

XL4 Plus DF1 Protocol

Introduction

The XL4 Plus RTU firmware implements the DF1 protocol for communications to PLC devices. This application note provides supplementary information for users wanting to configure communications from a PLC to the RTU using the QTech Workbench software utility. Additional notes are supplied regarding the older implementation of DF1 on a Q03/Q22 RTU, and the considerations required when upgrading from these RTUS to an XL4 Plus.

General

QTech Workbench uses the terminology of master and slave DF1 operations. This does not strictly align to DF1 nomenclature the following table shows the relationship:

RTU configuration in QTech Workbench	DF1 Meaning
DF1 Master enabled	RTU configured in Full duplex mode as a command Initiator only (It is not a command executor)
DF1 Slave Enabled	RTU configured in Full duplex mode as a command executor only (It is not a command initiator)
DF1 Slave and Master Enabled	Not allowed or supported

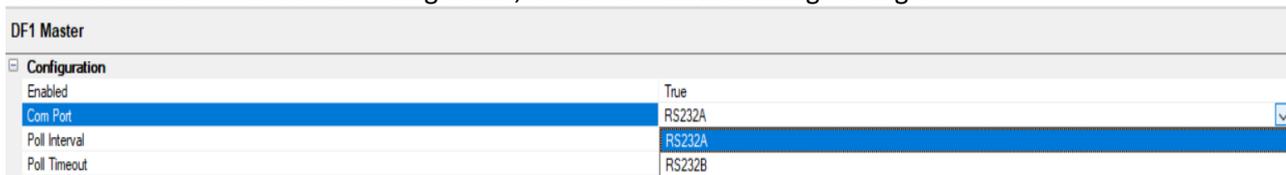
Important:

1. The RTU does not support half duplex operation as described by Allen Bradley.
2. When the RTU is transmitting a command, it will not listen or receive inbound communications simultaneously. PLC devices must transmit responses only after the end of the message transmission
3. If the RTU is configured as a slave, then it will simply respond to DF1 request that is sent to it by a DF1 command initiator. If the RTU is configured as a Master, then it will periodically send DF1 read and write requests to a connected DF1 slave (command executor) at a rate configured by the Poll Interval setting.

All configuration is done with QTech Workbench.

Communication Options

The RTU supports DF1 communications via either of its two RS232 serial ports. The DF1 source and destination address fields are configurable, as are the UART framing settings.



The screenshot shows the 'DF1 Master' configuration window in QTech Workbench. It has a 'Configuration' section with the following settings:

Property	Value
Enabled	True
Com Port	RS232A
Poll Interval	RS232A
Poll Timeout	RS232B

DF1 Slave	
Configuration	
Enabled	False
Com Port	RS232A
RTU Address	RS232A
PLC Address	RS232B

DF1 commands and PLC Types

The DF1 protocol specification outlines several commands used for reading and writing I/O. The XI4-Plus RTU supports the following three options.

- "Protected Logical Read/Write with three address fields" (CMD:0F, FNC:A2 and FNC:AA)
- "Word Range Read/Write" (CMD:0F, FNC:01 and FNC:00)
- "Unprotected Read/Write" (CMD:01 and CMD:08)

Refer to "Allen Bradley DF1 Protocol and Command Set Reference Manual, Publication 1770-6.5.16 - October 1996".

If the RTU is configured as the DF1 master, you can choose which set of commands it will send to the DF1 slave. If the RTU is the slave, then it will respond appropriately based on the type of command that was sent to it by the DF1 Master.

To specify which commands the RTU will use, select the appropriate PLC type in Workbench:

- SLC (also Micrologix) -> The RTU will use "Protected Logical Read/Write with three address fields" commands.
- PLC5 -> The RTU will use the "Word Range Read/Write" commands. There is also a secondary option to either use "Logical ASCII Addressing", or "Logical Binary Addressing".
- CIF -> The RTU will use the "Unprotected Read/Write" commands. By convention, these commands interact with the Common Interface File (N9).

DF1 Master	
Configuration	
Enabled	True
Com Port	RS232A
Poll Interval	200 ms
Poll Timeout	1000 ms
RTU Address	0
PLC Address	0
PLC Type	SLC
Com Port Settings	
Baud Rate	PLC5
Parity	SLC

Data Mapping

The way that the I/O in the RTU relates to the I/O in the PLC is controlled by the Data mapping configuration.

This was designed in order to accommodate the following arrangements:

- INTEGER type registers in the PLC can map to Digital as well as Analogue points in the RTU.
- BIT type registers in the PLC can map to Digital as well as Analogue points in the RTU.

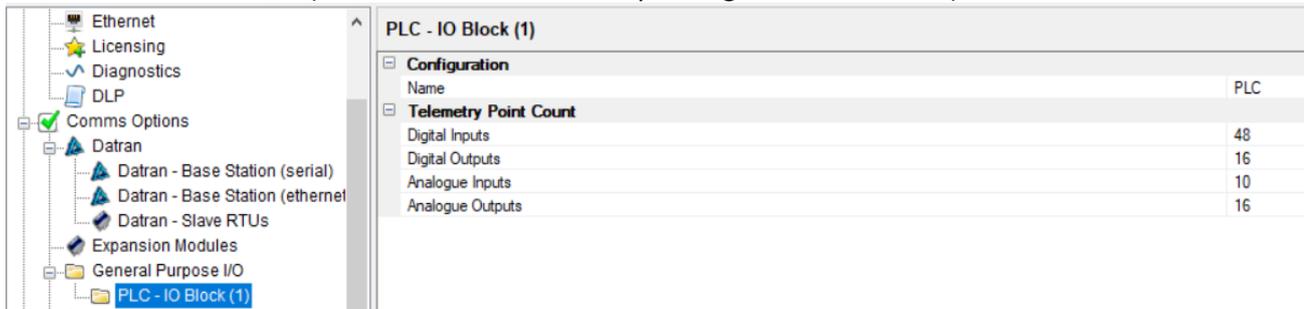
As a result of this feature, the following constraints must be observed:

- All I/O commands must align to WORD (16bit) boundaries in the RTU. This means that all PLC data that maps to Digital points in the RTU, must map to RTU points starting at multiples of 16 + 1 (eg RDO17). The RTUs Analogue points are inherently aligned to WORD addresses so this constraint does not apply to them.



- All I/O read and write commands must read or write a multiple of 16 bits (i.e. use an even number of bytes).

When configuring the RTUs DF1 interface, the I/O is not automatically allocated in the RTUs data table. It must be explicitly allocated as block of General Purpose I/O in the RTU if the PLC I/O is to map points other than the RTUs native I/O (or I/O that was allocated by adding slaves to the RTU).



Simply all this really means is that the two aspects of the configuration (commands used, and data block allocated), are independent from each other.

So, the RTU does not implicitly allocate I/O based on what commands have been specified, nor does it implicitly choose commands to send based on the I/O allocation.

From QTech Workbench Manual v2.7

DF1 Master

Data mappings can be made in the Slave or Master categories. Mappings made in the master will appear in the slave and vice versa. The main difference when defining a DF1 master is that the RTU will initiate requests to the DF1 slave (PLC).

DF1 Master	
Configuration	
Enabled	False
Com Port	RS232A
Poll Interval	200 ms
Poll Timeout	1000 ms
RTU Address	1
PLC Address	2
PLC Type	PLC5
PLC5 Addressing Mode	BINARY
Com Port Settings	
Baud Rate	19200
Parity	none
Data Bits	8
Stop Bits	1
Data Mappings	
[+] { RD117 - N1:1 } (2 bytes)	

When configuring a DF1 master for PLC-5 processors the addressing mode must also be specified. With logical addressing the address is specified for each level of the PLC-5 memory.

PLC-5 Addressing mode – specify either logical binary address mode or ASCII.

Logical binary addressing specifies a series of bytes to encode up to 4 levels of an address. E.g. 0x03,0x00,0x07,0x1E, equivalent to 3 level address: level 1 = 0 (data table), level 2 = 7 (file), level 3 = 30 (element or word).

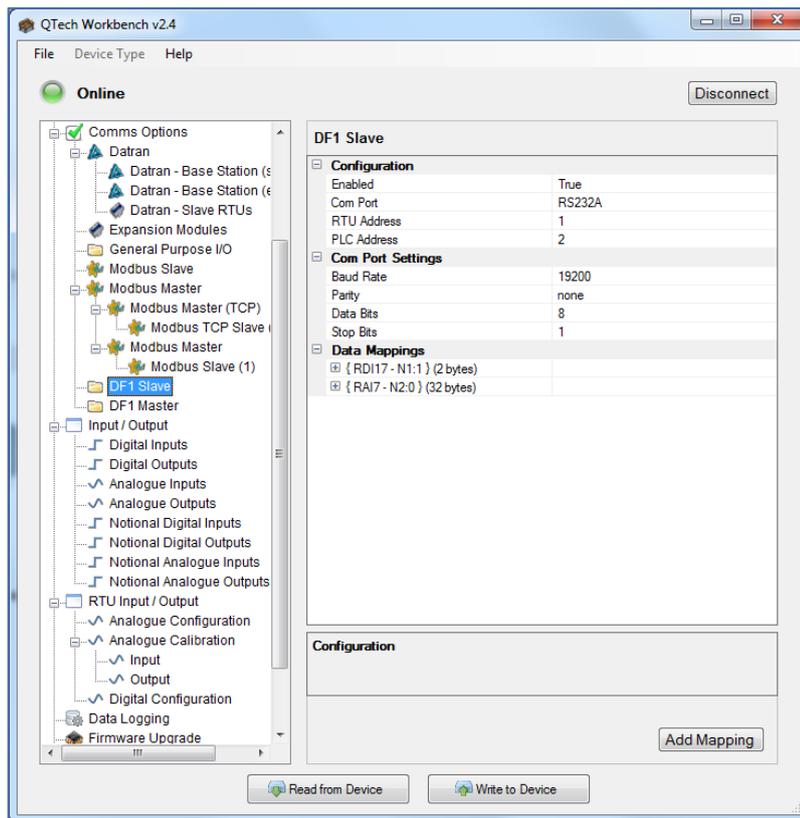
Logical ASCII addressing provides a user specified address in the same form as the PLC, this enables any device to communicate with the PLC without knowing the internal memory structure of the target device. E.g. “\$N7:30”.

DF1 Slave

The RTU support the DF1 protocol, used for connection to Programmable Logic Controller (PLC) devices. The RTU supports **Full duplex** DF1 protocol communications and if configured as a slave it will respond to requests from a DF1 Master (PLC).

An RTU can be configured as a DF1 master or DF1 slave but not both simultaneously.

Irrespective of whether the RTU is configured as a DF1 Master or Slave the protocol defines a method of mapping memory and I/O in the RTU to the memory map of the PLC, often referred to as a file with data elements.



Commands Supported

Three processor command types are supported: SLC, CIF and PLC-5. Each of these types one or more of the following DF1 commands:

1. Protected type logical **read** with three address fields
2. Protected type logical **write** with three address fields
3. Unprotected **Read**
4. Unprotected **Write**
5. Word Range **Read**
6. Word Range **Write**

Data transfer usually occurs as multiples of 16 bit words (2 bytes), irrespective of whether a mapping is defined bitwise or integer wise.

File types supported in with protected operations include:

1. Bit file type (85 hex)
2. Integer file type (89 hex)

Unprotected operations read data from a common interface file (CIF). The SLC 500 CIF is data file number 9. The Micrologix 1000 CIF is integer file 7.

Unprotected operations for PLC-5 processors read from the PLC-2 compatibility file. The size field is calculated from the data mapping and transfer occurs as a multiple of words (2 bytes), the address of a word should be even.

Configuration

Enabled – Setting the item to true will enable the DF1 slave service in the RTU.

Com Port – Selects the physical serial port on the RTU to use. Take care to ensure that this port is not already allocated to other services. Click the **comms option** category to review the current port allocation if necessary.

RTU address – The device (SRC) address of this RTU for DF1 comms (irrespective of RTU acting as a master or slave).

PLC address – The device destination (DST) address of the remote DF1 device, usually the source of DF1 comms to this RTU (irrespective of RTU acting as a master or slave).

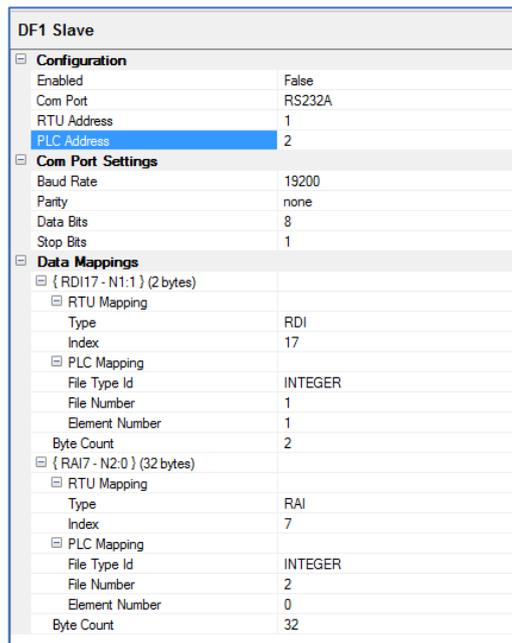
PLC type - refers to the supported PLC processor command types including:

- Common Interface File (CIF) for unprotected read/write operations
- SLC for SLC (and Micrologix 1000) processor types which support protected read/writes and unprotected read/writes
- PLC-5 which support word range read/writes

Com port Settings – Baud rate, parity, data bits and stop bits are defined per the RS232 protocol to match the settings made in the PLC.

Data Mappings

Data mappings are defined by specifying a i/o/memory range in the RTU and a corresponding file (with elements) in the PLC.



DF1 Slave	
Configuration	
Enabled	False
Com Port	RS232A
RTU Address	1
PLC Address	2
Com Port Settings	
Baud Rate	19200
Parity	none
Data Bits	8
Stop Bits	1
Data Mappings	
{ RD117 - N1:1 } (2 bytes)	
RTU Mapping	
Type	RDI
Index	17
PLC Mapping	
File Type Id	INTEGER
File Number	1
Element Number	1
Byte Count	2
{ RAI7 - N2:0 } (32 bytes)	
RTU Mapping	
Type	RAI
Index	7
PLC Mapping	
File Type Id	INTEGER
File Number	2
Element Number	0
Byte Count	32

Clicking the add mapping button creates a template entry in the data mappings filed which can then be modified to suit. The mappings are summarized in the first line in the form:

{ <RTU data type><RTU data point index>:<PLC file data type><file number>:<element number> }
(number of bytes to transfer)

The following RTU data types are supported:

1. RDI – real digital input
2. RDO – real digital output

3. RAI – real analogue input (word)
4. RAO – real analogue output (word)
5. TDI – telemetry digital input
6. TDO – telemetry digital output
7. TAI – telemetry analogue input (word)
8. TAO – telemetry analogue output (word)

RTU Mapping – Select from one of the above data types

RTU Index – the starting index number of the digital input per the data point table as summarised in the input/output category

PLC Mapping – specifies the memory mapping reference in the PLC. In PLC-5 nomenclature this is represented in the form for example \$N1:1 meaning Integer file type file number 1, element 1, or \$B3:4 (bit file type file 3 element 4)

File Type ID – Elect from Integer or bit file data types supported

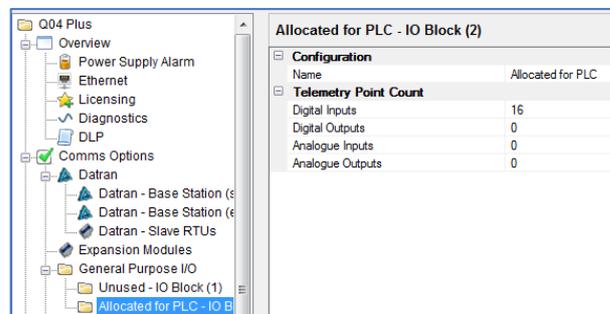
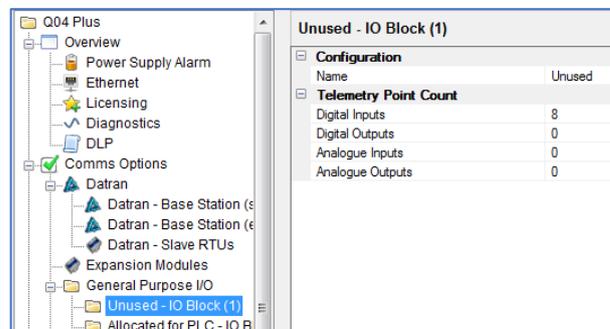
File Number – The corresponding file number in the PLC to map the memory address

Element Number – The corresponding element number or specified row of the file in the PLC

Byte count – The size of the memory block (as an even number of bytes)

Note: Mappings do not actually allocate data in the RTU data table. If a section of memory is to be set aside to hold say PLC memory values, then the user could allocate general purpose memory for PLC data.

Note: Take care with digital inputs. The starting index of the digital input must lie on a word boundary (1, 17,33 etc) Since the RTU itself has only 8 native digital inputs and in situations where there is no other i/o defined it may be useful to create an unused or unallocated space so that the first mapped digital input has an index of 17 (see example below).



General Purpose I/O							
Name	DI	Range	DO	Range	AI	Range	AO
Unused	8	9 - 16	0		0		0
Allocated for PLC	16	17 - 32	0		0		0
Totals	24		0		0		0

Name	Type	DI	DO	AI	AO
RTU's	Native IO	1 - 8	8	1 - 8	8
Unused	Placeholder	9 - 16	8	0	0
Allocated for PLC	Placeholder	17 - 32	16	0	0
Totals			32	8	6

DF1 Slave	
Configuration	
Enabled	False
Com Port	RS232A
RTU Address	1
PLC Address	2
Com Port Settings	
Baud Rate	19200
Parity	none
Data Bits	8
Stop Bits	1
Data Mappings	
{ RDI17 - N1:1 } (2 bytes)	
RTU Mapping	
Type	RDI
Index	17
PLC Mapping	
File Type Id	INTEGER
File Number	1
Element Number	1
Byte Count	2

In this manner the digital inputs do not overlap the RTUs own digital inputs. However, the mapping can include the RTU i/o if desired, for example if the PLC wants to read the state of RTU inputs.

Upgrading from Q03/Q22

When replacing a Q03 RTU with the XL4 *Plus* the following considerations should be made:

1. The PLC needs to be configured to use the "Full Duplex" (peer to peer) variant of DF1, and not the "Half Duplex" variant.
2. The RTU supports access to INTEGER and BIT type files in the PLC, but not other file types (such as timers, counters, strings, etc).
3. The RTU is configured as a DF1 Master (specifically in the case of replacing a Q03)
4. The RTU will ignore commands initiated from the PLC and may indicate that they are out of sequence (a Warning in the diagnostics about TNS) if the PLC does not respond with the Sequence number of the command initiated by the RTU.

5. The Q03 has a hard-coded source (SRC) address set to 0. Workbench must be set the PLC (slave/command executor) destination (DST) address to the address defined in the PLC as its SRC address.
6. The Q03 only uses unprotected read/write (command 1 and 8) which access file N9. The XL4 *Plus* supports more commands but even though you may select say SLC as the processor type it would usually use protected reads and writes so it may be more useful to use the CIF mode when trying to replicate Q03 functionality explicitly.

Diagnostics

A trace of communications can be enabled in QTech Workbench by turning on and displaying the Diagnostics window.

If the DF1 category is selected the RTU will display diagnostics relating to the DF1 protocol. To see a trace of raw data transfer also turn on the serial comms category in the diagnostics.