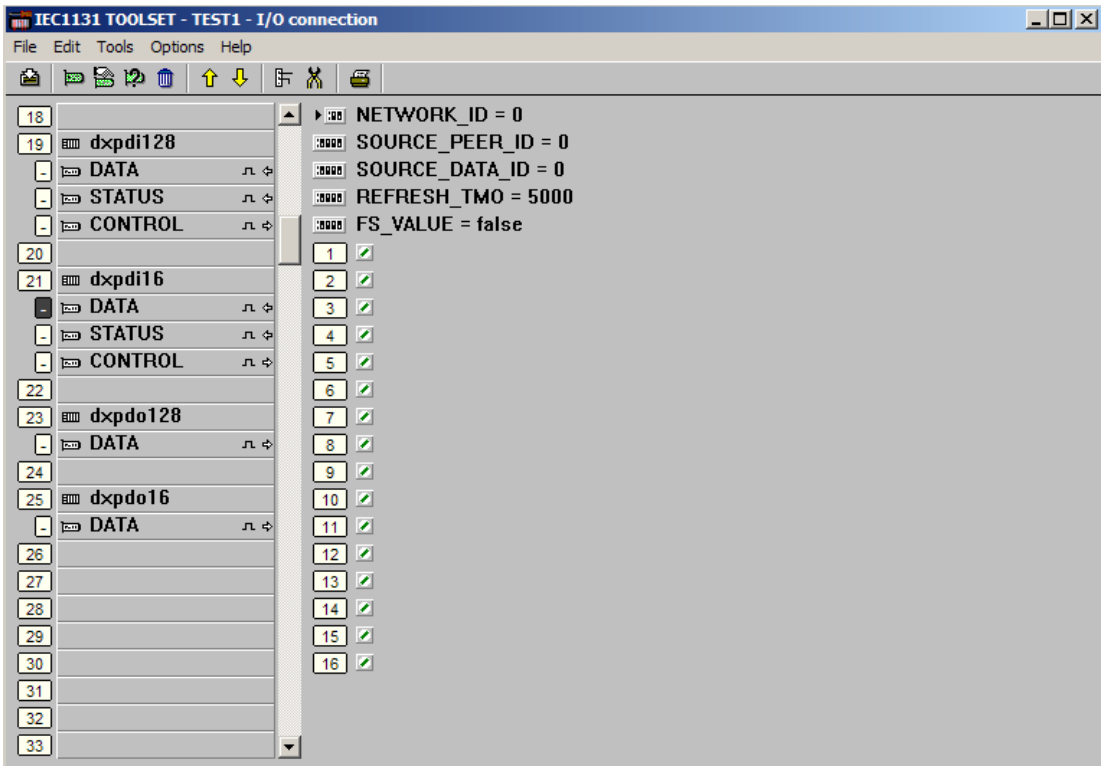

Figure 8 Peer to Peer Input Data Rack Display

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.

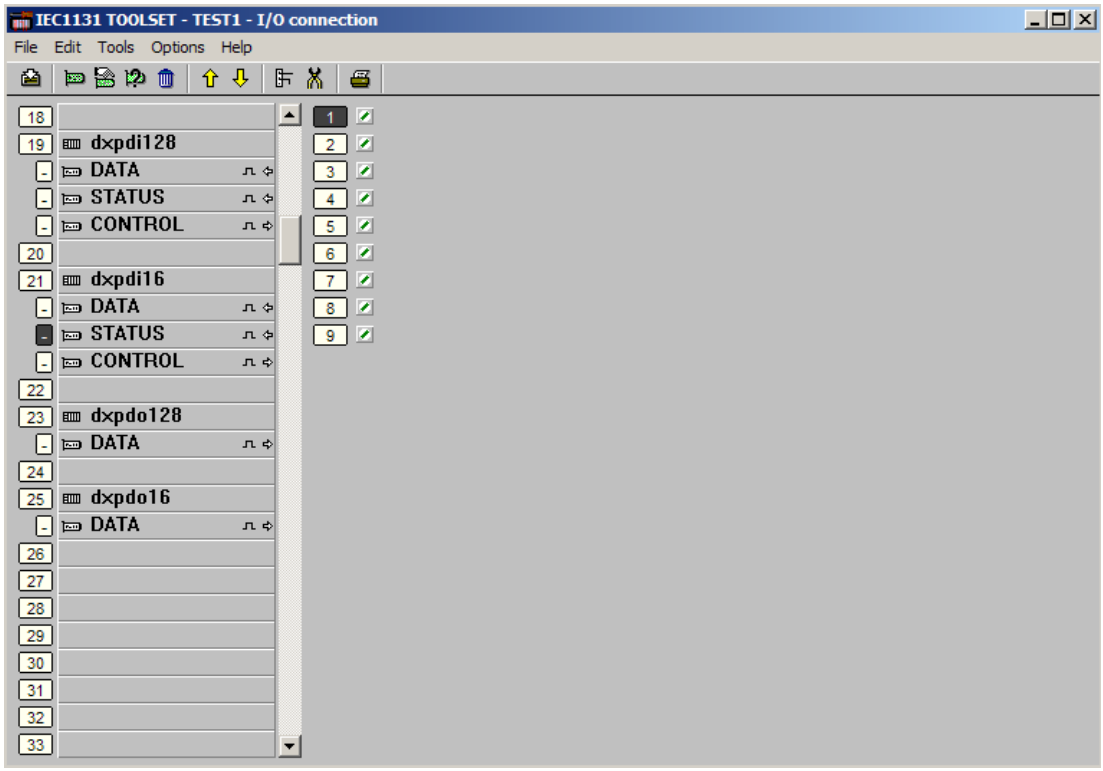

Figure 9 Input Board Status Display

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.

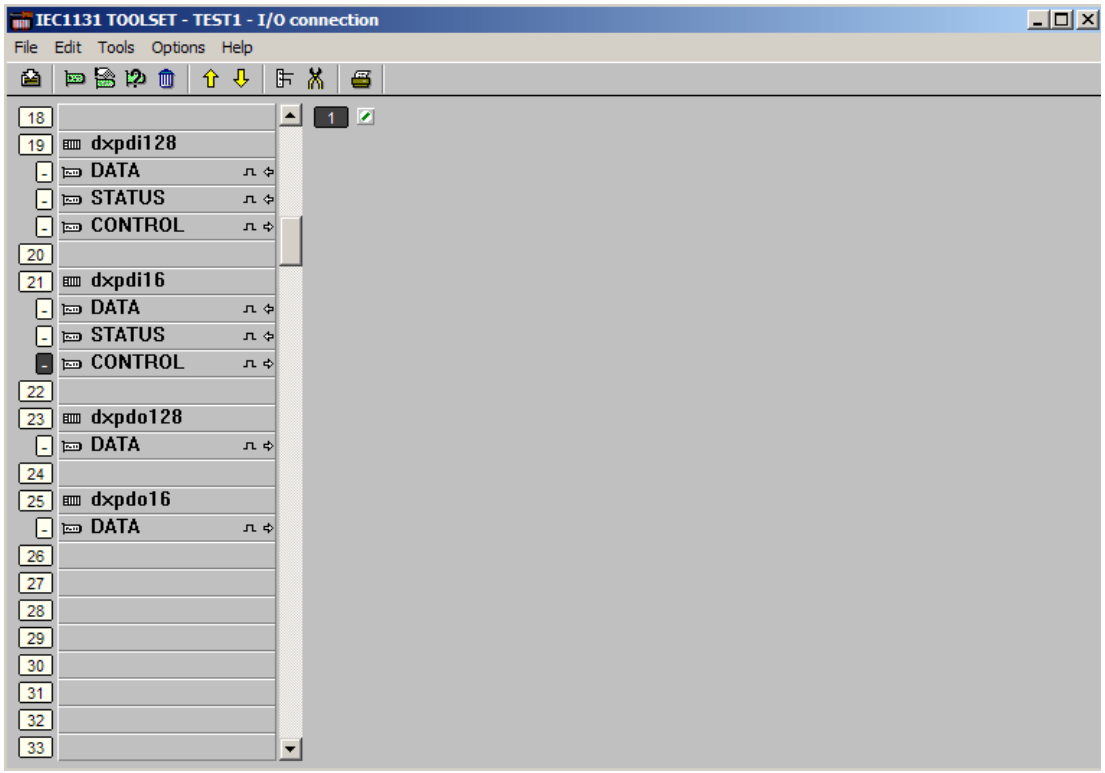

Figure 10 Input Board Control Display

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.

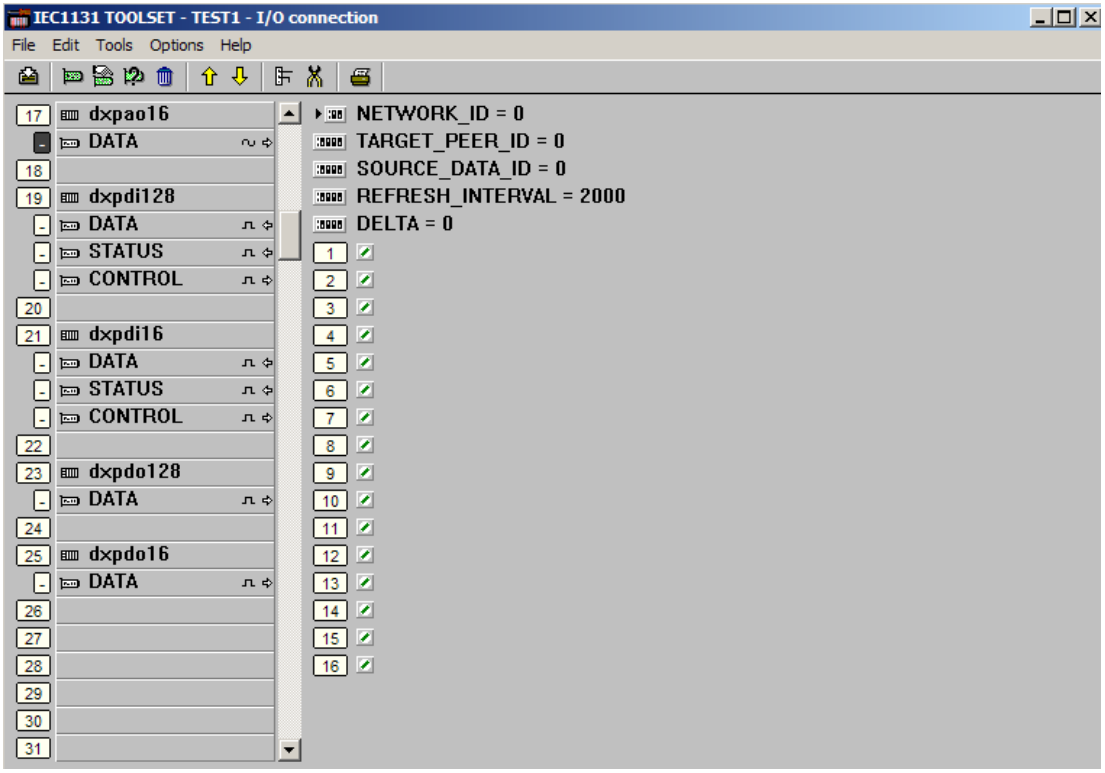

Figure 11 Peer to Peer Analogue Output Board Display

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.