PROFINET Redundancy Function Block

This document provides an overview and explanation of PROFINET network redundancy and the PROFINET IO Controller using the PROFINET Redundancy Function Block. It also addresses CX-Server OPC use with the Redundancy FB.

Introduction

PROFINET, as it is based on ethernet communication, is capable of having redundancy on different levels. In an application where redundancy would be useful the major areas are the network level, the IO Controller level and the SCADA level. At all these three levels there is a solution using standard functionality of the devices and standard communication protocols.

Network redundancy

PROFINET has defined a specific redundancy protocol for the network level. It is called Media Redundancy Protocol or MRP. With it, a redundant ethernet ring topology can be constructed. Should a single point of failure occur, it will disturb the communication for a very short period because the network must discover the fault and rebuild the communication links.

IO Controller redundancy

Normally one IO Controller controls an IO Device. But the PROFINET specification defines that two or more IO Controllers can have a connection to an IO-device. One of them is in control. The other is in standby. As soon as the one that is in control fails, the standby can take over immediately as all connections are already established. To simplify implementation of this function, a redundancy Function Block is available. Actually the implementation is within the IO Device as it needs to support the multiple connections.

SCADA redundancy

If there are two IO Controllers that can control an application then it is difficult for a SCADA application to esthablish which one is in control. Actually it is not of importance for a SCADA to which PLC it is communicating as it are two PLCs forming one application. The OMRON CX-Server OPC V2.0 can present two redundant PLC's as one to the SCADA application. The CX-Server OPC will read from the PLC that is in control and write to both PLC's. In this way the PLC's are kept in sync. There is also the possibility to have multiple communication paths from CX-Server OPC to the PLC's to increase availability.

PROFINET redundancy

With Network, IO Controller and OPC server redundancy a system can be built with a high grade of availability. An example of such a system is shown below.
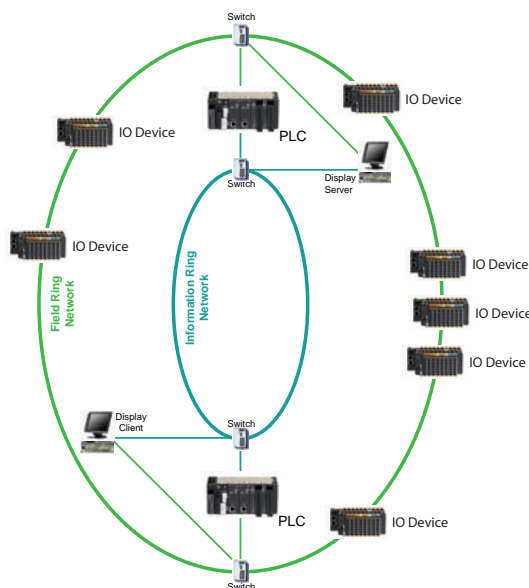
For the implementation of the redundancy functionblock this network setupis used. There is a Fieldnetwork or Controlnet and a Informationnetwork or Infonet.

PROFINET Network Redundancy

Media Redundancy Protocol

Network Redundancy issues in office networks are handled by the network switches. There are several protocols that handle network redundancy. Some are standardised like Spanning Tree and Rapid Spanning Tree. They fulfill their tasks within the office environment with detection and rebuild times of several seconds to minutes.

However, the networks used in industrial automation are intended for control. Applications normally can not withstand this gap of several seconds. Control must be back very quickly. A couple of 100 ms are really the maximum value.

For PROFINET there was the need for an open and fast network redundancy protocol. Therefore the Media Redundancy Protocol (MRP) was developed. It is open to all vendors that implement PROFINET.

MRP devices are connected in a ring structure. If the ring breaks, this is detected and signalled. The network is then re-established very quickly. In MRP the following devices are defined.

- MRP manager, takes care of sending MRP packets over the ring and detecting and rebuilding the ring if there is a failure.
- MRP client, forwards MRP packets and signals to the MRP manager if a packet can not be forwarded.

MRP Manager

The following switches with MRP manager are recommended in combination with Omron SmartSlice.

Manufacturer	Type
Hirschmann Automation and Control GMBH	Series RS20/30/40, Software Version 4 or higher.

MRP Client

The OMRON GRT1-PNT SmartSlice IO Device coupler has two ethernet ports built in. In this way a line topology can be built by daisy-chaining from one device another. Next logical step is to build a ring to have network redundancy. Therefore an MRP Client is incorporated in the GRT1-PNT. There are no settings needed. The GRT1-PNT will handle MRP packets by default.

Setup in the MRP manager

The MRP manager switch needs to be setup before it can handle MRP ring redundancy. This is an example how to set it up in the a Hirschmann RS20 switch. Before making changes make sure both DIP-switches on on the RS20 switch are set to the ON position. Otherwise the RS20 wlill not accept changes made through its configuration webpages.

To setup the MRP redundancy through software both DIP-switches on the ethernet switch must be set to the ON position.

The ethernet switch also have some status and alarm LEDs and a Alarm contact. The Status LEDs will show if all is alright and if this switch works as Ring manager. In the sofware settings you can setup when the Alarm LED and contact are set. There is a multitude of possibilities like the redundant powersupply, temperature of the switch but also the redundant ring status.

Assuming that you have already set up the IP-address of the Hirschmann switch with the Hirschmann HiDiscovery tool you can access the switch through a web-browser. The default username and password to do the settings are:

Username: admin
Password: private

First set up the MRP redundancy:
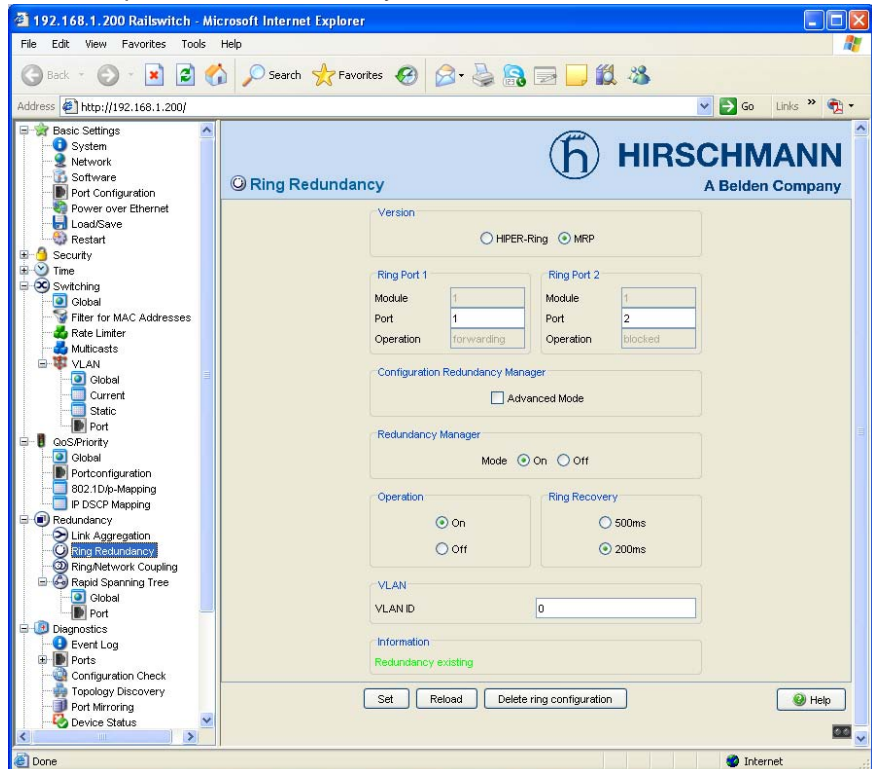
By default the Hirschmann switches have RSTP (Rapid Spanning Tree Protocol, another ring protocol) switched on. This must be turned off to prevent conflicts with MRP
If a ring is detected, the setup screen will show that redundancy exists. Any other switch in the network participating in the MRP communication also needs to have MRP set up, but it should have the Redundancy Manager switched off. So the switch will act as an MRP client. The Omron GRT1-PNT IO Devices have MRP client functionality switched on by default. No settings can be made.

.
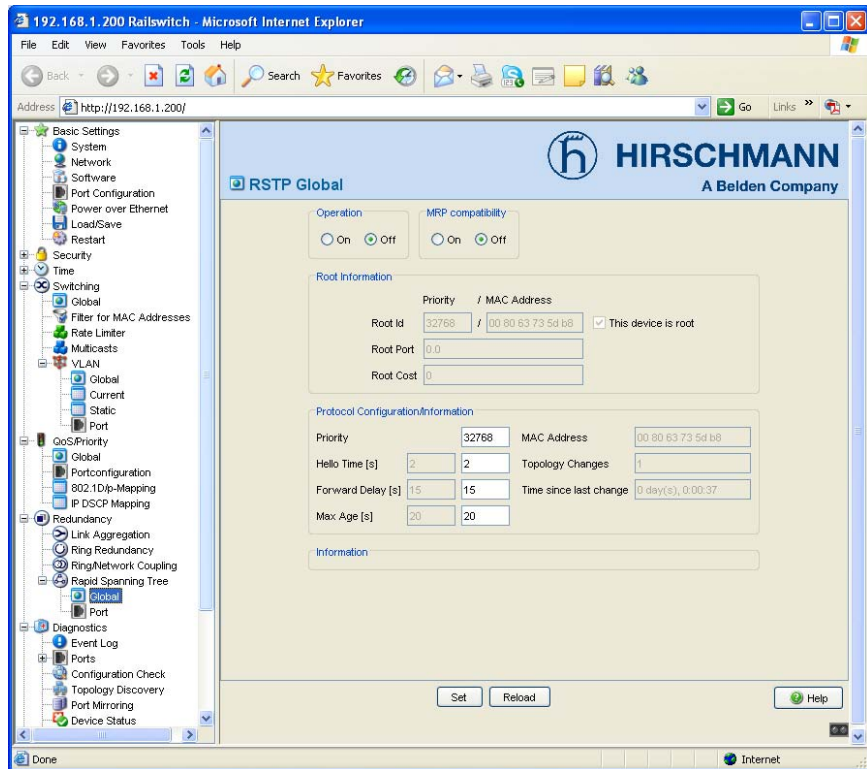
One last setting is the support of VLAN0. PROFINET uses this VLAN0 tagging to gain priority. Although it is the standard and lowest priority it should have priority over other traffic. However, some switches remove the VLAN0 tag from the message and therefore alter the message. For compatibility Hirschmann implemented this tag removal but for PROFINET the tag should stay in. There is a setting to keep the VLAN0 tag in the message. Therefore enable the VLAN0 transparent mode.
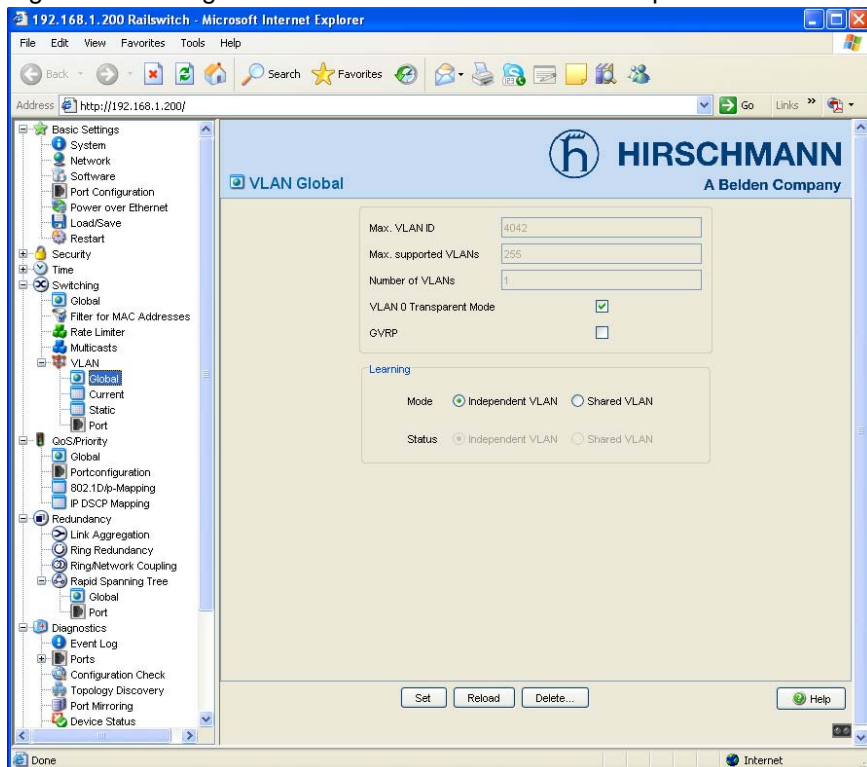
PROFINET IO Controller Redundancy

PROFINET IO defines three types of devices, IO Controllers, IO Devices and IO Supervisors. In this case we only focus on IO Controllers and IO Devices.

IO Controller

IO Controllers initiate a connection to an IO Device and send configuration and parameter data to the IO Device. The IO Device must first accept the configuration and parameter data and then starts to exchange I/O-Data with the IO device.
In a master-slave configuration this is the master.

IO Device

An IO Device is a peripheral device. Typical IO Devices can be input/ output devices, valves, drives, and measuring transmitters. It can not initiate a connection, and will only send out Input data if an IO Controller has a connection to it.
In a master-slave configuration this is the slave.

Provider status

In the I/O Data exchanged between the IO Controller and IO Device there is a bit called the Provider status. With this bit the provider of the data (for Input data this is the IO device, for output data this is the IO Controller) can mark the data as being valid or invalid. Invalid data is discarded by the receiver of the data. IO Controller redundancy in PROFINET is based on this principle of Provider status.

Multiple connections

The GRT1-PNT IO Device is capable of connecting to two IO Controllers. Input data is sent to both IO Controllers. However, output data is accepted only from one IO Controller.
The GRT1-PNT accepts only the output data from that IO Controller that set the Provider status first.
In case both IO Controllers set their Provider status to valid then the GRT1-PNT will service the first one that connected first. It wil ignore the output data of the second one. However this situation is not recommended.

User Bit Controlled.

There are two methods to control the CJ1W-PNT's Provider status. The method is chosen in the configuration DTM. It can be:
• PLC Mode Dependent
• User Bit Controlled

When PLC Mode Dependent is selected the CJ1W-PNT21 IO Controller will set the Provider status according to the PLC mode.
In Program mode the IO Controller will set the Provider status to invalid. The IO Device will have its outputs set to a failsafe state.
When it is in Monitor/Run mode then the Provider status is set to valid and the IO Device will set the outputs according the output data.
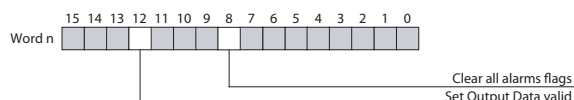
This behavior needs to be set in Configuration - IO Controller Setup under

Valid Output Data Handling.
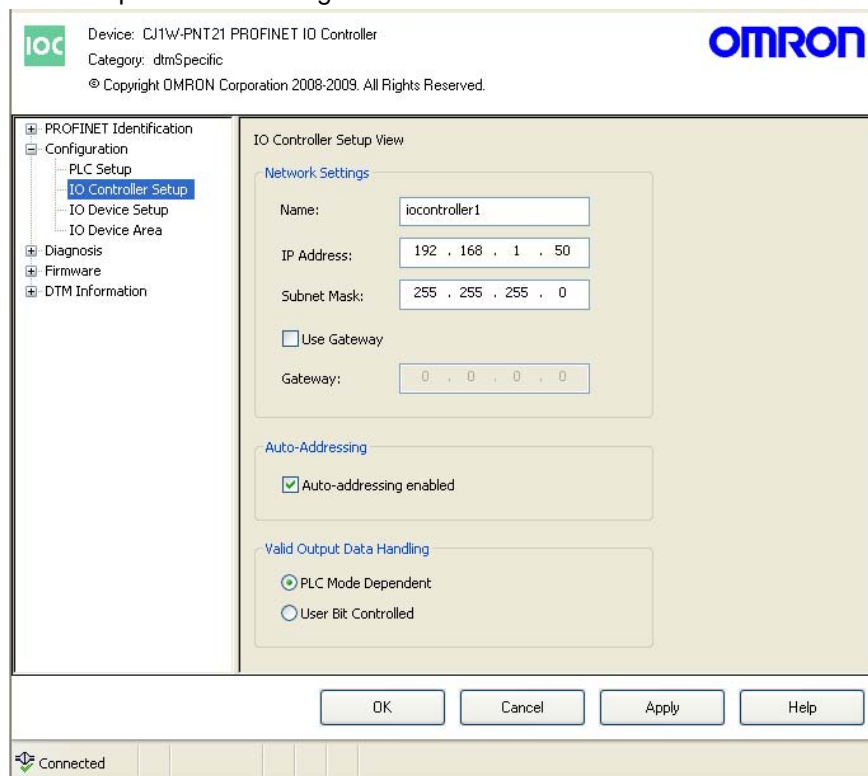
User Bit Controlled gives the possibility to control the Provider status from the PLC-program. This is what is used by the Redundancy FB and should be set if the Redundancy FB is used.
The bit that controls the Provider status is in Software Switches 1 CIO 1500+n.12
.

Recovery Time   The switch that is the MRP Manager needs a certain Recovery Time to switch over if the ring is broken or is established again. In the configuration tool the IO Controller is set per connection to the IO Device's Update Rate, Watchdog Time and Data Hold Time.

Update Rate   The Update Rate is the time between the updates of the I/O Data between an IO Controller and an IO Device.
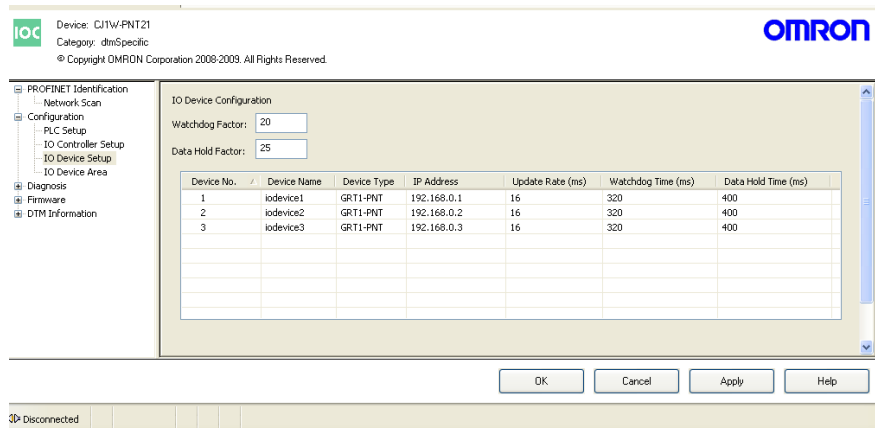
Watchdog Time   The Watchdog Time is used by both the IO Controller and the IO Device to allow the connect ion to time out. If within the Watchdog Time there has not been an IO data update then the connection is closed. To start communication again the connection needs to be re-esthalbished. This re-connection of the IO-Controller to the IO Device takes time so it is preferred that conncetions are not closed.

Data Hold Time   The Data Hold Time is the time that the IO Device maintains the status of its output data after the last IO Data update. The IO Device will reset its outputs (safe state) if the Data Hold Time passes.
The Data Hold Time must always be longer than the Watchdog Time.

The Update Rate has no relation to the Recovery Time. However the Watchdog Time and DataHold Time must be longer then the Recovery Time. A typical Recovery Time is 200ms for a MRP ring. But the Recovery Time depends on the type and number of MRP Client devices in the ring. Rule of thumb is to set the Watchdog Time above 300ms and the Data hold Time above 400ms.

As a result the IO Devices will disconnect and turn the ouputs to a safe state in 300 to 400 ms.

In this case a unconnected period can be as long as 400 ms before this state is noticable in the application. However the application must be capable of withstanding this period of maxiumum 400 ms with no control.

Redundancy FB

The Redundancy concept requires two PLC's that run exactly the same program. One will be the active controller the other is on standby. They exchange status information and with this decide which one is in control of the IO Devices. The status information transfer is not dependant on a specific network type. It will work using data transfer over datalinks or FINS communication. Below is a logical overview of a redundant IO Controller setup.

Redundancy FB communication
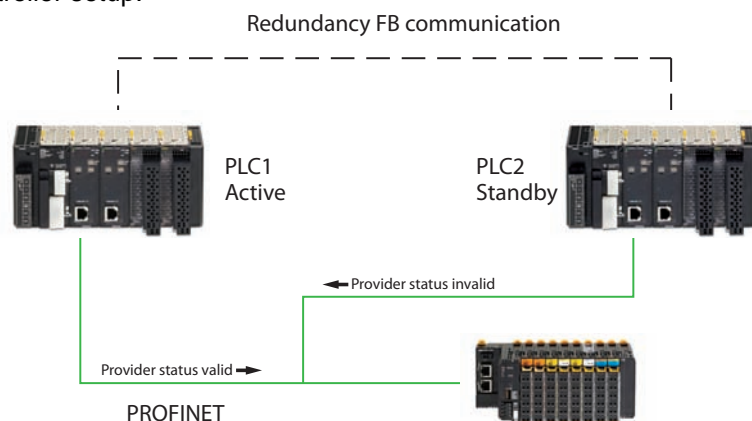
The preferred solution for the Redundancy FB communication is EtherNet/IP. This is because it is easy to set up datalinks to transfer data independent of the PLC program. It is also fast, reliable and easy to install. It can run on the same network as the PROFINET communication, but to have higher reliability we recommend it is used over a seperate (ethernet) network.

There are some things to consider:
• If using EtherNet/IP on the same physical network as PROFINET, set the connection method to point-to-point, and not multicast! As multicast

is a kind of broadcast message these multi-cast messages will be all over the network.

- Try also to set the RPI (packet interval) for EtherNet/IP to a value that is not an integer multiple of the update rate(s). This will prevent that a multitude of messages is sent at the same time. For the EtherNet/IP communication set per connection also to the RPI to a slightly different value like 50, 51, 52, 53... ms. In this way you will not have all the EtherNet/IP messages at the same moment.

The FB can be divided into 5 destinctive parts.

- Internal checksum of the PLC program/code is read from the CPU, and compared with the other PLC. If the programs are different, the PLC that started as standby will not participate in the IO Controller redundancy.
- Included is a single FINS communication path to transfer data between the 2 PLC's. This connection can then be redundant to e.g. an EtherNet/IP (EIP) connection. In the example there is a configuration file for the EIP connection. If a double set of EIP connections is used, the FINS alternative may be disabled. If FINS connection is used, it can be over any connection that supports it. Alternatives are EIP21, ETN21 and PNT21 units. Remember to define the Routing Table when using FINS. When FINS is used, it only sends 1 word if it is the backup for e.g. an EIP connection. If it is the main connection, it sends 522 words
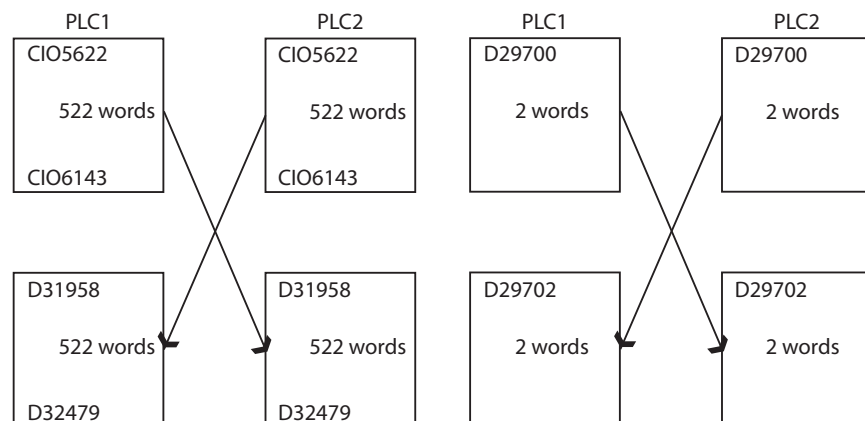
- A lifecycle value is continuously incremented between the 2 PLC's. As long as both PLC's are operational, communication checks indicate the status. There are 2 lifecycles, one for each connection route, e.g. an EtherNet/IP connection, and one for the FINS connection. Originally the FINS connection was designed to run on PROFINET, but any other available path may be used.
- The redundancy FB is controlling the CJ1W-PNT21 PROFINET IO Controller. Based on several conditions, the FB decides which PLC will be in control (Active) of the I/O Devices (IODs).
- Control over the FB can be achieved from an OPC interface for example. There are several bits/words for monitoring/controlling the FB. Most important are two control bits. One that can be used for manually switching the Standby PLC to become the Active. The other bit is used to force the Active PLC to maintain Active, and then automatic switchover is disabled. All these bits can be controlled by CX-Server OPC as they are available when a redundant communication setup is chosen.

For HMI communication interfaces that supports redundant connections (like CX-Server), there are 4 bits for manually changing the active status.

For HMI communication interfaces that NOT supports redundant connections (like Citect - can only read/write from 1 of the PLCs), there are only 1 bit for changing the active status.

To let the redundancy FB work properly settings must be made in both PLC's prior to operation. These are:

  D29980 = Info Network Node Number
  D31810 = EIP21 Unit Number
  D31800 = PNT21 Unit Number
  D31900 = FINS Network Number (Routing Table)
  D31901 = FINS Node Number (IP Address Table)
  D31902 = Timeout (1/10ms unit) for lifecycle watchdog
  D31889.6 = Disable FINS communication/connection
  D31889.7 = FINS is done over PROFINET
  D31889.10 = HMI (OPC is not used) can only write to Active PLC

Info Network = Main (EtherNet/IP) data exchange network
Process Network = I/O (PROFINET) and backup data exchange network

There are some special considerations that must be taken into account when the redundancy FB is used.

If the Active PLC is set to STOP/PROGRAM mode, all outputs on the IODs may drop off (analogs to zero) for a short time. To avoid this, the FB is using the IOM Hold Bit internally to hold any status in the CIO memory area. This bit is only set on the Active PLC. Once the Active PLC is set to STOP/PROGRAM mode, both lifecycle checks will detect this in the Standby PLC, and this PLC will take control over all IODs, and at the same time it sends a FINS command to turn off one bit that is used to control the IOC of the former Active PLC. This will cause the former Active to switch to Standby. To support this feature, any FINS connection between the 2 PLC's must be configured.

Memory areas in the 2 PLC's can be synchronised during operation. The Active PLC sends it's memory content to the Standby if it differs. To handle this functionality, the complete memory of the PLC's (up to 3 EM's are supported) are divided into datablocks of 512 words. For each datablock the FB is calculating a 1 word check sum (FCS) and counting the number of bits that's on (=1). The checksums and bitcounts are transferred from the Standby PLC to the Active, where it is compared, and based on the result the Active PLC updates the Standby PLC with it memory content. The following list of memories are NOT synchronised, as they are used by the redundant control FB's.
CIO1500-1899
CIO5120-6143
D29696-32767

CIO5622-6143 and D31958-32767 (both 522 words) are used by the FB to transmit data between the 2 PLC's, and must therefore not be used without checking the logics in the FB first.

CIO5120-5621 (502 words) and D29696-31957 (2262 words) are partially used by the FB for internal logics and calculations, and must therefore not be used without checking the logics in the FB first.

As communication in the Redundancy Functionblock partly uses FINS routingtables need to be set up. Do this within Cx-Integrator.

EtherNet/IP setup

In the EtherNet/IP setup there are two PLC's who excahnge two blocks of data with eachother. One is the lfecycle counter and the other is used for the data-synchronisation. The IP-addressses of the Ethernet/IP units are 192.168.250.1 and 192.168.250.2

192.168.250.1   192.168.250.2
CJ1W-EIP21   CJ1W-EIP21
...250.2   ...250.1

Each PLC initiates communication to the other in that it starts to fetch the data from the other.
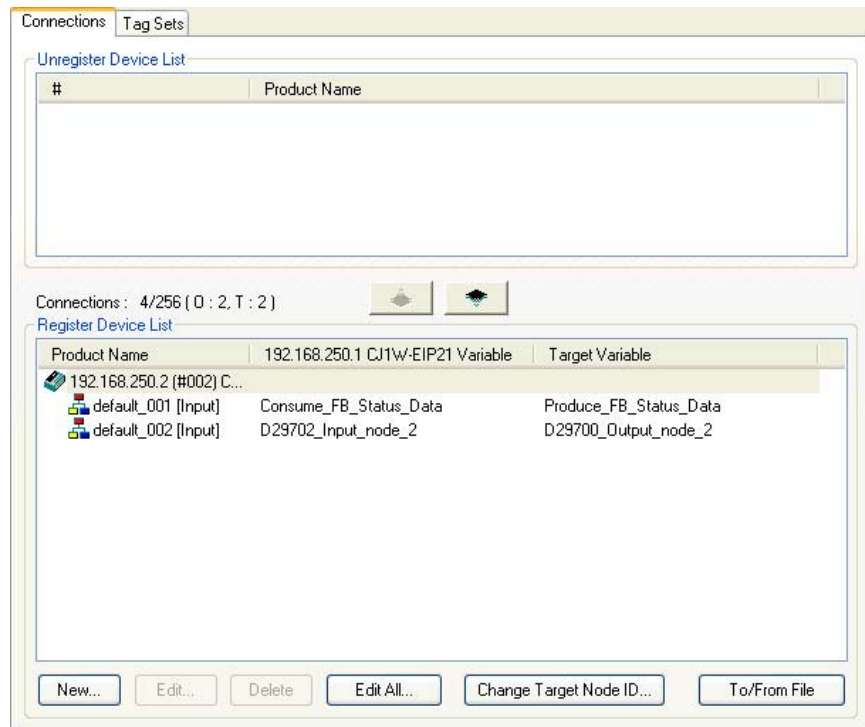
The update rate of the data is set to 50 ms this is fast enough to detect failure of the other PLC and switch over with difficulties. Also the synchronisation of the datablocks is fast enough.
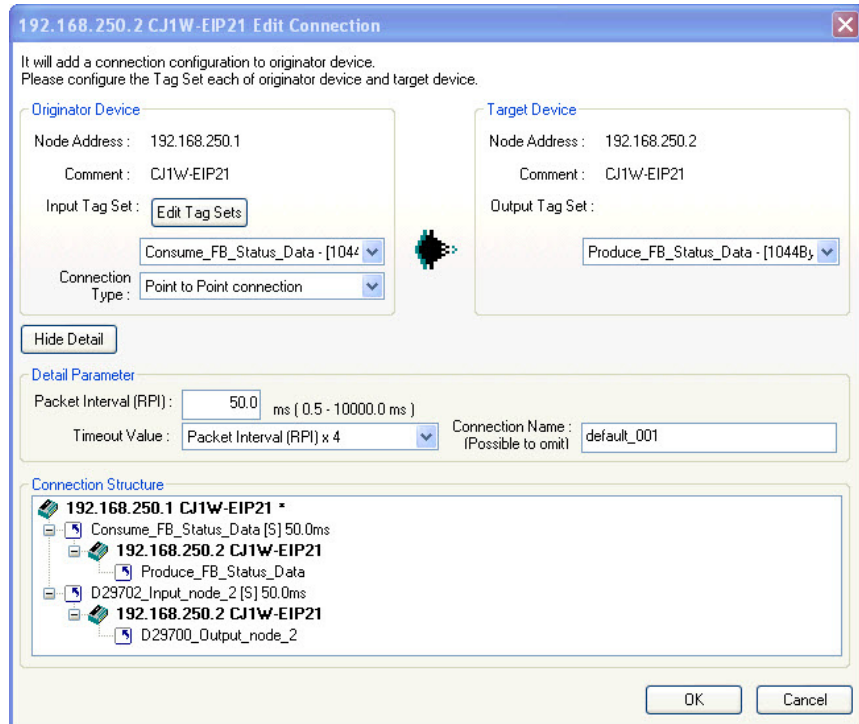
Both PLC's have exactly the same number and size of Tagsets and Tags in the in-Consume and the Out-Produce Area.
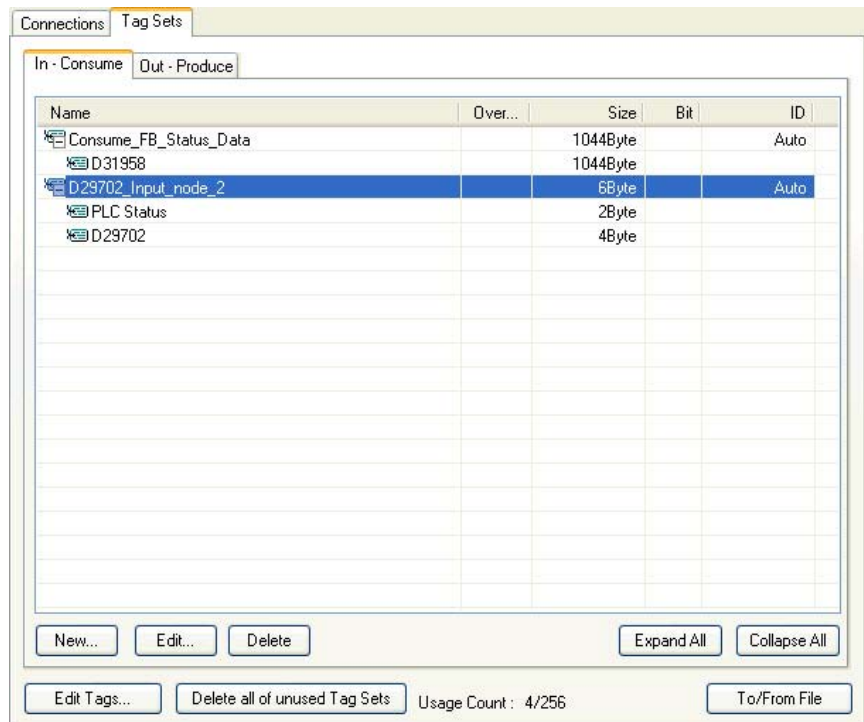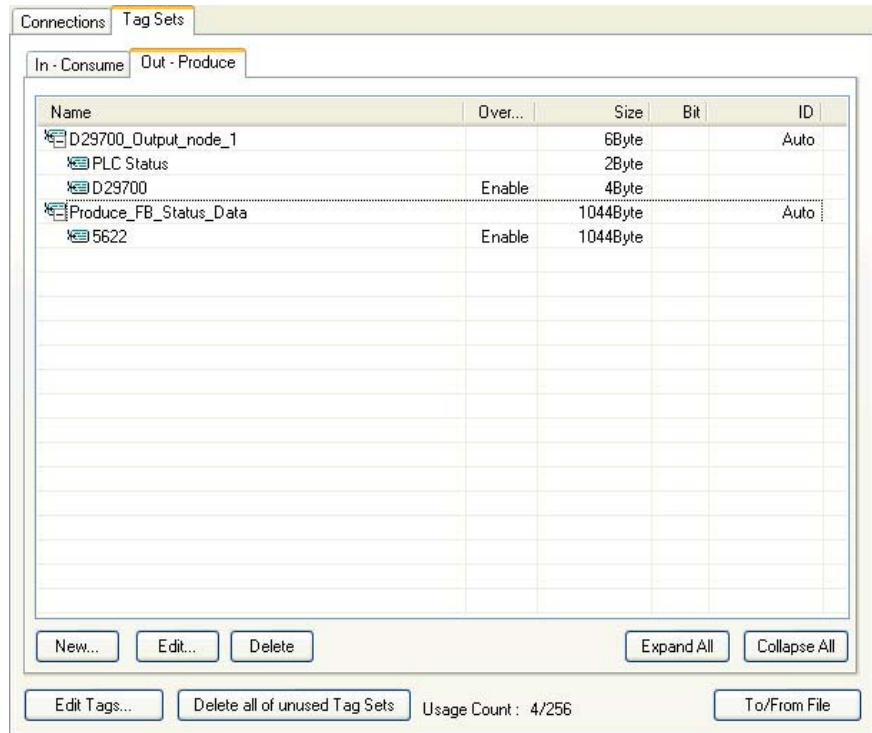
Setup example

The example setup is developed on a democase which consists of the following components.
Two PLC's
- CJ2M-CPU13
- CJ1W-EIP21
- CJ1W-PNT21

Two IO Devices.
- GRT1-PNT
- GRT1-ID4-1
- GRT1-OD4-1 4 pieces
- GRT1-END-M

Two Hirschmann RS20 4 ports managed switch.
One Omron W4S1-05B 5 ports unmanaged switch.
One Omron NS12 HMI terminal

All the project and configuration files are included. Filenames are according to the screenshot below.

Name ▲	Size	Type	Date Modified
PROFINETSIMPLE		Folder	20-4-2011 10:46
PLC_Left_IP_192_168_250_0...	41 KB	CX-Programmer Pro...	8-4-2011 13:19
PLC_Left_IP_192_168_250_0...	6 KB	OPT File	20-4-2011 11:53
PLC_Left_IP_192_168_250_0...	1 KB	Omron Routing Tabl...	8-4-2011 13:22
PLC_Right_IP_192_168_250_...	41 KB	BAK File	8-4-2011 13:36
PLC_Right_IP_192_168_250_...	42 KB	CX-Programmer Pro...	20-4-2011 11:54
PLC_Right_IP_192_168_250_...	6 KB	OPT File	20-4-2011 11:54
PLC_Right_IP_192_168_250_...	1 KB	Omron Routing Tabl...	8-4-2011 13:37
Profinet Redundancy ATK.cpr	1.239 KB	CX-ConfiguratorFD...	20-4-2011 11:53
Profinet Redundancy ATK.nvf	17 KB	Network Configurati...	20-4-2011 11:25
PROFINET redundancy.cin	5 KB	CIN File	8-4-2011 13:25
Profinet Redundancy_image 1...	86 KB	JPEG Image	11-4-2011 12:02
Profinet Redundancy_image 2...	100 KB	JPEG Image	11-4-2011 12:02
Profinet Redundancy_image 3...	85 KB	JPEG Image	11-4-2011 12:02
Profinet Redundancy_image 4...	85 KB	JPEG Image	11-4-2011 12:03
ProfinetSimple.IPP	64 KB	CX-Designer Project	8-4-2011 12:13
SW1-MRP-manager	14 KB	File	20-4-2011 11:57
SW2-MRP-client	14 KB	File	20-4-2011 11:58

The setup consists, as described in the introduction part of this document, of two seperate networks. One is serving the PROFINET communication, the other is handling the exchange of status information used by the redundancy FB. On this status information the decisions are made which IO Controller should be the Active and the Standby. This status information is exchanged over a EtherNet/IP connection between the two PLCs.

The NS-terminal is communcating to both PLCs over the EtherNet/IP network to do settings and display the status.
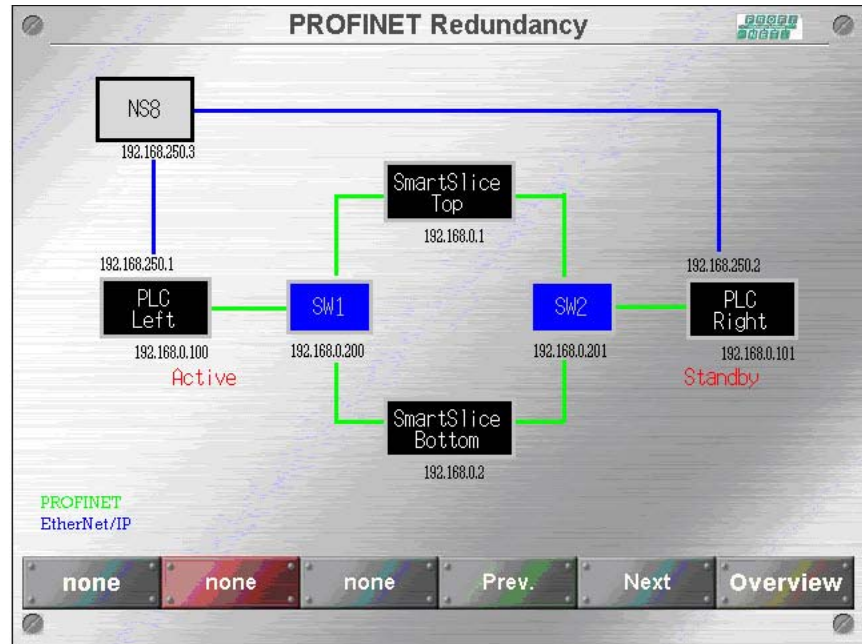
For each of the devices the IP-addresses are shown. These IP-addresses can be used to communicate to each of the devices.
For the PLC it can be to monitor the PLC-program or review the settings of the components of the PLC.
The Hirchmann switches have a web-page build in to check status and do settings.
For the IO Devices the IP-address can be used to acces the SmartSlice settings and information.

The Status and Control screen gives access to the operational information of the redundancy FB. With the Make active buttons the PLC that is on control can be selected.
Furhter there are some indications on errors and the possibilty to accept these errors. The Force to Run setting can be used to force that specific PLC to get in control of the IO Devices.
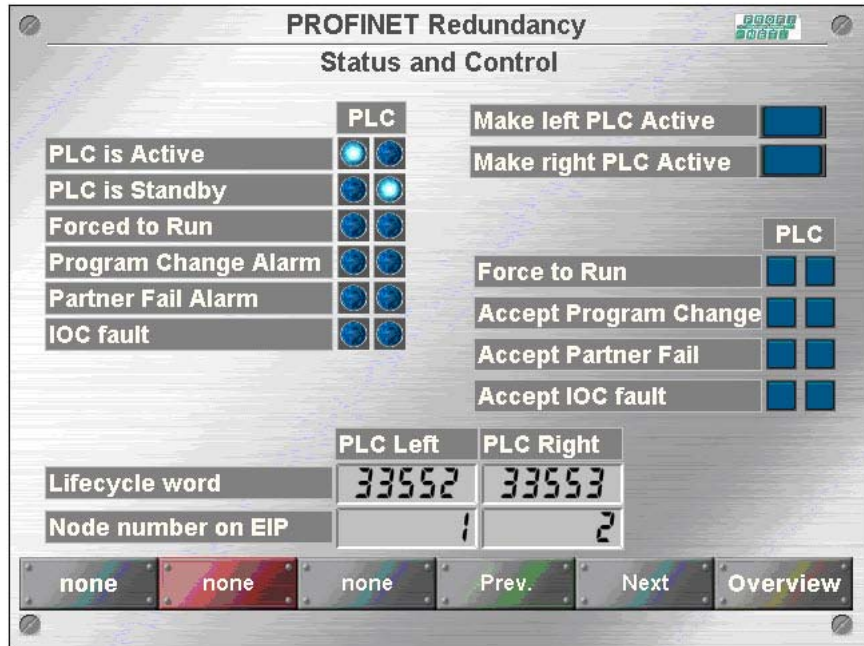
In the Setup screen the necassery setting can be made. For your convenience there is a Default settings button that sets the registers to the correct value.
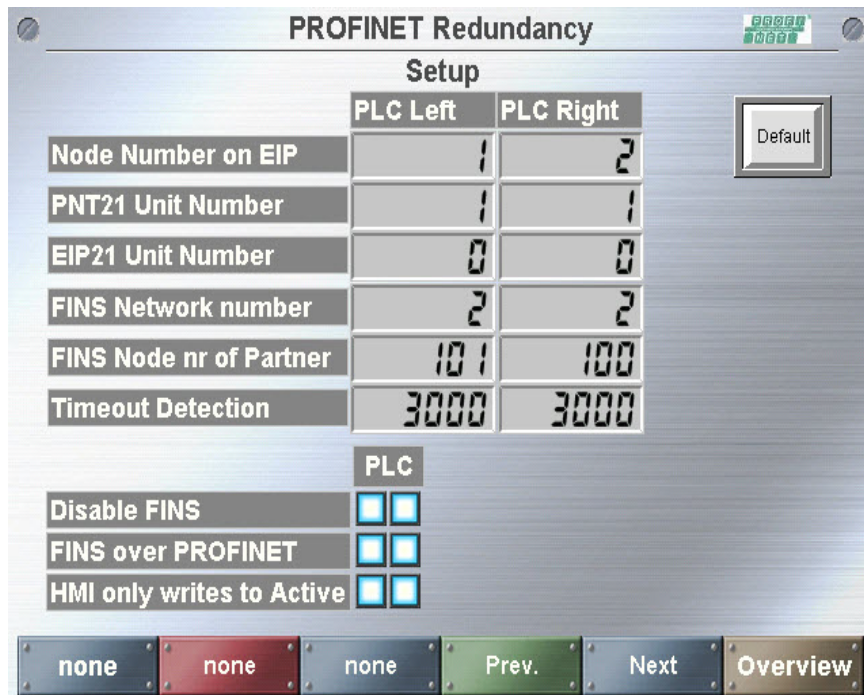
The Timeout Detection is set in units of 0.1ms. The set default value is here 300ms. It shuld be less then the
Disable FINS let you turn of the use of FINS communication to exchange the status information between the PLCs . A different mechanism is now used to exchange the blocks of data for status and memory synchronisation.
FINS over PROFINET forces the exchange of this information over the PROFINET network.
The HMI only writes to active is a convenience setting where you have a

SCADA or HMI that is not capable to write to two PLCs simultanious.
Now the HMI or SCADA only writes to the active one and then the content
is copied over to the other one.

Further the synchronization of memory areas must be set. The data is
copied from the active PLC to the standby one if the content of the data-
areas differ.
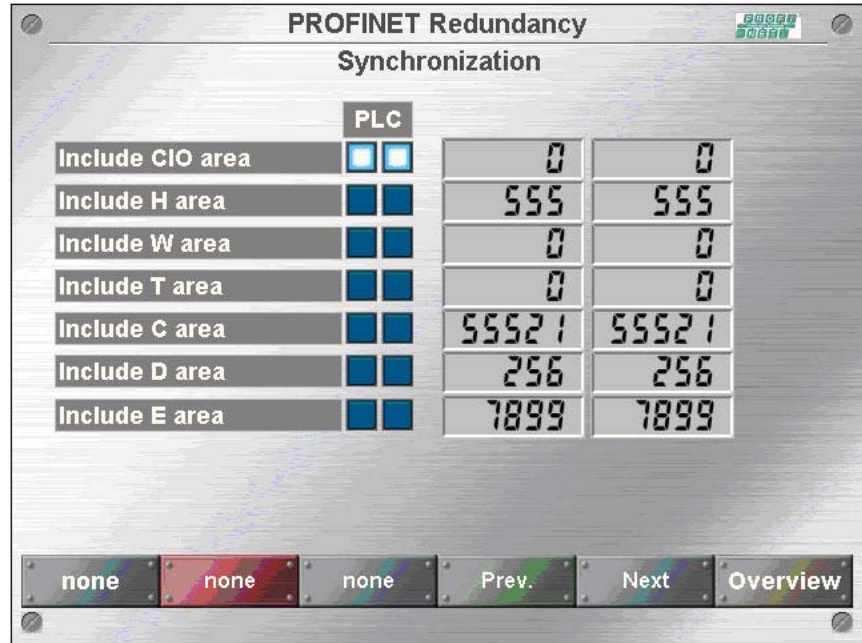
The Redundancy FB is developed to withstand a single-point-of-failure.
So when one component fails then this can be detected and handled.

SCADA redundancy

CX-Server OPC V2.0 From CX-Server OPC V2.0 redundant network connections to a PLC are supported. If there are redundant PLCs set up it can even facilitate the SCADA application by showing these two PLC's as one. Data supplied to the SCADA application is read from the active PLC. Data is written to both PLC's simultaneously to keep them in sync.

Setup With the normal configuration file for the address and the points of a PLC a redundancy file needs to be made. This is achieved using the CX-Server OPC project configuration.
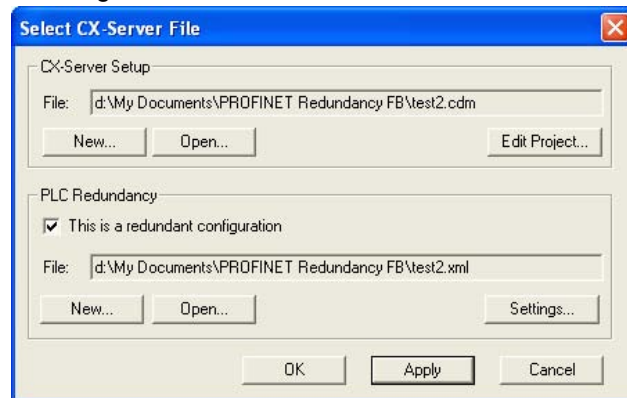
Here the configuration is marked being redundant, and the redundancy configuration file can be made. But before selecting the settings button first Apply the CX-Server setup changes.

The screen below will appear when the Setting button is pressed. Make sure to press the apply button first..

PLC1	Redundancy Level	Redundancy On	Address	Network Number	Node	PLC Status Location
CJ1M - CPU23	1st Network		192.168.0.55	4	55	StatusPoint
	2nd Network	☑	192.168.0.56	12	56	
Partner	1st Network	☑	44.55.66.77	4	77	
	2nd Network	☑	44.55.66.78	12	78	
PLC2	Redundancy Level	Redundancy On	Address	Network Number	Node	PLC Status Location
CJ1M - CPU23	1st Network		192.168.0.61	4	61	S2
	2nd Network	☐				
Partner	1st Network	☑	44.55.66.80	4	80	
	2nd Network	☐				
PLC5	Redundancy Level	Redundancy On	Address	Network Number	Node	PLC Status Location
CJ1M - CPU23	1st Network		10.50.59.99	4	99	
	2nd Network	☐				
Partner	1st Network	☐				
	2nd Network	☐				

PLC addresses What would then be one PLC to the SCADA system, in this case PLC1, PLC2 or PLC3, CX-Server OPC can access two redundant PLC's and each over two different connections.

Redundant OPC connections. In addition to the device-level redundancy there is also network-level redundancy- i.e. for each device two separate Ethernet connections, associated with two different networks, can be specified. It is possible for example, to connect to a PLC via two entirely separate Ethernet networks, with the only common hardware being the PC and the PLC.

Control and Status CX-Server OPC handles the SCADA data depending on which PLC is the active one. This information is read from the PLC at assigned locations.

There is a block defined in the Redundancy FB starting at CIO5610 and 8 words in size. This start address must be set in the PLC Status Location field.

The following tags are predefined in CX-Server OPC to handle the Control and status of the Redundancy FB:

- PLCNAME_Active – Whether a PLC is currently the active device (boolean)
- PLCNAME_Inactive – Whether a PLC is currently the inactive device (boolean)
- PLCNAME_ForcedRun – Whether the PLC forced run bit is set
- PLCNAME_ProgChangeAlm – Whether the PLC FB "Program Change Alarm" bit is set.
- PLCNAME_PartnerFailAlm – Whether the PLC FB "Partner Change Alarm" bit is set.
- PLCNAME_Lifecycle – Whether the PLC FB "Lifecycle" bit is set.
- PLCNAME_PrimaryNodeNum – PLC FB Primary Node Number
- PLCNAME_MakeActive – When set, makes a PLC Active
- PLCNAME_MakeInactive – When set, makes a PLC Inactive
- PLCNAME_ForceRunPLC – When set, forces a PLC to run
- PLCNAME_AutoSwitch – When set, indicates that the server should treat a device as inactive when communication with it is lost (otherwise the FB Active and Inactive setting will always be treated as correct – i.e. the redundancy will be under full Function Block control).
- PLCNAME_OKConnections – Number of currently valid connections to a device (e.g. in a system with both device redundancy and network redundancy this value will normally be 4).

Data synchronisation.

In a redundant system both PLC's should be equal to each other. Not only the program they are running but also in the content of the PLC-memory. This means not only normal variables but also the timers and counters used in the PLC-program.

The redundancy function block has for this purpose two functions built in:
- A check if the PLC-programs are equal. At startup of the second PLC the checksum of the two PLC's programs are checked and if not equal the second PLC will not go to Standby state and will not participate in the redundancy.
- Copying of PLC-memory content. When the two PLCs are working in redundancy mode, one is active the other is on standby, then the memory content of the active PLC is transfered to the standby PLC. In this way the standby PLC memory will be a copy of the active PLC.

The data in the PLCs can be changed by three sources. These are:
1. The I/O and communcaition units of the PLC have their memory area where they store their status information.
2. The memory area that is used by the PLC-program to store its variables which it works with.
3. The memory area that the HMI or SCADA is reading and writing.

For the first one no synchronisation needs to take place as the data comes from the I/O. As this is for both PLC's the same source data in both PLCs is equal.

The variables of the PLC-program only need to be syncronised when the standby PLC is starting. As both PLC-programs and I/O are the same content of the variables will be the same.

For the HMI or SCADA this is however needed to keep the two PLC's in sync. From Cx-ServerOPC V2 functionality is built in to write to both PLCs and read from the active PLC. For HMI and SCADA systems that do not support this functionality the redundancy FB can take care of this by copying the content of memory areas over when something changes. The FB calculates a checksum over a given memory area and concludes if it needs to be transfered. If different then the block is sent over.

Addres	Bit	Description
D31889	0	Include CIO in the synchronization
	1	Include H in the synchronization
	2	Include W in the synchronization
	3	Include T in the synchronization
	4	Include C in the synchronization
	5	Include D in the synchronization
	6	Disable FINS communications - 'Process-Active' status will be OFF
	7	FINS communication is done over Profinet
	8-9	E banks included in the FCS calculation and synchronization (max 3)

Addres	Bit	Description
	10	HMI can only write to Active PLC - used for manual changeover
	11	Restarts IOC if problems detected
	12-15	Number of CIO blocks (512 words/block) in synchronization (0 -> 10 (max))

Notes.

The network redundancy is based on the MRP protocol as defined by the PROFINET Organisation. Functionality is according to this specification.

The Redundancy FB is published 'as is' and must be used as an example for IO Controller Redundancy. Changes to the functionality can be made freely. However it is advised to make first a risk analysis of the application and then test accordingly.