U SCIENCE TECH
FACULTAT DE CIÈNCIES
I TECNOLOGIA
UVIC-UCC

Annexa del treball de Fi de Grau

Connectivitat sense fils en sistemes automatitzats

Dani Fàbrega Colomer

Grau en mecatrònica

Tutor/a: Juli Ordeix

Vic, Juny de 2017

Índex

U SCIENCE TECH
FACULTAT DE CIÈNCIES I TECNOLOGIA
UVIC-UCC

A1 PLC del control de qualitat

A1.1 Configuració del PLC

A continuació en la Figura 1.1 es detallen tots els punts importants pel que fa la configuració del PLC. Com serà l'adreça IP, el nom d'equip i les marques del sistema.

Una vegada afegit tot el hardware disponible es configura la seva adreça IP dins la xarxa així com el nom d'equip que pot modificar-se o deixar el de defecte.

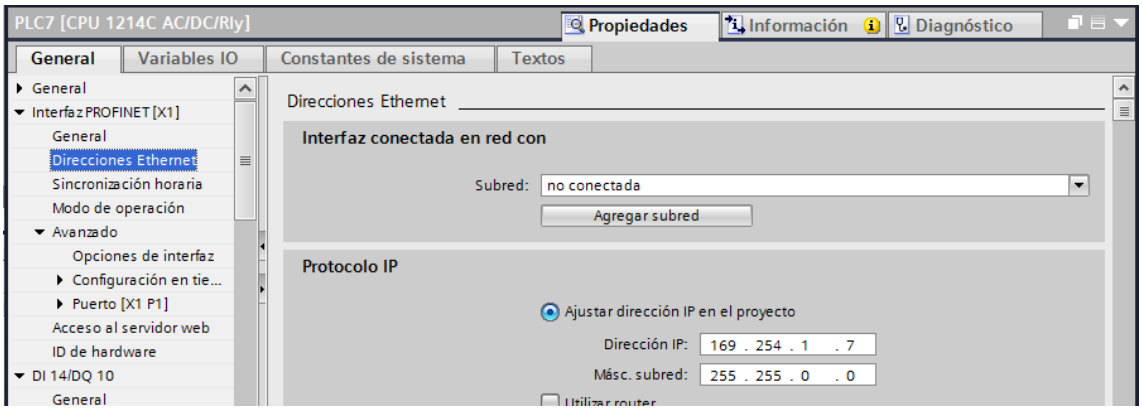


Figura 1.1 - Adreça IP

Per tenir el webServer activat i poder veure les dades a través del navegador cal fer-ho tal i com la Figura 1.2.

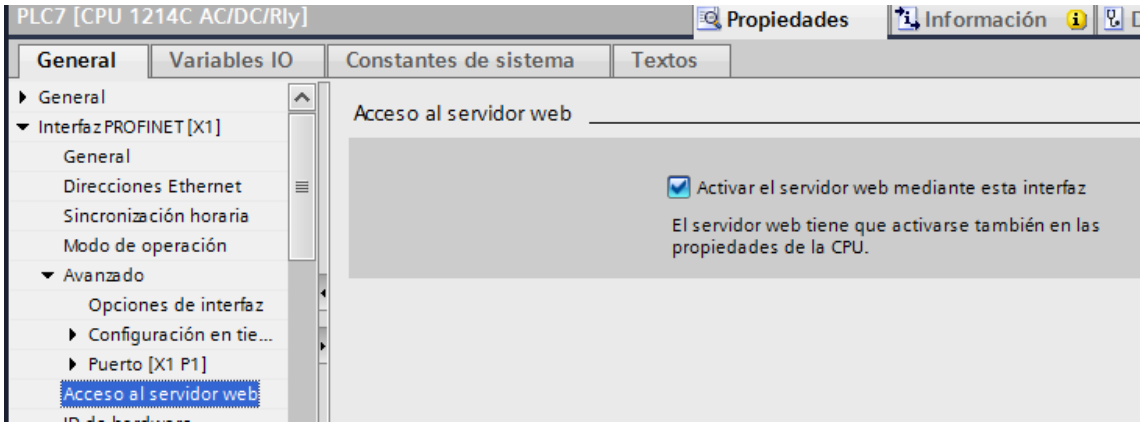


Figura 1.2 - Activació del servidor web

SCIENCE TECH
FACULTAT DE CIÈNCIES I TECNOLOGIA
UVIC-UCC

L'activació de les marques del sistema tant per al First Scan com per marques cícliques que serveixen per a la transferència de dades s'activen segons la Figura 1.3.

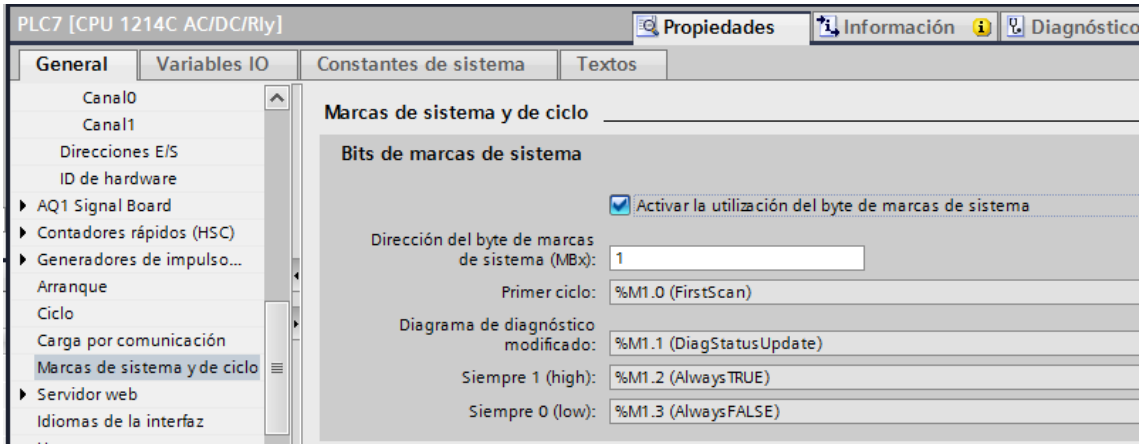


Figura 1.3 - Activació de les marques de sistema

Activació del servidor web en tots els mòduls com la Figura 1.4.

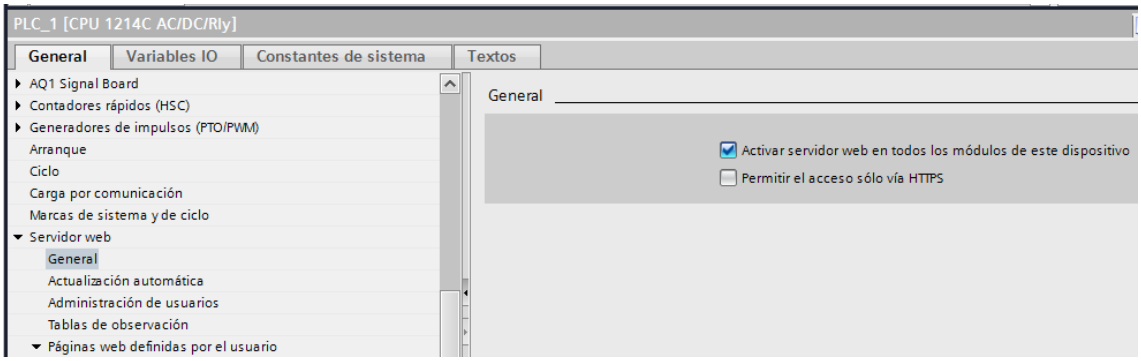


Figura 1.4 - Activació del servidor web en tots els móduls

U SCIENCE TECH
FACULTAT DE CIÈNCIES I TECNOLOGIA
UVIC-UCC

A2 Variador de freqüència del control de qualitat

A2.1 Configuració inicial

És molt important que al afegir el hardware al variador s'introdueixi en versió v6.0 tal i com diu l'enunciat i a més que el seu nom sigui "Var_1" com mostra la Figura 2.2 ja que d'una altra manera no es connectaria amb el PLC. Amb aquestes característiques el variador es connectarà amb qualsevol PLC que s'hagi configurat amb el Telegrama Standard 1 i tingui una IP 169.254.1.xxx (per exemple la 169.254.1.2 com es veu a la Figura 2.1). Això ho farà gràcies a que els variadors prioritzen el nom del dispositiu i com a segona opció l'adreça IP

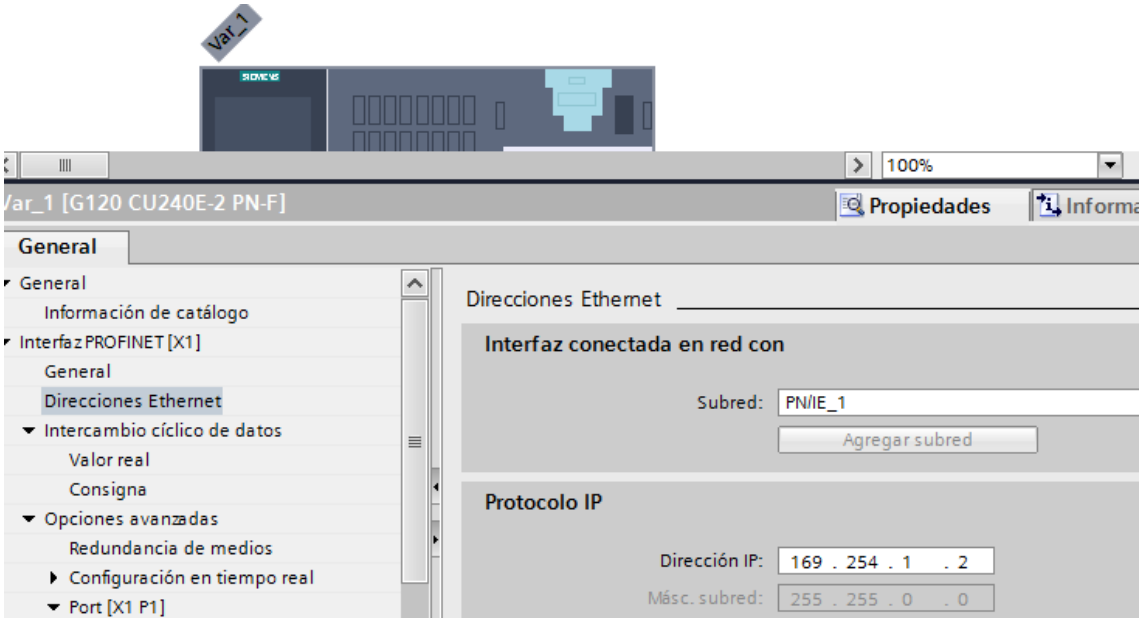


Figura 2.1 - Configuració de la IP del variador

Figura 2.2 - Configuració del nom del variador

A2.2 Configuració del variador a la xarxa

També, una vegada instal·lat el nou hardware a la xarxa i tenint la connexió assignada amb el 1200 cal treure la connexió ressaltada per tal que quedi com la Figura 2.3 següent:

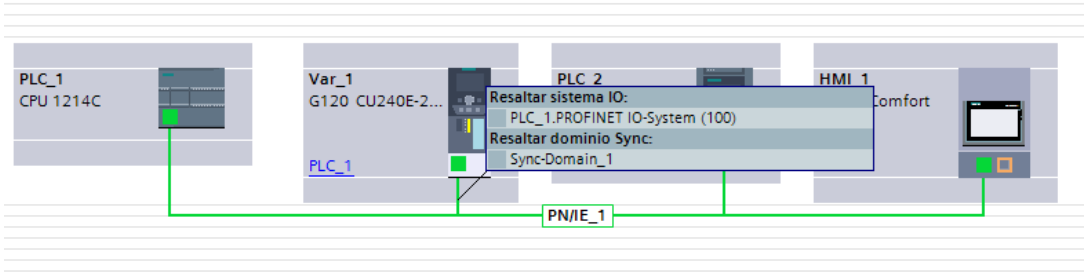


Figura 2.3 - Configuració de la xarxa complerta

En un principi queda una connexió ressaltada però només cal desactivar el clip en l'apartat "Resaltar sistema IO"

A2.3 Fonamentació teòrica del telegrama

Els telegrames tenen l'estructura de la Figura 2.4 següent:

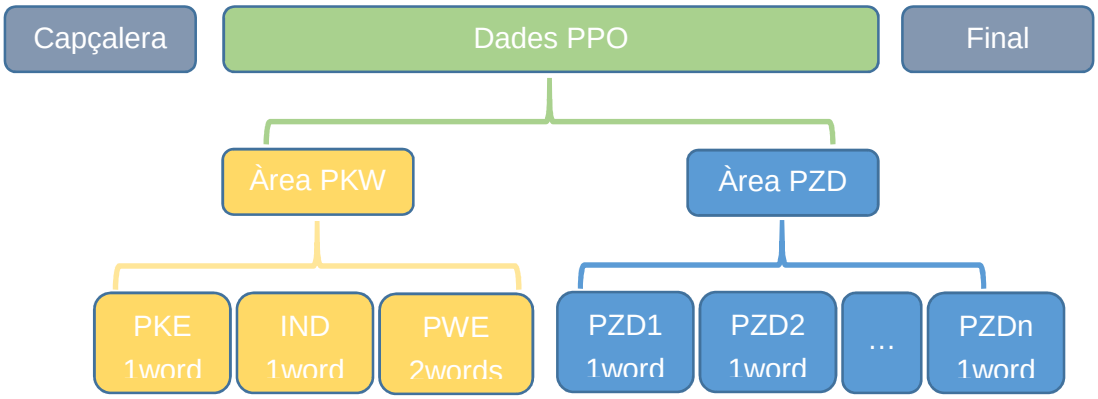


Figura 2.4 - Esquema del telegrama

A2.3.1 Paràmetres de l'objecte de dades del procés (PPO)

L'estructura de dades pel canal cíclic del PLC està definit pel perfil. Utilitzant el PPO el mestre accedeix als esclaus de manera cíclica.. Aquesta estructura de dades es divideix en dues zones. La zona PKW i la zona PZD (veure Figura 2.4 - Esquema del telegrama). Gràcies a aquesta divisió es poden separar ja que normalment la zona PKW és més lenta que la zona PZD.

2.3.1.1 Àrea PKW, paràmetres del valor d'identificació o també anomenat identificador del paràmetre

El canal de paràmetres està composat per 4 paraules. En aquesta zona es poden visualitzar i modificar cada un dels paràmetres del convertidor, per exemple els valors de límits mínim i màxim. La zona consta de com a mínim 4 paraules:

- PKE : identificador del número de paràmetre

SCIENCE TECH
FACULTAT DE CIÈNCIES I TECNOLOGIA
UVIC-UCC

- IND : índex de paràmetre i el tipus de petició (lectura o escriptura)
- PWE : valor del paràmetre. Pot ocupar 1 o 2 paraules.

2.3.1.1.1 PKE

L'identificador de paràmetre PKE sempre és un valor de 16 bits que conté:

- AK : Identificador de servei o resposta. Va del bit 12 al 15 i és possible que existeixin identificadors de servei per cada tipus de convertidor.
- SPM : El bit 11 s'utilitza com bit d'activació (toggle/canvi d'estat) dels avisos espontanis en la transferència dels paràmetres.
- PNU : Els bits del 0 al 10 contenen el numero del paràmetre desitjat.

2.3.1.1.2 IND

En la comunicació cíclica, l0index de paràmetre conté el subíndex en el byte més alt. El byte de menys pes no està definit i cada convertidor el pot assignar pel que desitgi

Al realitzar la elaboració d'un paràmetre, en el subíndex se li assigna un índex.

2.3.1.1.3 PWE

La transferència del valor del paràmetre sempre es realitza com a doble paraula. En un telegrama PPO només es pot transferir el valor d'un paràmetre.

2.3.1.1.4 Perfils de telegrames definits

Existeixen els perfils ja definits PROFIdrive V2.0 amb 5 tipus PPO (veure Figura 2.5), els quals es diferencien per la presència o no de zona PKW, o bé per la longitud de la zona PZD:

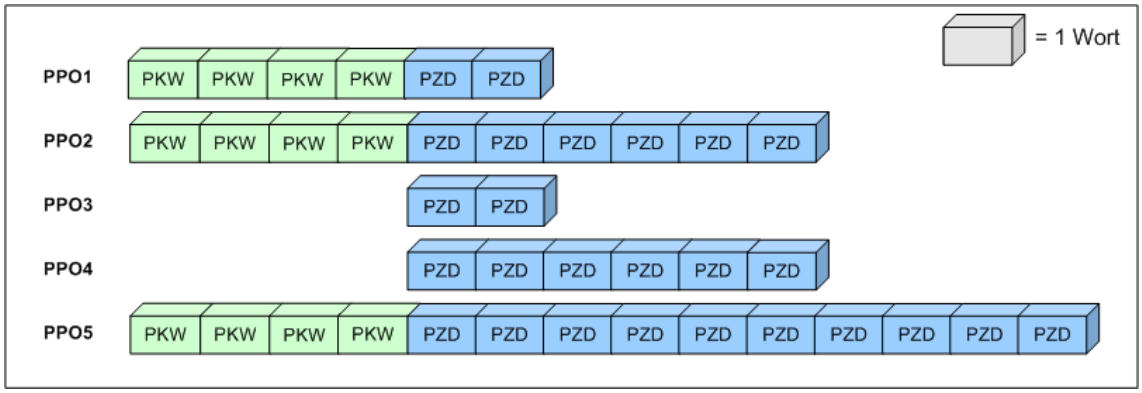


Figura 2.5 - Perfils de telegrama

U SCIENCE TECH
FACULTAT DE CIÈNCIES I TECNOLOGIA
UVIC-UCC

A2.4 Configuració del telegrama

La configuració del telegrama al variador es fa segons la Figura 2.6.

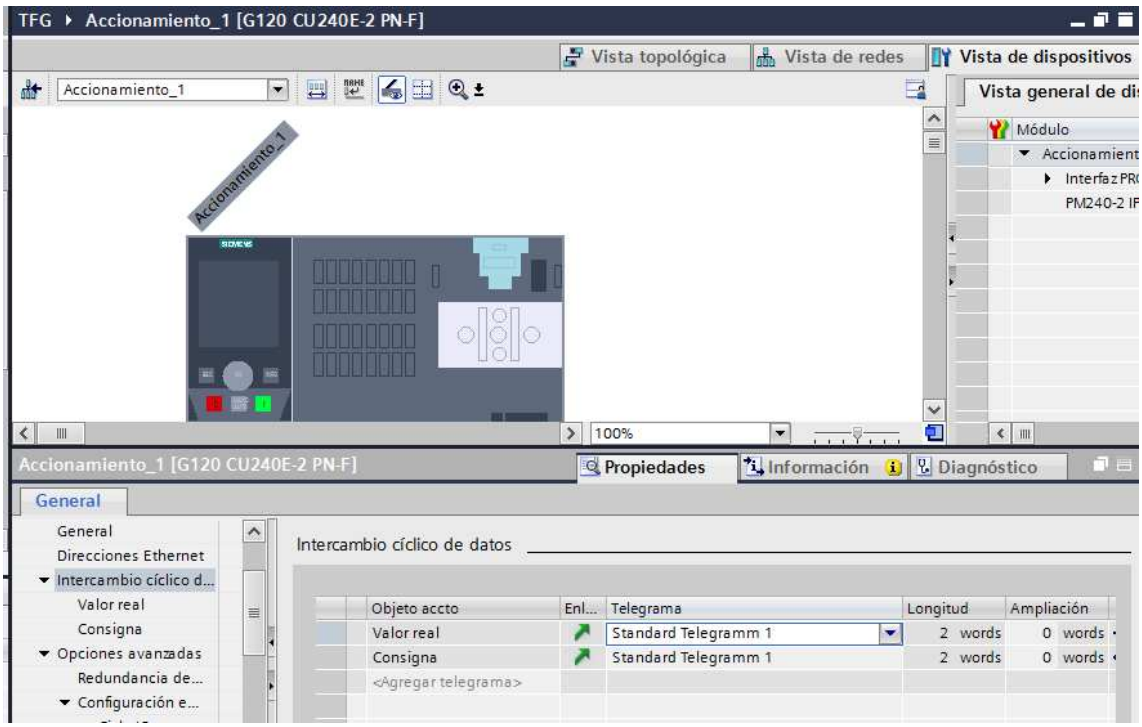


Figura 2.6 - Configuració de l'intercanvi de dades mitjançant telegrama

U SCIENCE TECH
FACULTAT DE CIÈNCIES
I TECNOLOGIA
UVIC-UCC

Els telegrames disponibles per al variador són els següents i es programa en el numero de paràmetre p0922:

- 1: Telegrama estàndard 1, PZD-2/2 (ajust de fàbrica)
- 20: Telegrama estàndard 20, PZD-2/6
- 350: Telegrama SIEMENS 350, PZD-4/4
- 352: Telegrama SIEMENS 352, PZD-6/6
- 353: Telegrama SIEMENS 353, PZD-2/2, PKW-4/4
- 354: Telegrama SIEMENS 354, PZD-6/6, PKW-4/4
- 999: Ampliació de telegrames i modificació de les senyals

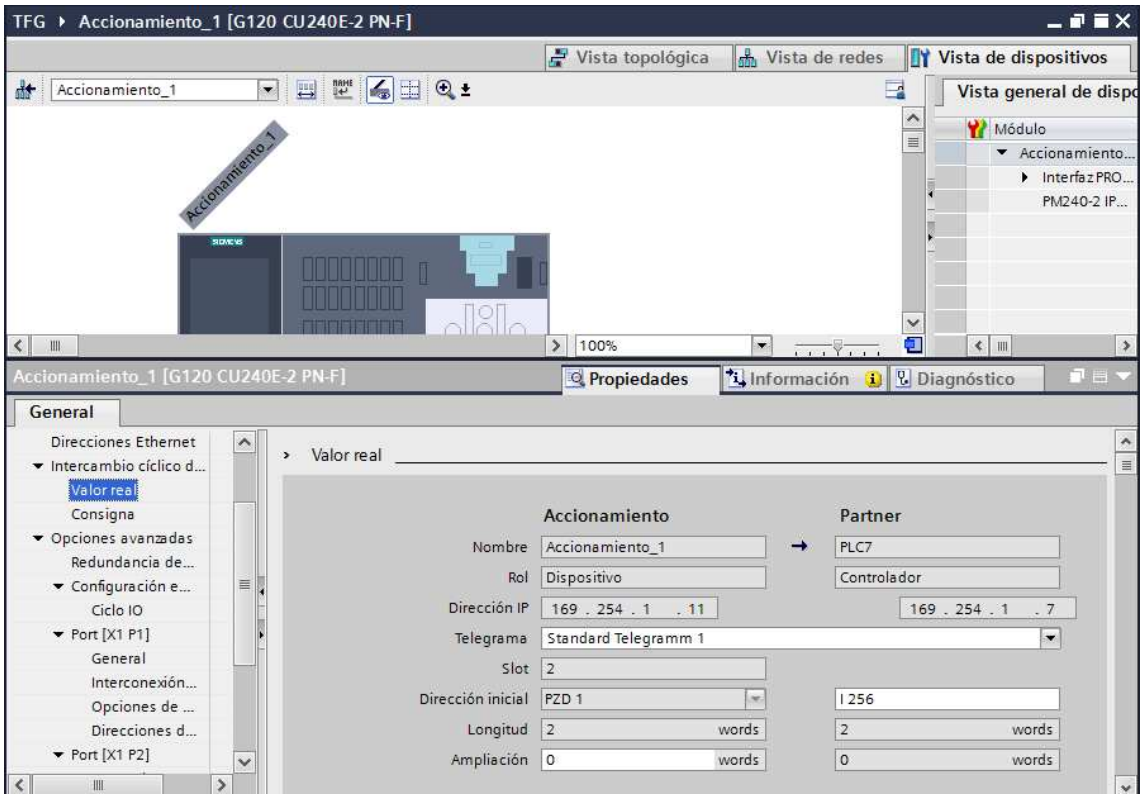


Figura 2.7 - Configuració del telegrama entre els dos dispositius si hi ha la xarxa configurada

Ja només quedarà definir les paraules en les següents adreces que es veuen a la Figura 2.7:

- QW256 – paraula de control
- QW258 – Consigna de velocitat
- IW256 – Paraula d'estat
- IW258 – Velocitat real

U SCIENCE TECH
FACULTAT DE CIÈNCIES I TECNOLOGIA
UVIC-UCC

Cal però parar atenció a la direcció inicial mostrada a la Figura 2.8, ja que aquestes són les que vénen per defecte però l'adreça pot ésser una altra si aquesta part de memòria ja està assignada.

Figura 2.8 - Direcció inicial del telegrama

U SCIENCE TECH
FACULTAT DE CIÈNCIES
I TECNOLOGIA
UVIC-UCC

Es configura l'apartat "Asistente de puesta en marcha" per ajustar el tipus de motor (asíncron). El control quadràtic del variador. I el reconeixement del mateix motor. Ho pot fer tant girant el motor com aquest parat. Per activar-ho veure la Figura 2.9.

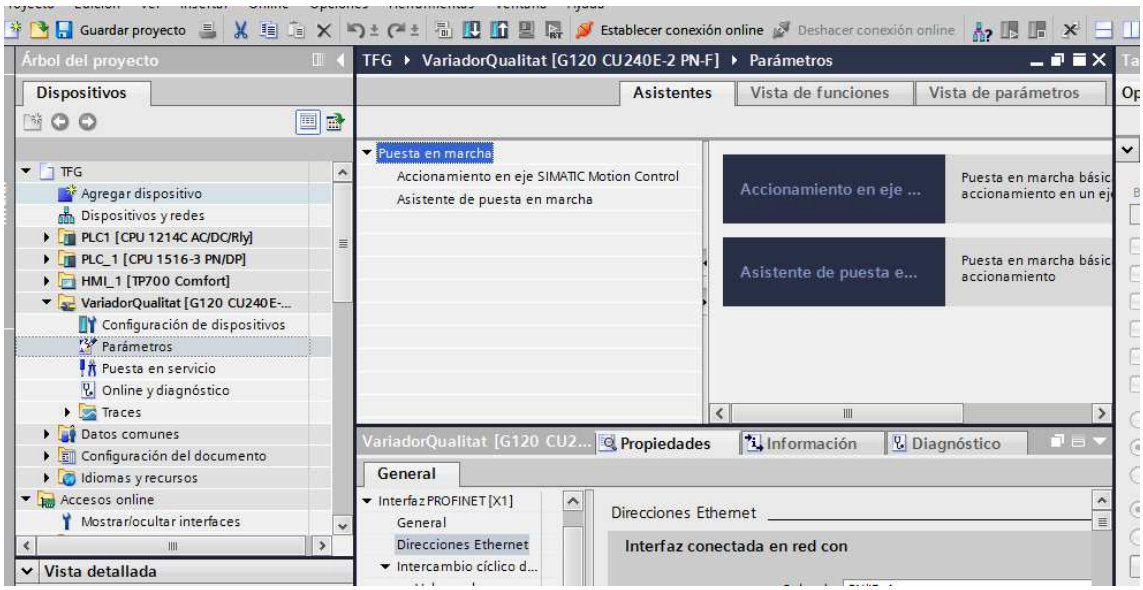


Figura 2.9 - Assistente de puesta en marcha

El valor de les paraules a enviar ho trobem a la Taula 2.1 i cal tenir present que el Bit0 és el de menys pes i el Bit15 el de més pes.

Palabra de mando 1 (STW1)

Palabra de mando 1 (bits 0 ... 10 según perfil PROFIdrive y VIK/NAMUR, bits 11 ... 15 específicos del convertidor).

Bit	Significado		Explicación	Interconexión de señales en el convertidor
	Telegrama 20	Resto de telegramas		
0	0 = DES1		El motor frena con el tiempo de deceleración p1121 del generador de rampa. El convertidor desconecta el motor durante la parada.	p0840[0] = r2090.0
	0 → 1 = CON		El convertidor pasa al estado "Listo para el servicio". Si además el bit 3 = 1, el convertidor conecta el motor.	
1	0 = DES2		Desconectar inmediatamente el motor; a continuación se produce parada natural.	p0844[0] = r2090.1
	1 = Sin DES2		Se puede conectar el motor (orden CON).	
2	0 = Parada rápida (DES3)		Parada rápida: el motor frena hasta la parada con el tiempo de deceleración DES3 p1135.	p0848[0] = r2090.2
	1 = Sin parada rápida (DES3)		Se puede conectar el motor (orden CON).	
3	0 = Bloquear servicio		Desconectar inmediatamente el motor (suprimir impulsos).	p0852[0] = r2090.3
	1 = Habilitar servicio		Conectar el motor (habilitación de impulsos posible).	
4	0 = Bloquear GdR		El convertidor ajusta inmediatamente a 0 su salida del generador de rampa.	p1140[0] = r2090.4
	1 = No bloquear GdR		Es posible la habilitación del generador de rampa.	
5	0 = Detener GdR		La salida del generador de rampa permanece en el valor actual.	p1141[0] = r2090.5
	1 = Habilitar GdR		La salida del generador de rampa sigue a la consigna.	
6	0 = Bloquear consigna		El convertidor frena el motor con el tiempo de deceleración p1121 del generador de rampa.	p1142[0] = r2090.6
	1 = Habilitar consigna		El motor acelera con el tiempo de aceleración p1120 hasta alcanzar la consigna.	
7	0 → 1 = Confirmar fallos		Confirmar el fallo. Si todavía está presente la orden ON, el convertidor conmuta al estado "Bloqueo conexión".	p2103[0] = r2090.7
8,9	Reservado			
10	0 = Ningún mando por PLC		El convertidor ignora los datos de proceso del bus de campo.	p0854[0] = r2090.10
	1 = Mando por PLC		Mando a través del bus de campo; el convertidor adopta los datos de proceso desde el bus de campo.	
11	---[1]	0 = Inversión de sentido	Invertir la consigna en el convertidor.	p1113[0] = r2090.11
12	No utilizado			
13	---[1]	1 = Subir PMot	Aumentar la consigna almacenada en el potenciómetro motorizado.	p1035[0] = r2090.13
14	---[1]	1 = Bajar PMot	Reducir la consigna almacenada en el potenciómetro motorizado.	p1036[0] = r2090.14
15	CDS bit 0	Reservado	Conmutación entre ajustes para distintas interfaces de manejo (juegos de datos de mando).	p0810 = r2090.15

[1] Si se conmuta al telegrama 20 desde otro telegrama, se conserva la asignación del telegrama anterior.

Taula 2.1 - Relació dels bits per al telegrama de control

O també poden trobar-se a dins l'assistent segons mostren les dues figures següents (Figura 2.10 i Figura 2.11)

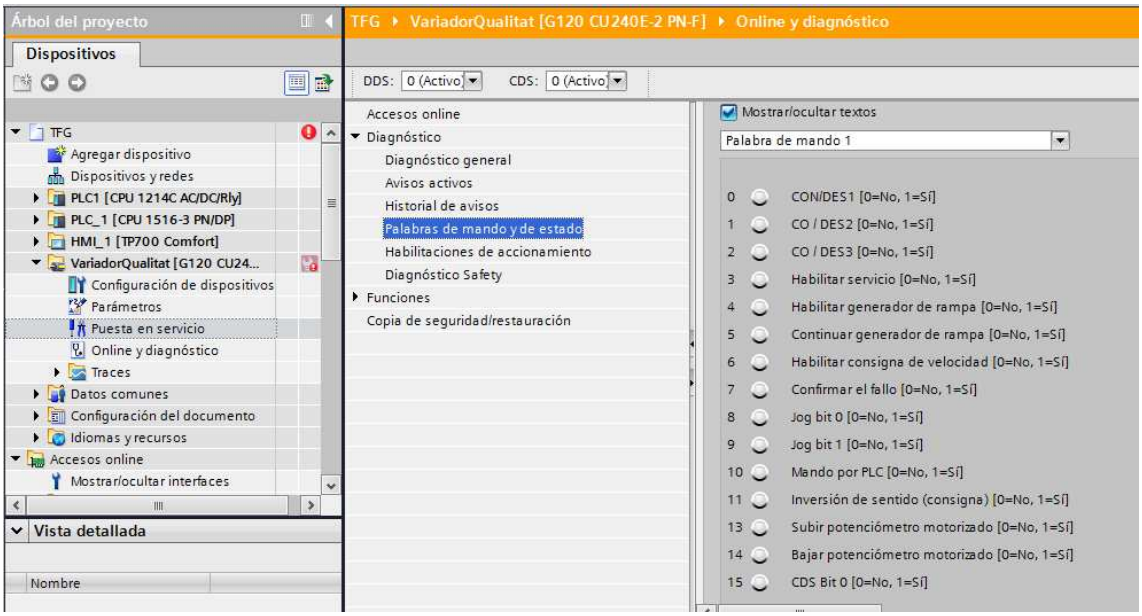


Figura 2.10 - Bits de la paraula de control amb l'assistent

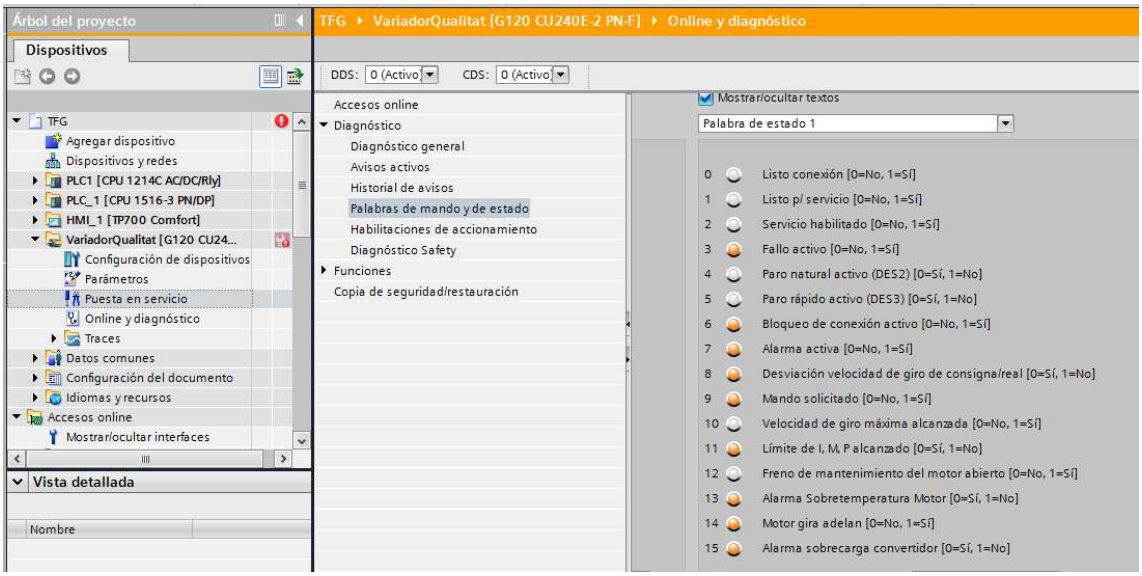


Figura 2.11 - Bits de la paraula d'estat amb l'assistent

Així doncs, els MOVE del telegrama seran amb els següents valors tal i com s'explica a la memòria:

0000010001111110 = 47E Habilitacions
0000010001111111 = 47F Ordre de marxa

La consigna de velocitat tant endavant com enrere haurà de calcular-se.

U SCIENCE TECH
FACULTAT DE CIÈNCIES I TECNOLOGIA
UVIC-UCC

Si a la pantalla de qualitat es vol veure si la cinta transportadora va endavant, endarrere, la quantitat de peces bones i dolentes i la velocitat de consigna i real a la que va el motor, han de visualitzar-se una sèrie de bits dintre la paraula d'estat, segons la Taula 2.2. Tanmateix, també es vol marcar amb un requadre vermell el variador si aquest té un fallo (I257.3), una alarma (I257.7), un excés de temperatura del motor (I256.5), excés de temperatura del convertidor(I256.7) s'haurà de fer un segment al programa per tal que al activar-se un d'aquests bits es marqui el requadre.

Palabra de estado 1 (ZSW1)

Palabra de estado 1 (bits 0 ... 10 según perfil PROFIdrive y VIK/NAMUR, bits 11 ... 15 específicos del convertidor).

Bit	Significado		Observaciones	Interconexión de señales en el convertidor
	Telegrama 20	Resto de telegramas		
0	1 = Listo para conexión		La alimentación está conectada, la electrónica inicializada y los impulsos bloqueados.	p2080[0] = r0899.0
1	1 = Listo para servicio		El motor está conectado (CON/DES1 = 1); ningún fallo está activo. Con la orden "Habilitar servicio" (STW1.3), el convertidor conecta el motor.	p2080[1] = r0899.1
2	1 = Servicio habilitado		El motor sigue la consigna. Ver la palabra de mando 1, bit 3.	p2080[2] = r0899.2
3	1 = Fallo activo		Existe un fallo en el convertidor. Confirmar fallo mediante STW1.7.	p2080[3] = r2139.3
4	1 = DES2 inactiva		La parada natural no está activada.	p2080[4] = r0899.4
5	1 = DES3 inactiva		La parada rápida no está activada.	p2080[5] = r0899.5
6	1 = Bloqueo de conexión activo		La conexión del motor es posible tras DES1 y CON.	p2080[6] = r0899.6
7	1 = Alarma activa		El motor permanece conectado; no se requiere confirmación.	p2080[7] = r2139.7
8	1 = Divergencia de la velocidad en el margen de tolerancia		Divergencia consigna-valor real en el margen de tolerancia.	p2080[8] = r2197.7
9	1 = Mando solicitado		Se solicita al sistema de automatización que asuma el mando del convertidor.	p2080[9] = r0899.9
10	1 = Velocidad de referencia alcanzada o superada		La velocidad es mayor o igual a la velocidad máxima correspondiente.	p2080[10] = r2199.1
11	0 = Límite de I, M o P alcanzado		Se ha alcanzado o superado el valor de comparación para la intensidad, el par o la potencia.	p2080[11] = r1407.7
12	---[1]	1 = Freno de mantenimiento abierto	Señal para la apertura o cierre de un freno de mantenimiento del motor.	p2080[12] = r0899.12
13	0 = Alarma Exceso de temperatura Motor		--	p2080[13] = r2135.14
14	1 = Motor gira a derecha		Valor real interno del convertidor > 0.	p2080[14] = r2197.3
	0 = Motor gira a izquierda		Valor real interno del convertidor < 0.	
15	1 = Indicación CDS	0 = Alarma Sobrecarga térmica Convertidor		p2080[15] = r0836.0/r2135.15

[1] Si se conmuta al telegrama 20 desde otro telegrama, se conserva la asignación del telegrama anterior.

Taula 2.2 - Bits de la paraula d'estat

A3 Webserver

Per poder veure dades remotament s'ha de fer una web amb html i activar els serveis del PLC. El primer que es fa per provar és connectar-se directament al PLC i veure el webserver que porta per defecte. Es pot comprovar com fins i tot es poden enumerar les variables ja definides i veure el seu valor.

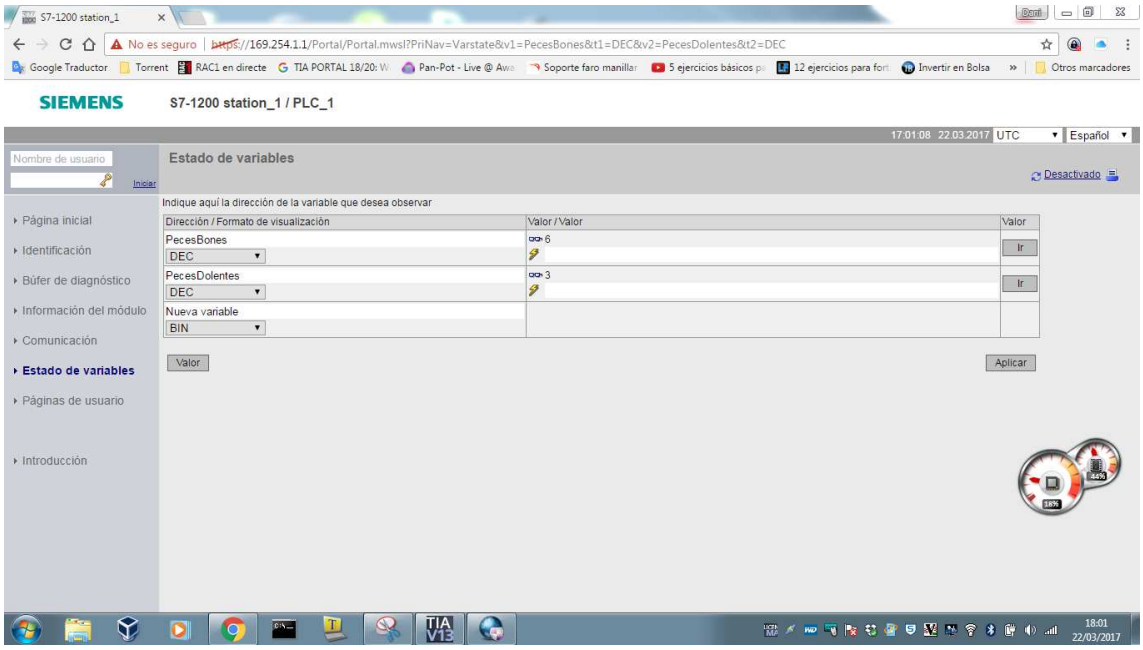


Figura 3.1 - Visualització de les variables entrades directament al PLC

Llavors és l'hora de començar a a crear una simple pàgina web mitjançant HTML. Una pel PLC del Trepant i una altra pel PLC de Qualitat

SCIENCE TECH
FACULTAT DE CIÈNCIES
I TECNOLOGIA
UVIC-UCC

A3.1 Programació de la pantalla web del Trepant

web Trepant: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
<html>
<head>

<meta http-equiv="content-type" content="text/html; charset=utf-8">
<!- Format del text de la pàgina ->

<meta http-equiv="Refresh" content="5">
<!- Refresc del navegador per actualitzar dades ->

<title> web Trepant </title>
<!- Titol del web a la pestanya del navegador ->

</head>

<body bgcolor=#f6d1d1>
<!- Color del fons de pantalla ->

<div align="center">
<img src= "logoUVic.jpg">
<!- logo UVic centrat ->

<H1> DADES DEL PLC DEL TREPANT HIDRAULIC </H1>
<!- Titol principal ->
</div>

<br>
<center> Numero de forats realitzats </center>
<div id="PecesBones" align="center">:=PecesBones:</div>
<!- variable PecesBones del PLC ->

<br>

<center> Forats a fer </center>
<div id="PecesBones" align="center">:=PecesBones:</div>
<!- variable PecesBones del PLC ->

<br>

<center> Xapes foradades </center>
<div id="PecesBones" align="center">:=PecesBones:</div>
<!- variable PecesBones del PLC ->

<br>

<form align="center">
<input type="submit" value="Reset contador">
<input type="hidden" name="ResetContador" value="0">
</form>

<div align="center">
<img src= "logoCoeva.jpg">
<!- logo Coeva centrat ->

</div>

</html>
```

Figura 3.2 - Codi html per a la pàgina del trepant

U SCIENCE TECH
FACULTAT DE CIÈNCIES
I TECNOLOGIA
UVIC-UCC

A3.2 Programació de la pantalla web del control de qualitat

web Qualitat: Bloc de notas

Archivo Edición Formato Ver Ayuda

```
<html>
<head>

<meta http-equiv="content-type" content="text/html; charset=utf-8">
<!- Format del text de la pàgina ->

<meta http-equiv="Refresh" content="5">
<!- Refresc del navegador per actualitzar dades ->

<title> web Qualitat </title>
<!- Títol del web a la pestanya del navegador ->

<body bgcolor=#BDBDBD>
<!- Fons de pantalla de color gris ->

<div align="center">
<img src= "logoUVic.jpg">
<!- logo UVic centrat ->

<title>LECTURA VARIABLES PLC de QUALITAT</title>
<!- Títol principal ->

</head>

<body>
<table style="border: 1px solid #454545;" align="center" cellspacing=10" cellpadding=10">
<!- Recuadre pel text ->

        <tr>
                <td COLSPAN=2>LECTURA DE DADES - PLC CONTROL DE QUALITAT</td>
                <td COLSPAN=2 style="padding-top:20px;" height="50"Lectura</td>
        </tr>
        <tr>
                <td> Peces Bones: </td>
                <td>:="PecesBones":</td>
                <!- variable PecesBones del PLC ->
        </tr>
        <tr>
                <td> Peces Dolentes: </td>
                <td>:="PecesDolentes":</td>
                <!- variable PecesDolentes del PLC ->
        </tr>

</table>

</body>

<div align="center">
<img src= "logoCoeva.jpg">
<!- logo Coeva centrat ->
</div>

</html>
```

Figura 3.3 - Codi html per la web del control de qualitat

A3.3 Configuració del WebServer al Tia Portal

Cal revisar que el WebServer estigui activat.

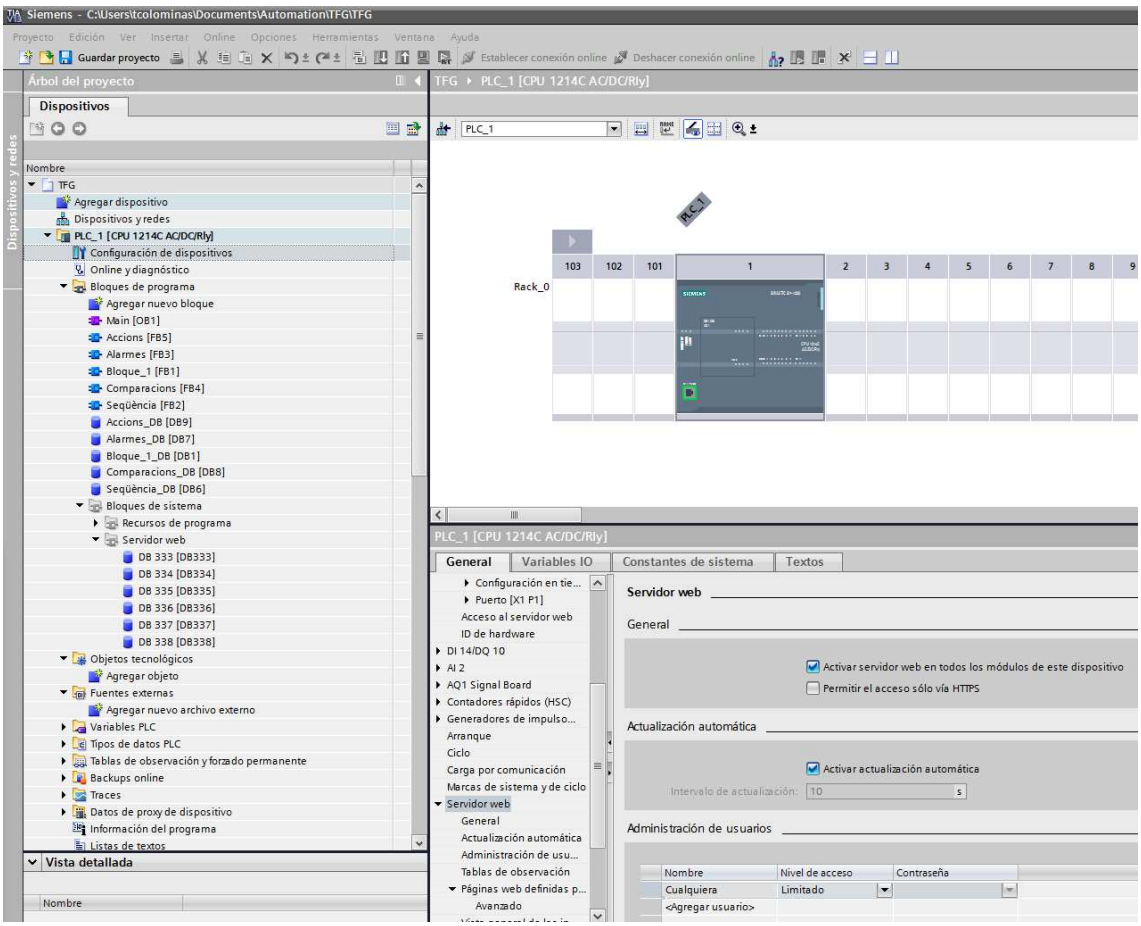


Figura 3.4 - Activació del webServer al plc de qualitat

També és molt important configurar l'administració dels ususaris ja que sinó, no es podrà accedir a les pàgines que volem.

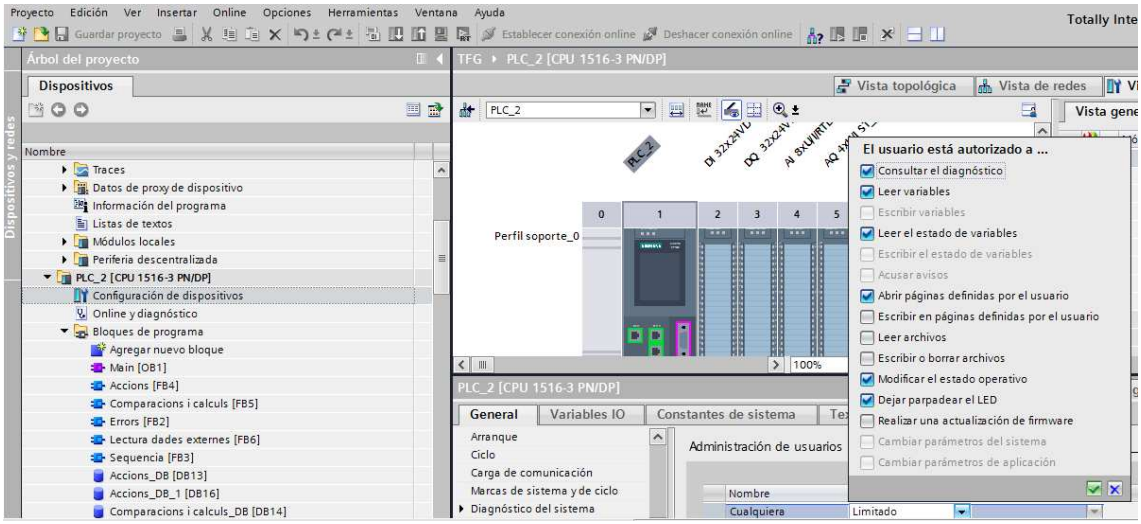


Figura 3.5 - Administració dels usuaris

U SCIENCE TECH
FACULTAT DE CIÈNCIES I TECNOLOGIA
UVIC-UCC

Seguidament a la pestanya de pagines web definides per l'usuari cal:

- Seleccionar la carpeta on s'ubiquen els arxius
- Seleccionar la pàgina d'inici
- Posar el nom per accés a la pàgina

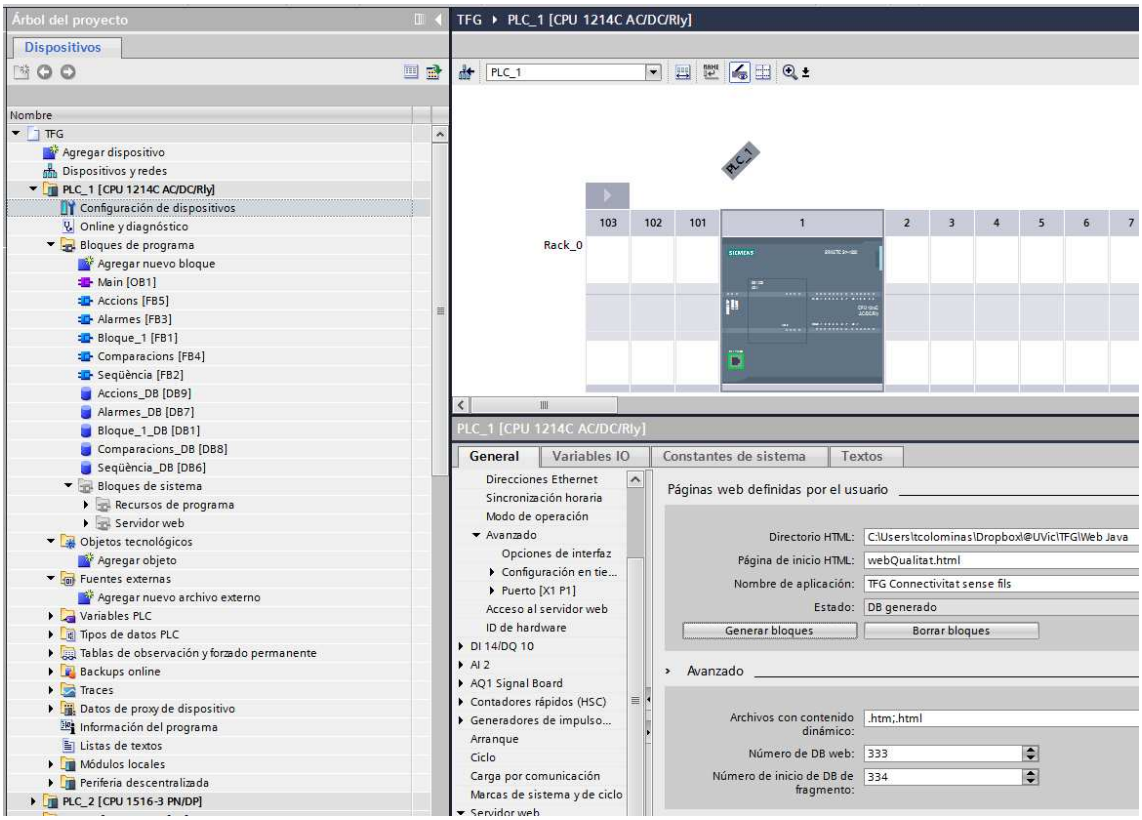


Figura 3.6 - Càrrega de la pàgina web al PLC

Finalment, clickar a "Generar bloques". En aquest punt es generen uns DB que fa servir el PLC per a les pàgines HTML, sempre que es vulgui actualitzar les pàgines s'hauràn de tornar a generar aquests DB i evidentment transferir al PLC. Un exemple dels DB generats es veu a continuació:

U SCIENCE TECH
FACULTAT DE CIÈNCIES
I TECNOLOGIA
UVIC-UCC

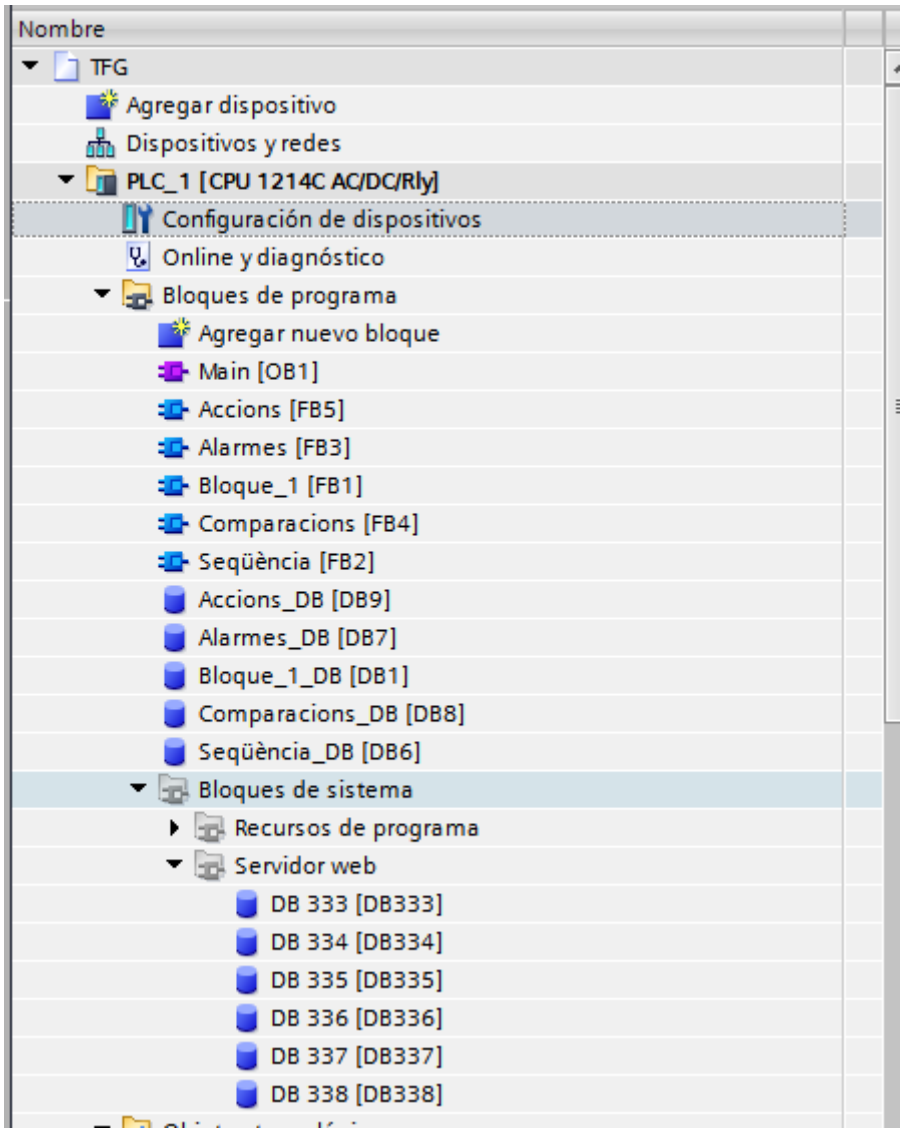


Figura 3.7 - Generació dels DB's a la web

Per tal que la pàgina d'exemple funcioni s'ha de fer una crida cíclica, per exemple en el OB1 de la funció www, on s'indica el DB inicial que s'ha generat:

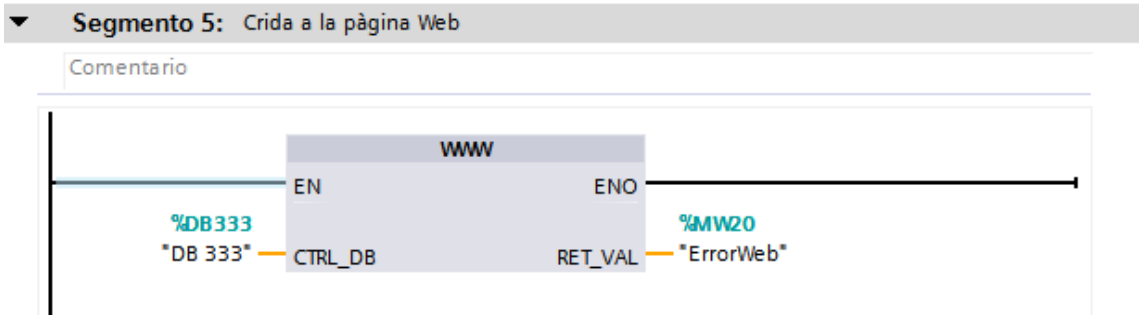


Figura 3.8 - Crida del DB inicial dins l'OB1

Finalment s'accedeix al PLC mitjançant la IP del mateix PLC, i a Páginas de usuario s'ha de veure l'enllaç a la pàgina amb el títol que se l'hi ha donat.

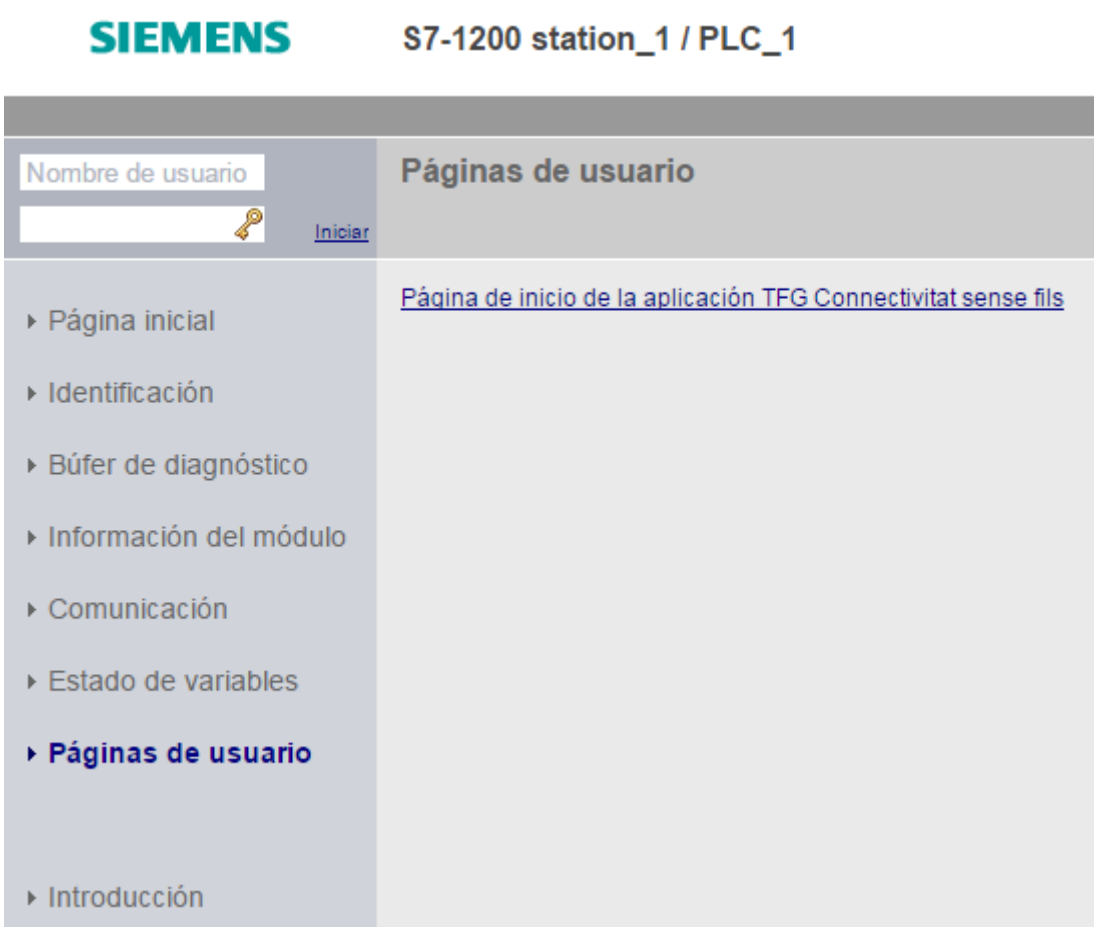


Figura 3.9 - Visualització de la pàgina web del PLC

El resultat en local podria ésser aquest:

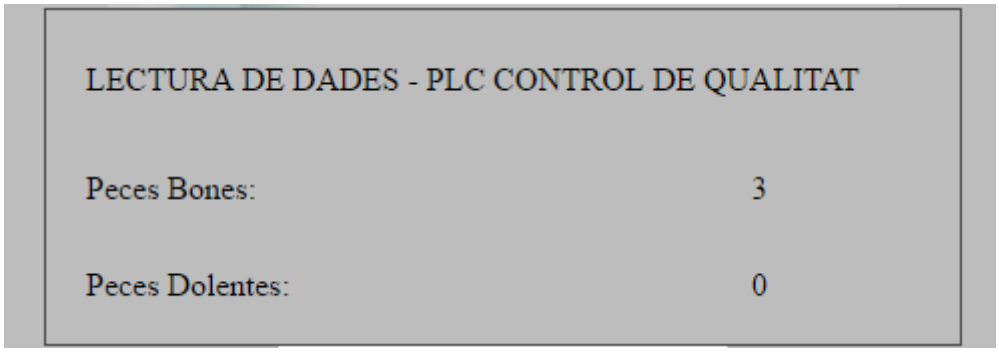


Figura 3.10 - Pàgina web de l'usuari visualitzada des del navegador

A4 ACCESS POINTS TP-LINK

A4.1 Configuració dels routers

Començo configurant el A-0501 com a punt d'accès (Access Point) on la seva funció és transformar la xarxa cablejada en una xarxa sense fils.

Connecto el cable de xarxa que va al PC en un port LAN i el cable que dona internet al port WAN. Tot i que en el TFG no necessitaré connexió a internet a través d'aquest punt.

Donat que no té els valors de fàbrica sinó està com a robot_UVic faig un reset mantinguent apretat el botó durant uns 8 segons aproximadament (fins que s'iluminen tots els leds del router). Una vegada reiniciat, entro a la IP 192.168.0.1 des del navegador

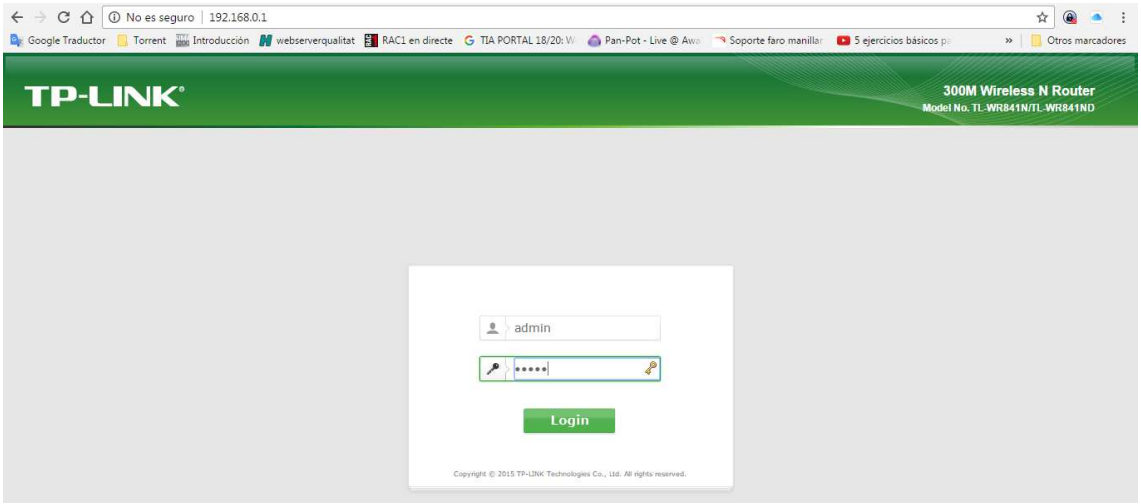


Figura 4.1 - Pàgina inicial dels routers TP_LINK

Es pot accedir amb admin als dos llocs.

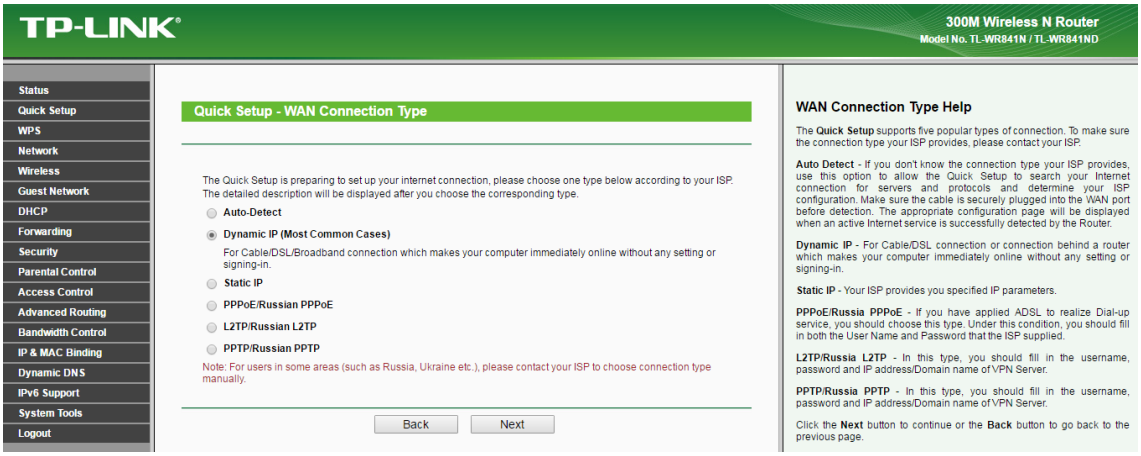


Figura 4.2 - IP dinámica

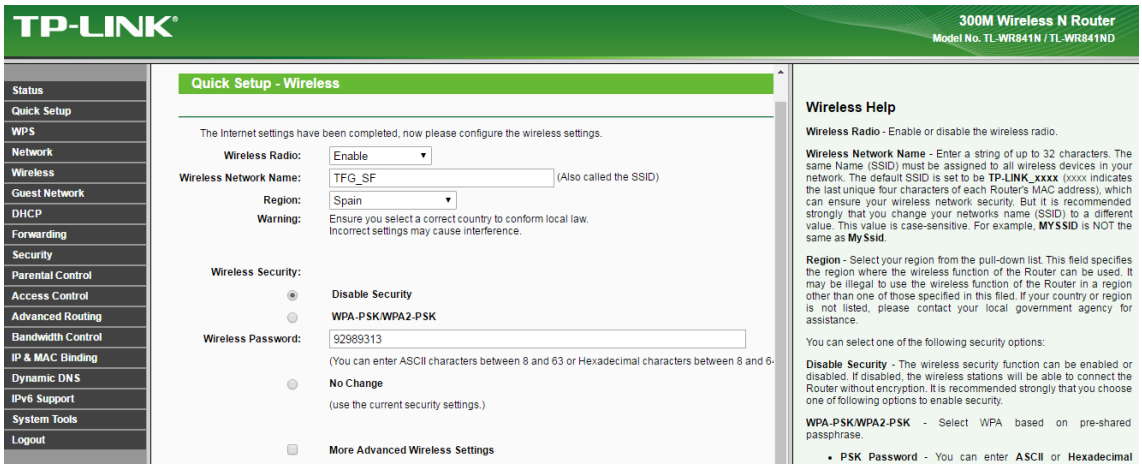


Figura 4.3 - Configuració del wifi

Finalment i per tal de poder tenir l'enllaç entre els dos routers, activo el "WDS Bridging" amb un canal fixe i entrant el SSID i la MAC de l'altre router:

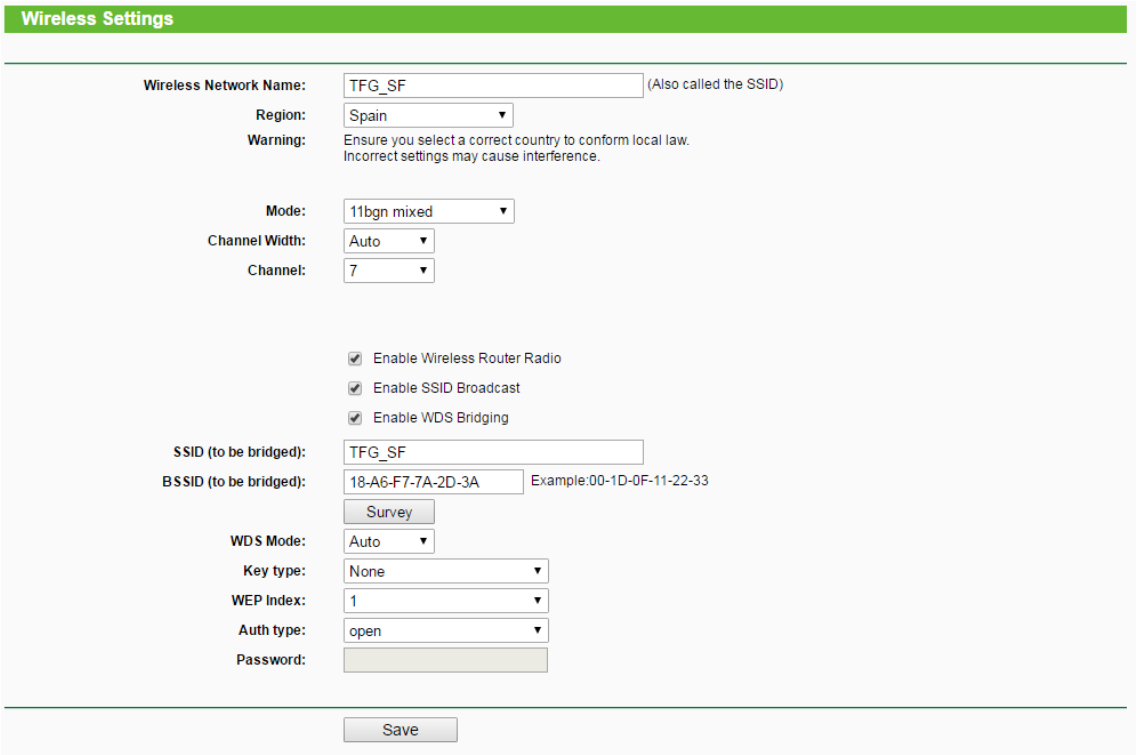
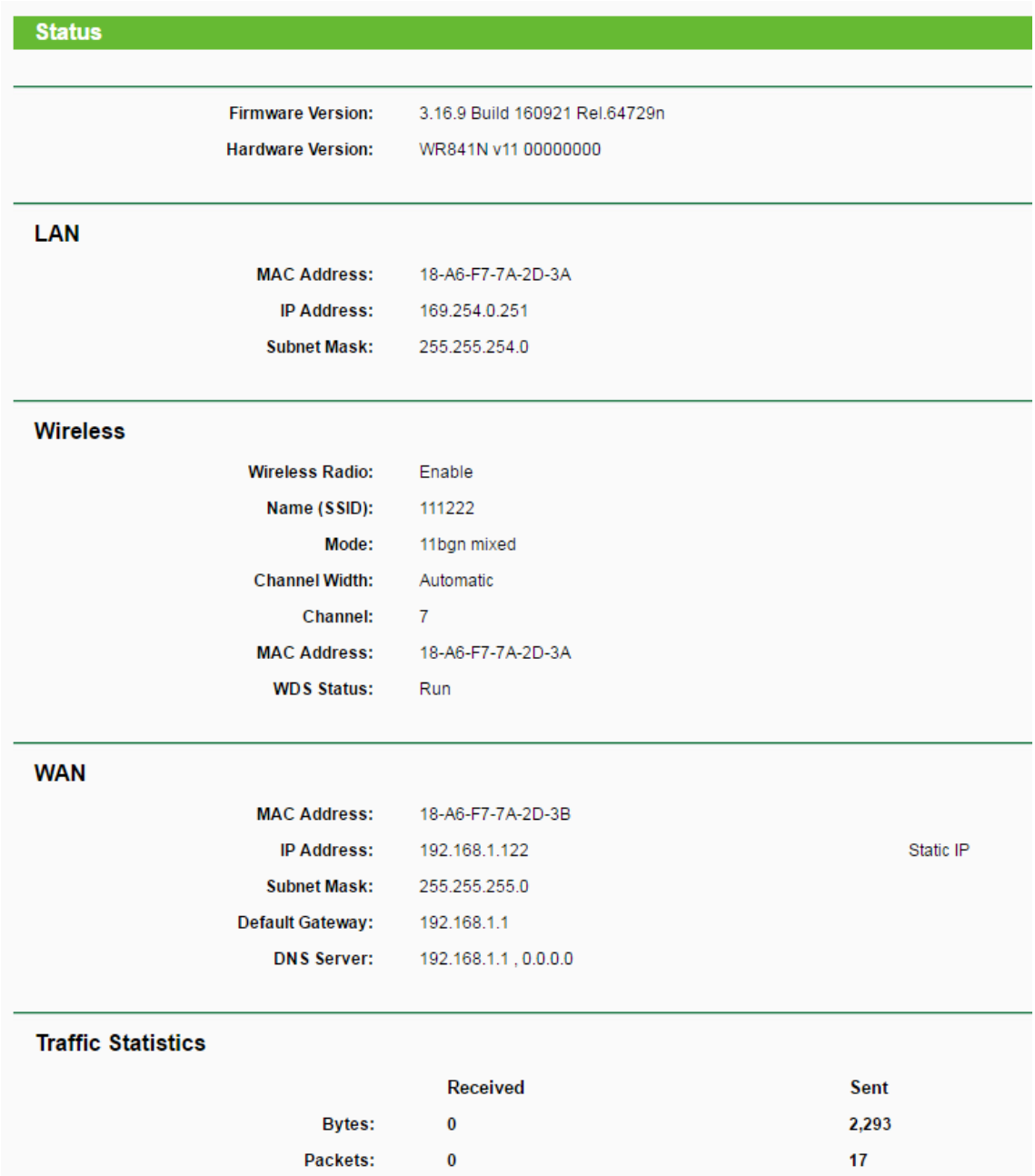


Figura 4.4 - Configuració del WDS Bridging

El resum de la configuració queda així:

Figura 4.5 - Resum de la configuració

A continuació, configuraré el A-0493 com a AP Client Router per tal que es connecti a la xarxa “TFG_SF” creada al A-0501 i ho transformi a una xarxa cablejada per al PLC de qualitat i el seu variador. Tot això ho faig posant una IP estàtica la xarxa WAN per evitar que entri en conflictes si agafés connexió a internet, el mateix canal que l’altra AP i finalment entrant el SSID i la MAC del A-0501 al “WDS Bridging”.Per últim, desactivo la DHCP ja que en qualsevol cas aquests routers han de gestionar les adreces IP.



A5 Instruccions GET I PUT

A5.1 Fonamentació teòrica

A5.1.1 Tipus de dades en els DB's

Els tipus de dades que ens podem trobar i definir dintre un DB són de dos tipus:

- Simples
- Compostes

Les dades simples son les següents:

- Bool: True/False
- Byte: B#16#A
- Word: W#16#432
- DWord: DW#16#12300
- INT: 124
- DINT: L#130000
- REAL: 0.45e+1
- S5TIME: S5T#2s
- TIME: T#1D5H
- DATE: D#2012-12-24
- TIME_OF_DAY:TOD#11:34:15
- CHAR: 'B'

S'ha de tenir en compte que l'assignació de memòria es fa per defecte amb paraules. Això implica per exemple si definim 3 bools s'ocuparan 2 bytes, si utilitzem un byte també s'ocuparan 2 bytes. Per tant, a l'hora de definir bools s'ha de definir molt bé la paraula fins a completar-la i deixant lliures els bits que no utilitzarem per a possibles nous usos.

Les dades compostes que es poden utilitzar són:

- DATE_AND_TIME: DT#12-12-24-11:34:1.0
- STRING: 'Hola mundo'
- ARRAY: Array[1..20]
- STRUCT
- UDT: UDT1

La utilització de les dades simples sé immediat però en el cas de les compostes s'ha de fer alguna consideració abans d'utilitzar-los:

- En el cas dels Strings (cadena de caràcters) s'haurà de definir la seva longitud de tal manera que la memòria reservada sigui major o menor segons definim com volem que sigui.
- Els arrays s'utilitzaran definint anteriorment la longituds de dades que tindran. Poden ser dades simples o compostes per exemple per altres estructures.
- Les estructures no són un tipus per elles soles ja que no emmagatzemen informació. Simplement, indica la forma en la que es guarden les dades. Per exemple, es pot crear un array de 10 posicions dins un STRUCT i dins seu emmagatzemar un enter i un string [18].
- Es poden inserir UDT ja definits amb les precaucions que ja s'han comentat anteriorment pel que fa a longituds. En la part de definició al introduir un UDT tan sols només veurem que en el DB es reserva la memòria que ocupa el UDT. Si es volen veure les variables internes a l'UDT haurem de posar-nos en mode visualització de dades.

A5.1.2 Obrir i realitzar crides al DB

Dins de qualsevol bloc que s'utilitza es poden realitzar crides al contingut dels DB. Així, podem carregar qualsevol valor que tingui tant sols fent una crida absoluta del tipus següent:

- U DB100.dbx0.0 per a carregar el valor del bit 0.0 del DB100
- L DB100.dbb0 per a carregar el byte 0 del DB100
- L DB100.dbw0 per a carregar la paraula 0 del DB100
- L db100.dbd0 per a carregar la doble paraula 0 del db100

A5.1.3 Tipus d'adreçaments

Els tipus d'adreçaments de DB són tres;

- Adreçament immediat:
- Adreçament directe
- Adreçament indirecte

Els dos primers, són fàcilment comprensibles:

- El direccionalment immediat és carregar directament el valor de l'operant (de qualsevol tipus) per exemple L 32.
- El direccionalment directe serà del tipus L MW10(on el valor del MW10 sigui el 32 anterior) és a dir, en la càrrega s'apunta directament al lloc de la memòria on està ubicat el valor que volem carregar.

5.1.3.1 Adreçament indirecte – Memòria i punters a àrea

Com s'ha comentat, es pot accedir a valors de la memòria d'una manera indirecta, pot esdevenir el cas que es vulgui saber el contingut d'una variable o àrea de memòria utilitzant una altra variable que es referirà a aquesta àrea de la que volem saber el seu valor.

Existeixen els següents tipus d'adreçaments indirectes:

- Adreçament Indirecte per Memòria amb Número
- Adreçament Indirecte per Memòria amb Punter d'Àrea
- Adreçament Indirecte per Registre i intra-àrea (àrea interna)
- Adreçament Indirecte per Registre i Inter-àrea (àrea creuada)

5.1.3.2 Adreçament indirecte per memòria

Dintre dels adreçaments indirectes per memòria amb número es pot utilitzar MW (o DW d'un DB) o MD (o DD d'un DB) per accedir:

- En format paraula: S'accedeix a temporitzadors, comptadors, s'obren DB i s'accedeix a FB i FC
- En format doble paraula: S'accedeix a dades del tipus bit, byte, paraula i doble paraula.

Format paraula – números (indexats)

És el més fàcil d'entendre: en un número enter (paraula) s'introdueix el valor del DB, FB, temporitzador o els que es vulgui.

Serveix per valors operants que estan indexats mitjançant un numero com ´son per exemple els comptadors. Per fer referència a ells, ens servim d'una variable que ja existeix en la llista d'elements.

Com a exemple, es llegeix el valor d'estat del comptador. On "ContaBones".CV és el valor del comptador de peces bones i "PecesBones" és la dada ubicada a dins el DB.

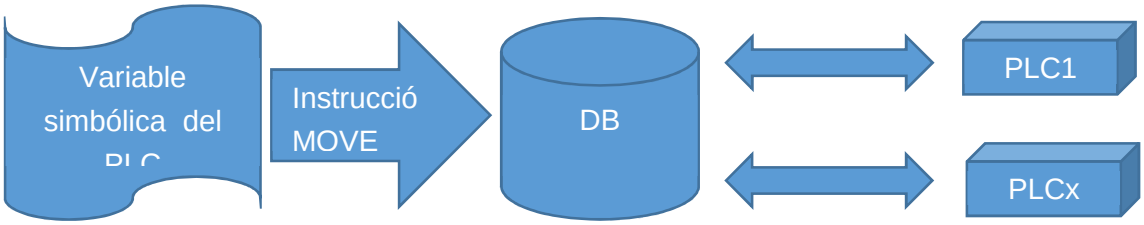


Figura 5.1 - Adreçament indirecte

Figura 5.2 – Adreçament indirecte

A5.1.4 Avantatges i inconvenients del client-servidor

Una disposició molt comuna són els sistemes multicapa en els que el servidor es descompon en diferents programes que poden ser executats per diferents processadors augmentant així el grau de distribució del sistema.

La xarxa client- servidor és una xarxa de comunicacions en la qual els clients estan connectats a un servidor, en el que

a disposició dels clients cada vegada que aquests són sol·licitats. Això significa que totes les gestions es realitzen i es concentren en el servidor, de manera que en ell es disposen els requeriments provinents dels clients que tenen prioritats, els arxius que són d'us públic i les que son d'us restringit, els arxius que són només de lectura i els que, pel contrari, poden ser modificats. Aquest tipus de xarxa pot utilitzar-se conjuntament en cas que s'estigui utilitzant en una xarxa mixta.

Avantatges de l'arquitectura client/servidor

Sol ésser recomanat, per a xarxes que requereixin un alt grau de fiabilitat. Les principals avantatges són:

- Recursos centralitzats: degut a que el servidor és el centre de la xarxa, pot administrar els recursos més comuns a tots els usuaris, per exemple: una base de dades centralitzada s'utilitzaria per evitar problemes provocats per dades contradictòries i redundants.
- Seguretat millorada: ja que la quantitat de punts d'entrada que permet l'accés a les dades no és important
- Administració al nivell del servidor: ja que els clients no juguen un paper important en aquest model, necessiten menys administració.
- Xarxa escalable: gràcies a aquesta arquitectura, és possible treure o posar clients sense afectar el funcionament de la xarxa i sense la necessitat de realitzar grans modificacions.

Desavantatges del model client/servidor

L'arquitectura client/servidor també té els següents desavantatges:

- Cost elevat: degut a la complexitat del servidor
- Un element crític: El servidor és l'únic element crític de la xarxa. Degut a que tota la xarxa està construïda al seu voltant.

És molt important també, tenir activat l'accés via comunicació mitjançant GET/PUT en els dos PLC's.

A5.1.5 Requisits per a l'ús de la instrucció GET o PUT:

- En les propietats de la CPU interlocutora, apartat "Protección" s'ha activat la funció "Permitir acceso vía comunicación PUT/GET del interlocutor remoto"
- Els blocs de dades els quals s'accedeix mitjançant la instrucció "GET" s'han creat amb el tipus de d'accés "estándar"
- Assegurar-se que les àrees definides pels paràmetres ADDR_i i SD_i es corresponen pel que fa a quantitat, longitud i tipus de dades.
- L'àrea que s'ha de llegar (paràmetre ADDR_i) no pot ser més gran que l'àrea d'emmagatzematge de dades (paràmetre RD_i).

A5.1.6 Estats de les funcions GET i PUT

La taula següent conté tota la informació d'errors i estats que poden ser retornats:

ERROR	STATUS (decimal)	Descripció
0	11	Advertència: La nova petició no té efecte ja que l'anterior encara no ha finalitzat.
0	25	La comunicació s'ha iniciat.
1	1	Problemes de comunicació. Per exemple, no s'ha trobat la CPU o connexió interrompuda perquè s'ha perdut la connexió a mitja transferència.
1	2	No hi ha confirmació de recepció per part del receptor. La resposta de la estació supera la longitud de dades màxim. La protecció contra accés està activada.
1	4	Error en els punters d'emmagatzemat de dades RD_i: Els tipus de dades dels paràmetres RD_i i ADDR_i no són compatibles entre sí La longitud de l'àrea RD_i es menor que la longitud de les dades a llegir del paràmetre ADR_i.
1	8	Error d'accés a la CPU interlocutora.
1	10	L'accés a la memòria d'usuari local no és possible.
1	20	• Número de peticions paral·leles excedit. • La petició es cridarà en una classe de baixa prioritat.

Taula 5.1 - Valors dels estats d'error del GET

A5.2 Configuració del DB i programació del GET o PUT

Per tal de poder fer transferència de dades amb el PLC mitjançant les instruccions programables GET i PUT és vital tenir activat l'accés amb comunicació:

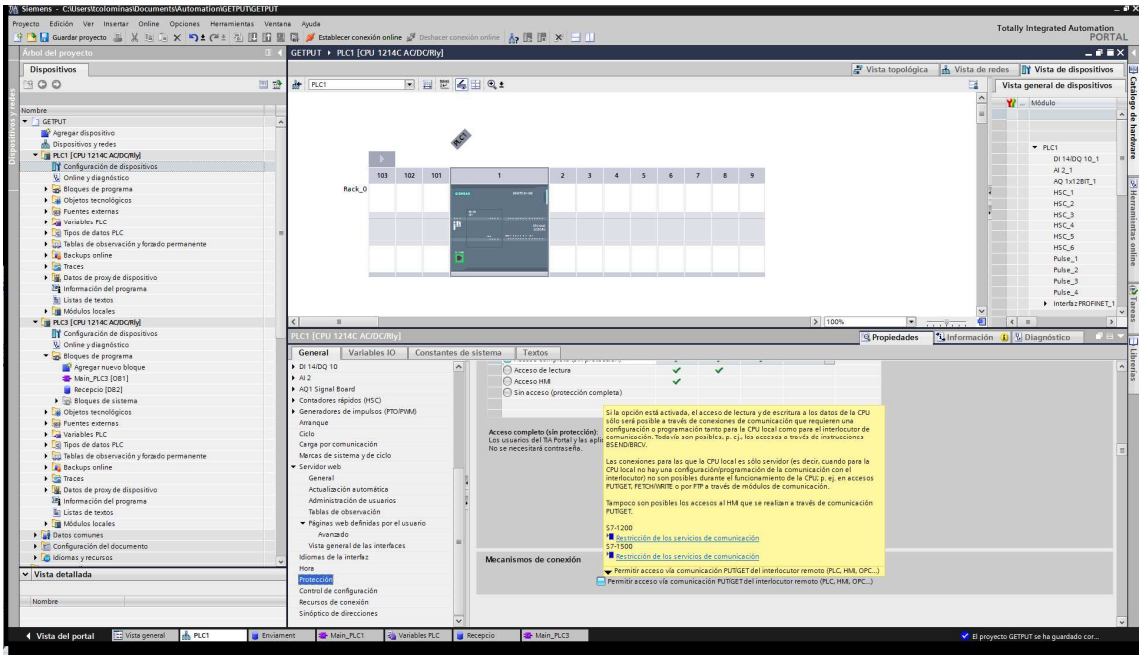


Figura 5.3 - Configuració de la comunicació amb GET/PUT

Seguidament el que es fa és crear un DB amb les dades a enviar. Des del primer moment de la transferència de dades ja es recomana convertir la paraula en un valor enter per tenir una lectura més fàcil del valor. Donat que el move és per una paraula de 16 bits ja es fa la conversió directa i el DB ja el tracta com a enter.

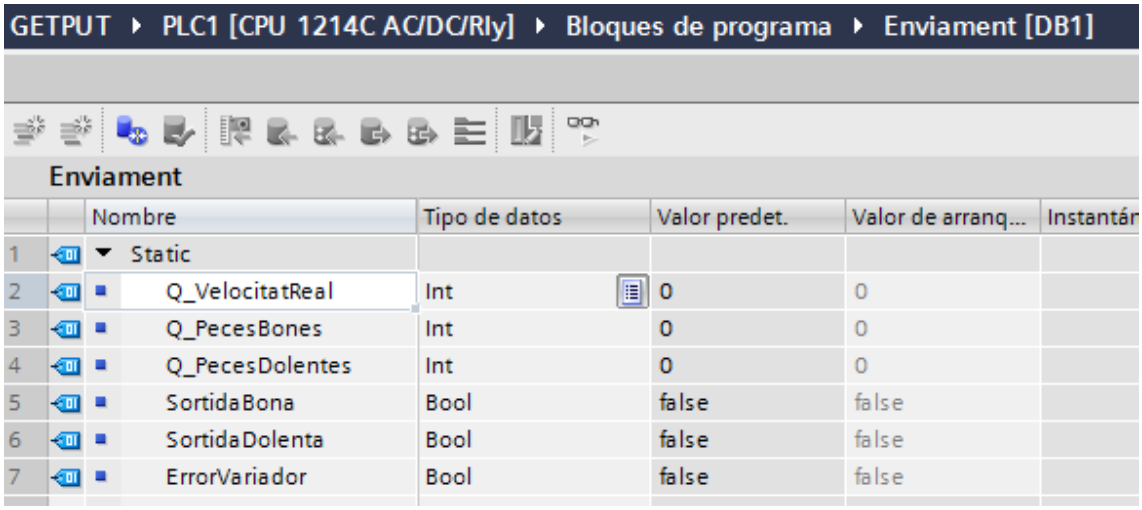


Figura 5.4 - Variables introduïdes al DB de Qualitat

En el PLC que es vol rebre les dades es fa un DB amb les dades també

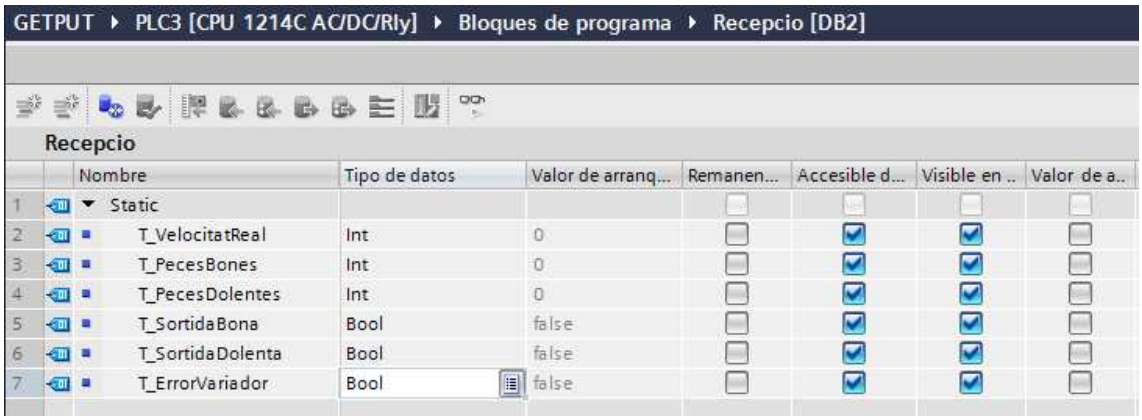


Figura 5.5 - Variables del DB al PLC del Trepant

A continuació i directament en l'OB1 es pot fer la funció PUT per tal d'enviar les dades al PLC de Qualitat

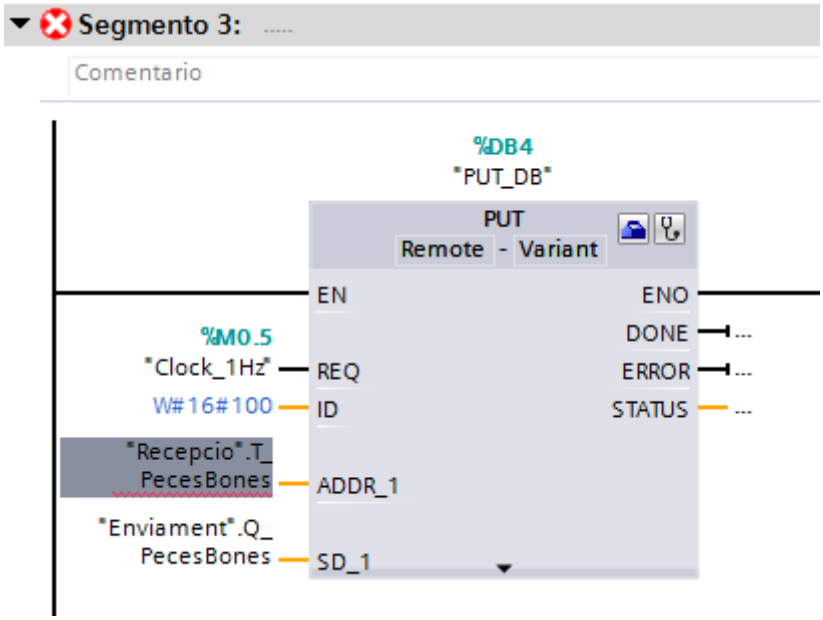


Figura 5.6 - Instrucció PUT

Aquí tinc un problema i és que els GETs i PUTs no poden ser en simbòlics, així que he de donar una dirección física. Per tal de poder saber la direcció he de fer el següent els els dos PLC's:

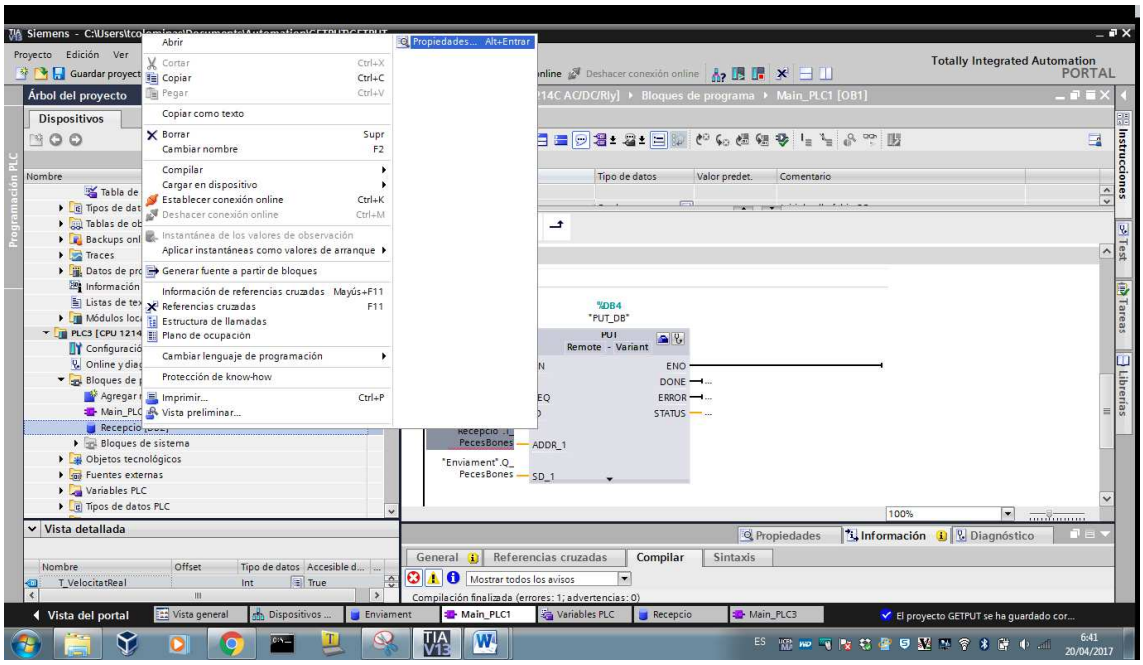


Figura 5.7 - Configuració de les propietats del DB

Desactivar el “Acceso optimizado al bloque” en els dos DB

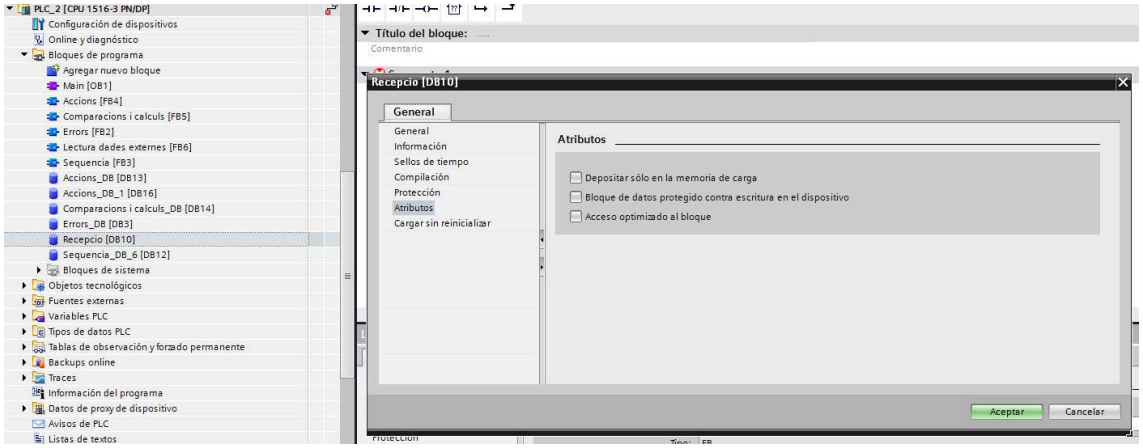


Figura 5.8 - Desactivació de l'accès optimitzat

D’aquesta manera, ja podem veure el direccionament de les dades.

U SCIENCE TECH
FACULTAT DE CIÈNCIES
I TECNOLOGIA
UVIC-UCC

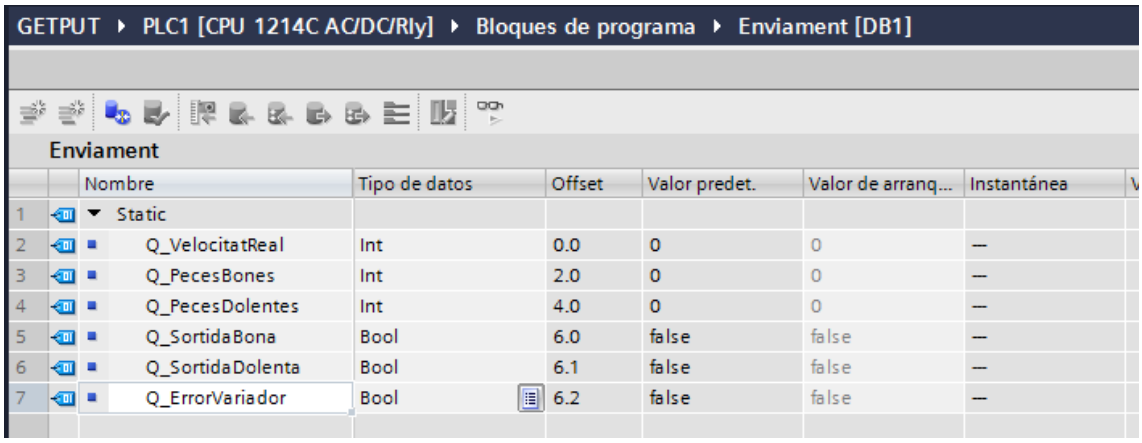
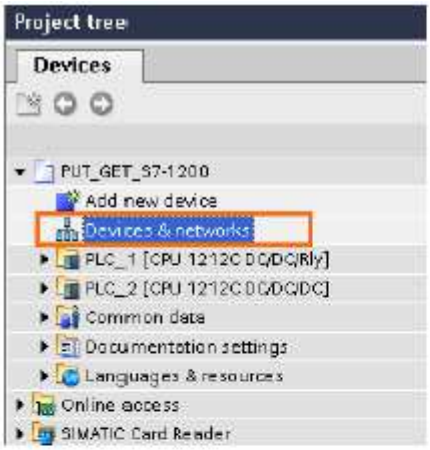


Figura 5.9 - Visualització de l'adreça física

Ara ja puc modificar el segment per tal de no tenir problemas a la compilació. En aquest moment, canvio el PUT al PLC de Qualitat per un GET al PLC del Trepant. D'aquesta manera en el cas de tenir varis PLC's no rebria dades massivament sinò que el PLC és qui llegeix quan pot al PLC de Qualitat.

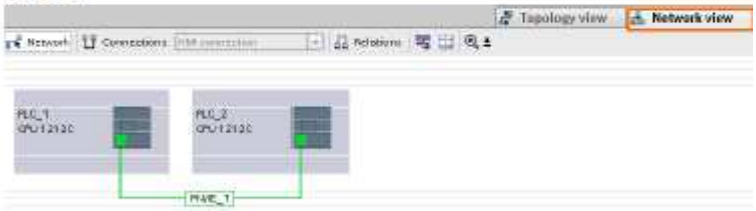
Per establir l'identificador (l'altre equip al que vull conectar-me), hem de fer un c"click" a la maleta (just al costat del "GET") allà escollirem el PLC que volem conectar-nos i ja es posarà automàticament l'identificador. Si només en tenim un ja sabem que sol començar per l'id W#16#100. Sinò també trobaríem aquest numero a la configuración de la xarxa:

U SCIENCE TECH
FACULTAT DE CIÈNCIES
I TECNOLOGIA
UVIC-UCC



In the hardware and network editor you select the Network view.

Figure 2-4



In the Network view area you open the "Connections" table. Here you take the connection number of the configured S7 connection.

Figure 2-5

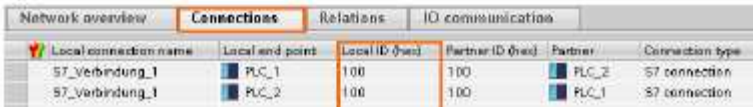


Figura 5.10 - Identificador del dispositiu de la xarxa

Una vegada ja està correcte, també aprofito la mateixa instrucció per llegir els tres valors enters que vull:

U SCIENCE TECH
FACULTAT DE CIÈNCIES
I TECNOLOGIA
UVIC-UCC

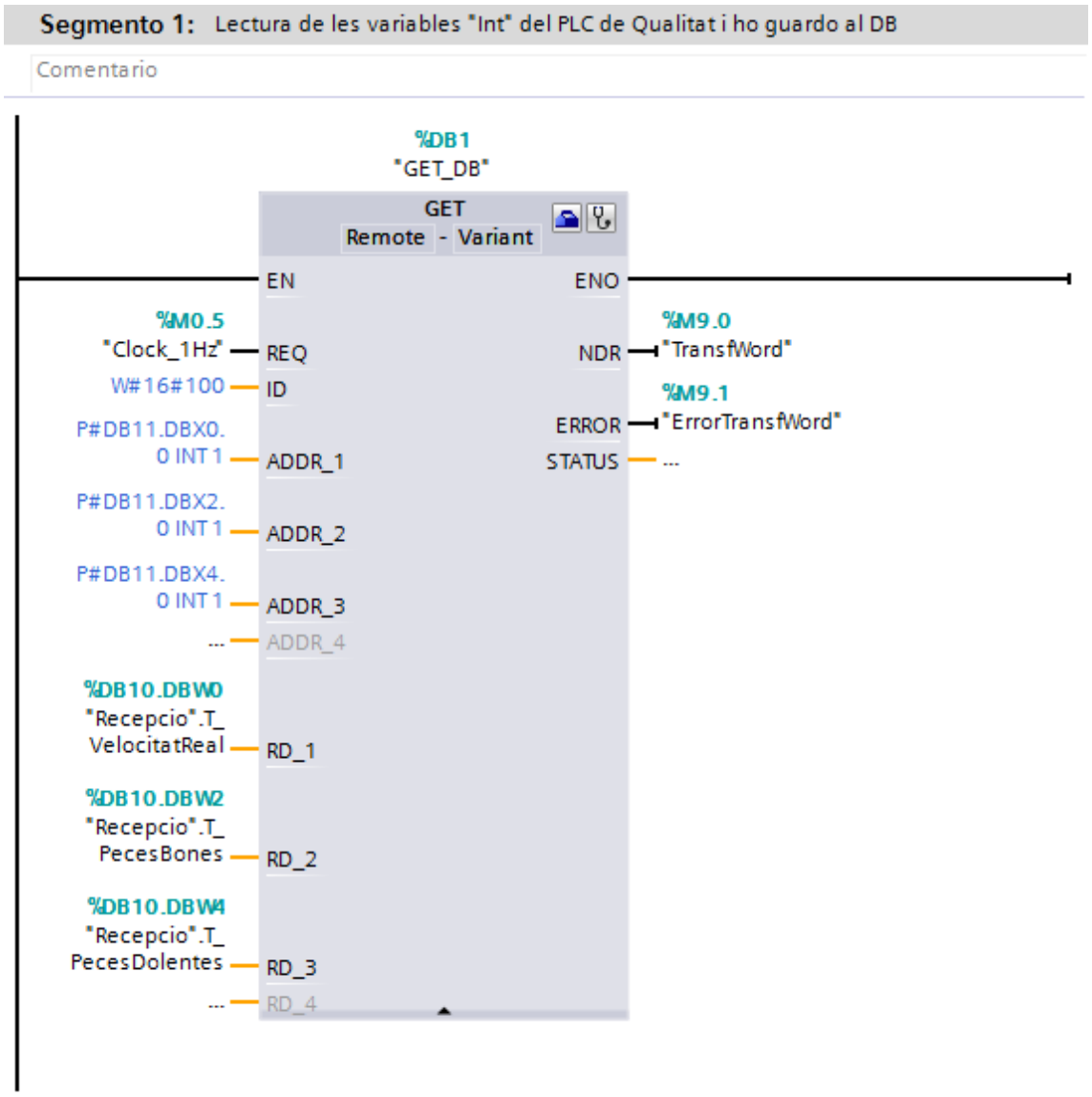


Figura 5.11 - Instrucció GET al PLC del trepant

Per acabar, agafo aquest valors del DB els passo a una variable del PLC per així no tocar de cap manera el DB.

A6 Connexió VPN i HELMHOLZ

A6.1 Fonamentació teòrica

A6.1.1 Característiques bàsiques de seguretat del VPN

Per tal de fer-ho possible de manera segura és necessari proporcionar els mitjans següents:

Autenticació i autorització: Qui està a l'altre costat? Cal definir l'usuari o equip i quin nivell d'accés a de tenir. L'autenticació permet verificar la identitat anunciada i assegurar-se que aquesta no ha estat sostreta. Utilitza el control d'accés.

Integritat: es refereix a quins recursos, dades, tractaments, transaccions o serveis no han estat modificats, alterats o destruïts de forma intencionada o accidental. Para a aconseguir-ho s'utilitzen funcions de Hash. Els algoritmes hash més comuns són els "Message Digest" (MD2 i MD5) i el "SHA).

Confidencialitat/privacitat: donat que tan sols pot ser interpretat pel destinatari. S'utilitzen algoritmes de codificació com "Data Encryption Standard" (DES), "Triple DES" (3DES) i "Advanced Encryption Standard" (AES).

No rebuig: és la prevenció a la negació de que un missatge ha estat enviat o rebut i assegura que l'emissor del missatge no pot negar el seu enviament o que el receptor negui haver-lo rebut.

Control d'accés: es tracta d'assegurar que els participants autenticats tinguin un accés únic a les dades que estan autoritzats.

Auditoria i registre d'activitats: es tracta d'assegurar el correcte funcionament i capacitació de la recuperació en cas necessari.

Qualitat del servei: tracta d'assegurar el bon rendiment del sistema. Doncs no n'hi ha prou amb que el recurs estigui disponible, sinó que sigui utilitzable amb temps de resposta acceptable. És a dir, pugui ser vista com a la protecció de les dades contra una difusió no autoritzada.

A6.1.2 Tipus de connexions VPN

Hi ha diversos tipus de túnels VPN, a continuació se'n descriuen els més comuns:

6.1.2.1 VPN PPTP (punt a punt)

PPTP és la abreviació del protocol de túnel punt a punt (Point-to_Point Tunneling Protocol). Com el seu nom ho indica, una connexió punt a punt crea un túnel i intercanvia les dades entre els dos extrems. Aquest tipus de comunicació és la més utilitzada, per exemple per a connectar oficines remotes o des de qualsevol lloc amb la seu central de la organització. Resulta molt útil per a empreses i l'us dels treballadors que no solen estar a l'oficina de manera permanent. Per accedir a la VPN, els usuaris

inicien sessió amb una contrasenya aprovada. Les VPN punt a punt són ideals per a un ús personal i empresarial perquè no requereix de la compra o instal·lació de hardware addicional i funcions habituals que poden fer-se amb programes complementaris molt econòmics.

Encara que sembli tenir molts beneficis, hi ha un desavantatge d'aquesta VPN, i és que no brinda codificació, que és normalment la raó per la qual un aconseguiria la VPN. Una altra desavantatge és que depèn del protocol punt a punt (PPP) per implementar les mesures de seguretat.

6.1.2.2 VPN Router a router

S'utilitza majoritàriament per a operacions corporatives. Degut al fet que moltes empreses internacionals tenen oficines ubicades dins i fora del país, una connexió d'aquestes característiques s'utilitza per a connectar la xarxa de la oficina principal amb la resta d'oficines. També es coneix amb el nom de VPN basada en intranet. En un terme més general, és un pont virtual que uneix les xarxes de diferents llocs per a connectar-les a internet i mantenir una comunicació segura i privada entre elles.

D'una manera molt semblant a la punt a punt, crea una xarxa segura. Però, no hi ha una línia dedicada en us que permeti que els diferents lloc d'una empresa es connectin per formar una VPN, sinó que vindrien a ser les dues xarxes connectades de manera global. Per aquesta codificació i descodificació no són els mateixos aparells qui ho encripten sinó que es realitza amb routers en forma de hardware o software als dos costats i destinats a ell.

6.1.2.3 VPN L2 TP

És la abreviació de protocol d'establiment de túnels (Layer to Tunneling Protocol) i va ésser desenvolupat per Microsoft i Cisco. Aquest tipus de VPN solen estar combinades amb algun altre protocol de seguretat per tal d'establir una connexió més segura. Una VPN del tipus L2TP forma un túnel entre dos punts de connexió L2TP, i una altra VPN amb protocol IPSec encripta les dades i es focalitza a assegurar la comunicació entre els dos extrems del túnel.

La L2TP és similar a la PPTP. Les semblances són en termes de falta d'encriptació i que les dues depenen de protocols PPP. Comencen a diferenciar-se en relació a la confidencialitat i integritat de les dades. Les VPN L2TP tenen les dues característiques mentre que la PPTP no.

6.1.2.4 IPsec

Significa Protocol de seguretat en Internet. És un protocol que s'utilitza per a protegir la comunicació per internet a través d'una xarxa IP. S'estableix un túnel en un lloc remot que permet l'accés al servidor o lloc central. Una IPSec funciona protegint la comunicació del protocol d'internet comprovant cada sessió i codificant individualment els paquets de dades durant la connexió. Opera en dos modes, amb transport i amb túnel. Els dos modes protegeixen la transferència de dades entre dues xarxes

diferents. Amb el mode transport, es codifica el missatge en el paquet de dades. En el mode túnel, s'encripta tot el paquet de dades. Un benefici per utilitzar aquest tipus de VPN IPSec és que també es pot utilitzar junt amb altres protocols de seguretat per tal que el sistema sigui més robust.

Encara que una VPN IPSec és molt valuosa i important, una gran desavantatge d'utilitzar aquest protocol és la necessitat d'unes instal·lacions costoses i que retarden molt temps en el costat del client.

6.1.2.5 SSL i TLS

SSSL significa "Secure Sockets Layer" i TLS "Transport Layer Security". Les dues funcionen com a un sol protocol. Tracta d'una connexió VPN on el navegador web funciona com a client i l'accés de l'usuari està restringit a certes aplicacions específiques en lloc de poder accedir a tota la xarxa. El protocol SSL i TLS es sol utilitzar en web de compres així com a proveïdors de serveis. UNA VPN SSL i TLS dóna una sessió segura des del navegador del teu PC cap al servidor de l'aplicació. Això es deu a que els navegadors web canvien a mode SSL fàcilment i gairebé no requereix de cap acció per part de l'usuari. Els navegadors ja vénen amb SSL i TLS integrat. Les connexions SSL tenen https (http de seguretat) al inici de la direcció URL enlloc del http.

6.1.2.6 VPN MPLS

S'anomenen MPLS a les VPN per etiquetes multi-protocol i són utilitzades amb major eficiència per a connexions del tipus router a router. Això es deu principalment pel fet que les MPLS són l'opció més segura i adaptable. Es tracta d'un recurs de base estàndard que s'utilitza per accelerar la distribució de paquets de xarxa a través de múltiples protocols. Les MPLS són sistemes que estan ajustat a ISP. Una VPN ajustada a ISP és quan dos o més llos estan connectats per formar una VPN utilitzant el mateix servidor d'internet. De totes maneres, la desavantatge més gran és el fet que la configuració de la xarxa té una certa complexitat tant a l'hora de crear-la com a l'hora de modificar-la.

6.1.2.7 VPN Híbrida

Una connexió d'aquest tipus comvina ¨MPLS i VPN basada en el protocol de seguretat internet o IPSec, encara que els dos tipus s'utilitzin per separa a diferents llocs. De totes maneres, es poden utilitzar els dos en el mateix lloc. Es fa amb la intenció d'utilitzar el VPN IPSec com a recolzament de la VPN MPLS.

Les IPSec són VPN que requereixen un equipament per part del clients d'algunes coses mencionades anteriorment. Aquest equipament generalment ve en forma de router o aparell de seguretat. A través del router es codifiquen les dades i es forma un túnel VPN tal i com s'ha descrit.

Per a connectar-se a través de dos VPN, s'estableix un portal per eliminar el túnel IPSec per un costat i enllaçar-lo cap a la VPN MPLS a l'altre costat mentre s'assegura la seguretat que pugui donar aquesta xarxa.

Les VPN híbrides solen ésser utilitzades per empreses perquè les MPLS no seria la millor opció per a elles. La connexió híbrida permet accedir al lloc central a través d'un lloc remot. En general aquestes connexions solen ser costoses però ofereixen una gran flexibilitat.

El protocol més utilitzats de tots és el IPSec, però el segueixen de ben a prop els protocols PPTP, L2 TP, SSL/TLS, etc. Cada un amb els seus avantatges i inconvenients de seguretat, facilitat, manteniment i tipus de clients suportats.

Actualment, hi ha una important onada en la utilització del protocol SSL/TLS:

- Les opcions a través de hardware normalment solen tenir una configuració més fàcil i un millor rendiment, encara que poden tenir mancances a l'hora de ser flexibles.
- Les opcions de software són més configurables i es poden adaptar més fàcilment. De totes maneres però, la configuració és més complicada i el rendiment menor.

En els dos casos però es poden utilitzar tallafocs per augmentar la seguretat del sistema.

A6.1.3 Arquitectures de connexió VPN

6.1.3.1 Conexió d'accés remot

Una connexió d'accès remot la realitza un usuària que es connecta a una xarxa local, els paquets de dades que s'envien sçon creats al client i aquest s'autentica al servidor, per altra banda el servidor s'autentica al client.

6.1.3.2 Connexió VPN router a router

Una connexió router a router és tal i com indica el seu nom, que el reouter es connecta a la xarxa privada. Els paquets enviats des de qualsevol router s'originen en el mateix router. Les autenticacions són de la mateixa manera entre ells dos.

6.1.3.3 Connexió VPN Firewall a Firewall

Aquest tipus de connexió és realitzada per un dels firewalls, i aquest es connexta a la xarxa privada. Amb aquest tipus de cconnexió els paquets poden ser enviats des de qualsevol client a internet.

6.1.3.4 Connexió VPN en entorns mòbils

La connexió VPN mòbil s'estableix quan el punt de finalització de la VPN no és fixe en una única direcció IP, sinó que es mou entre vàries xarxes com poden ser les dels

operadors mòbils o diferents punts d'accés wifi. Les VPN mòbils s'han utilitzat en aplicacions crítiques de seguretat pública amb la finalitat de protegir les dades. Cada vegada més aquest tipus de connexió s'utilitza més per a necessitats de connexions fiables. Tanmateix, s'utilitzen per a moure's entre xarxes sense perdre la connectivitat segura de la VPN.

A6.2 Configuració del router Helmholz

Al connectar-nos mitjançant shDIALUP hem de pensar a activar v2 perquè sinó no podrem entrar amb les credencials:

Usuari: UVIC@coevavic

Password: JuliAI2

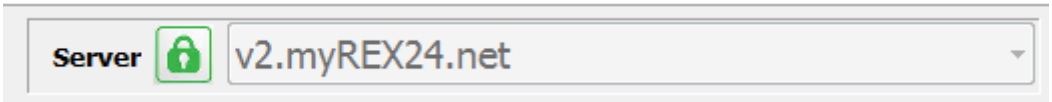


Figura 6.1 - Servidor al que ha de connectar-se

També és molt important recordar que l'accés a internet es dóna a través del port P1 WAN

Les propietats de seguretat que es deixa el router són:

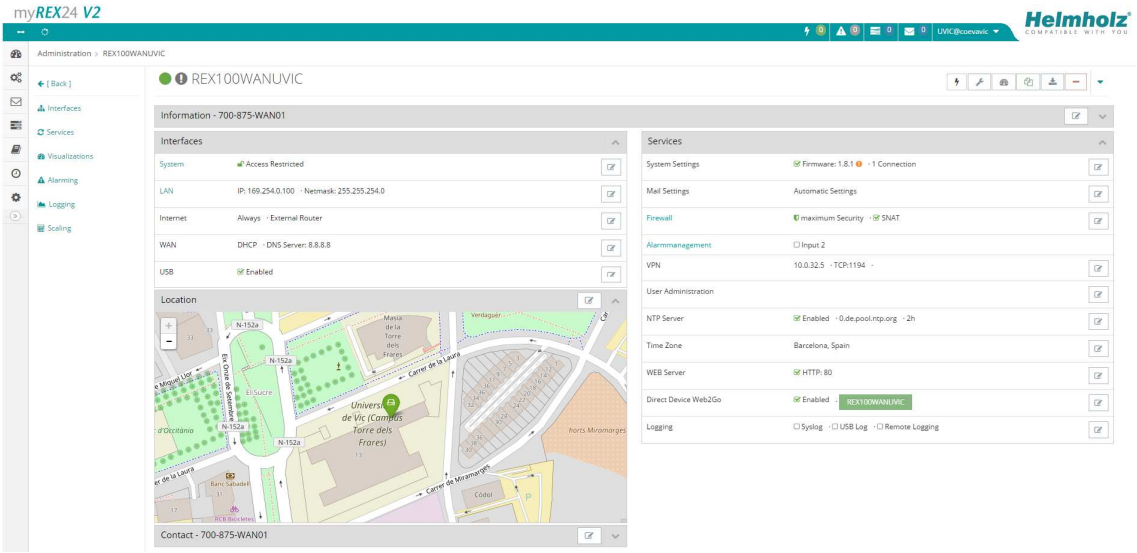


Figura 6.2 - Propietats del router

Des dels DAshboard veiem si tenim el router connectar pq està en verd

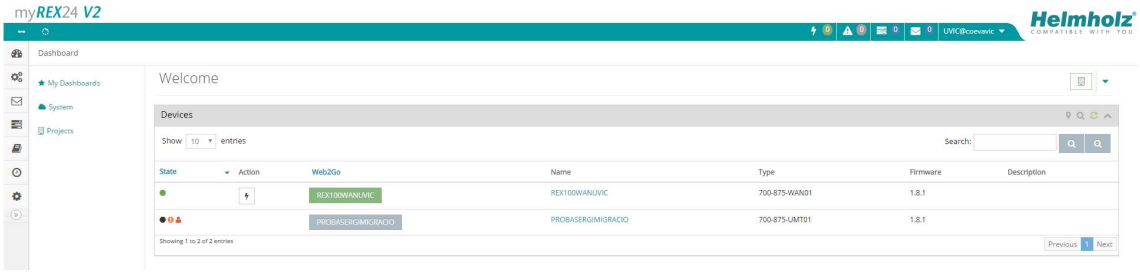
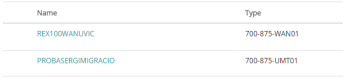


Figura 6.3 - Connexions disponibles

Clickem a REX100WANUVICper entrar



Veiem les connexions que tenim disponibles

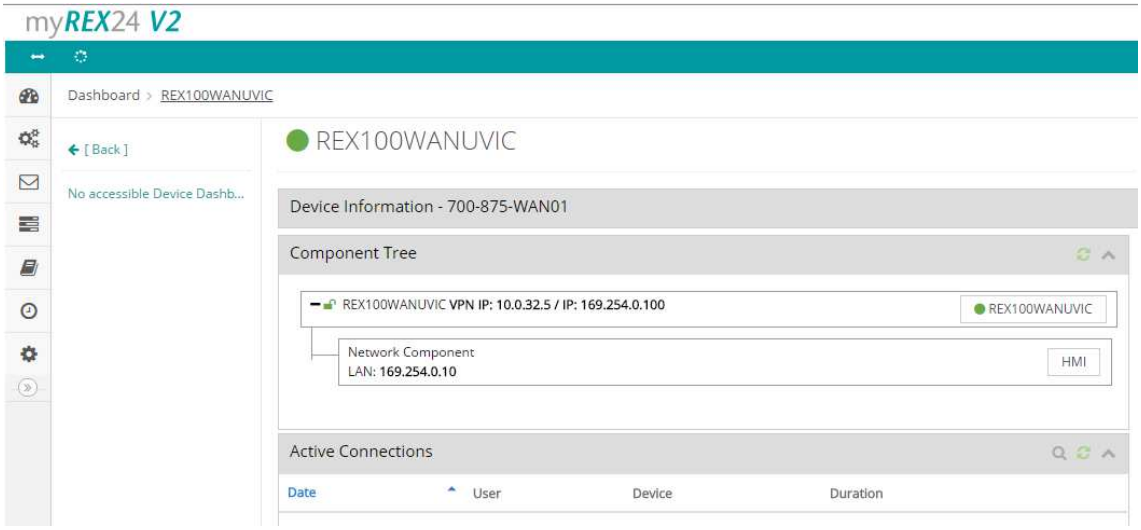


Figura 6.4 - Connexions disponibles al router

Volem afegir la connexió al webserver de Qualitat. Clickem a Administration, Projects, UVIC, REX100WANUVIC, interfaces, LAN. Afegim un comoponent amb el signe “+”

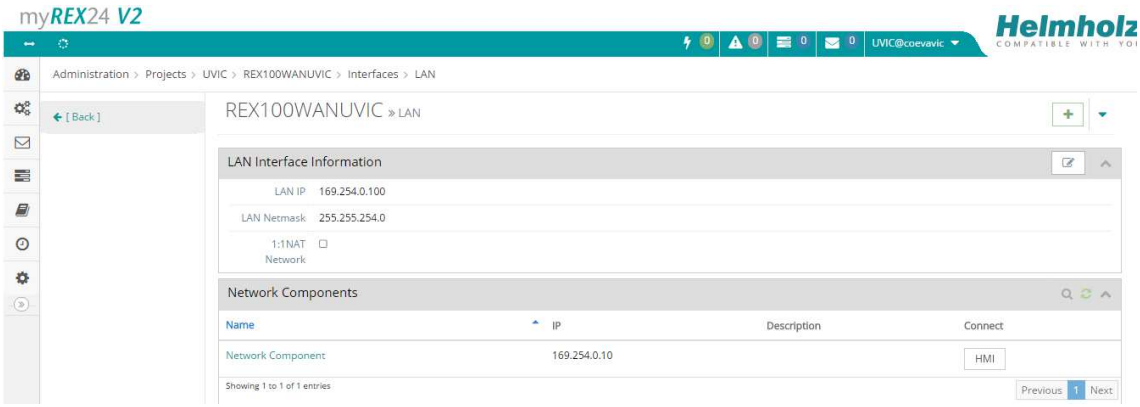


Figura 6.5 - introducció de components

Entrem les dades de la CPU

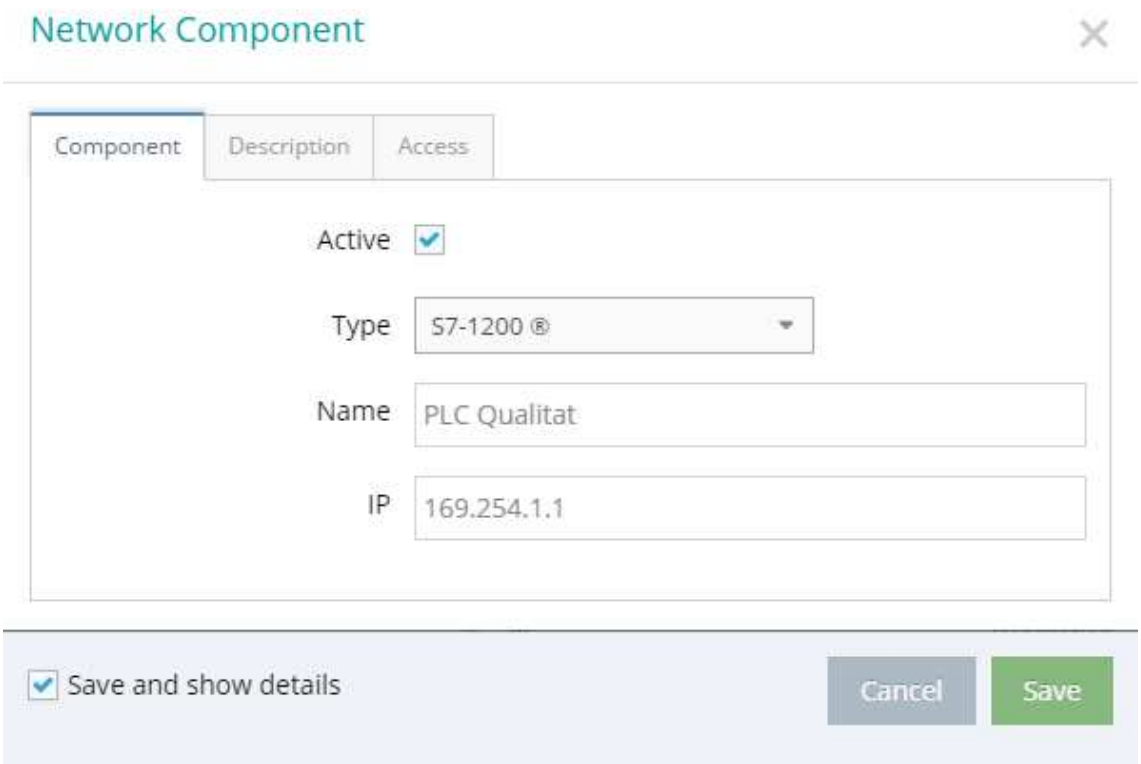


Figura 6.6 - Configuració del component

Creem una nova connexió al web2go amb el nom, tipus, port i path que és la ruta de la pàgina. En el meu cas és la que ens dona per defecte: /Portal/Intro.mwsl . D'aquesta manera entrem a la pàgina principal del PLC i on veiem totes les disponibilitats que ja ens ofereix Siemens per defecte.

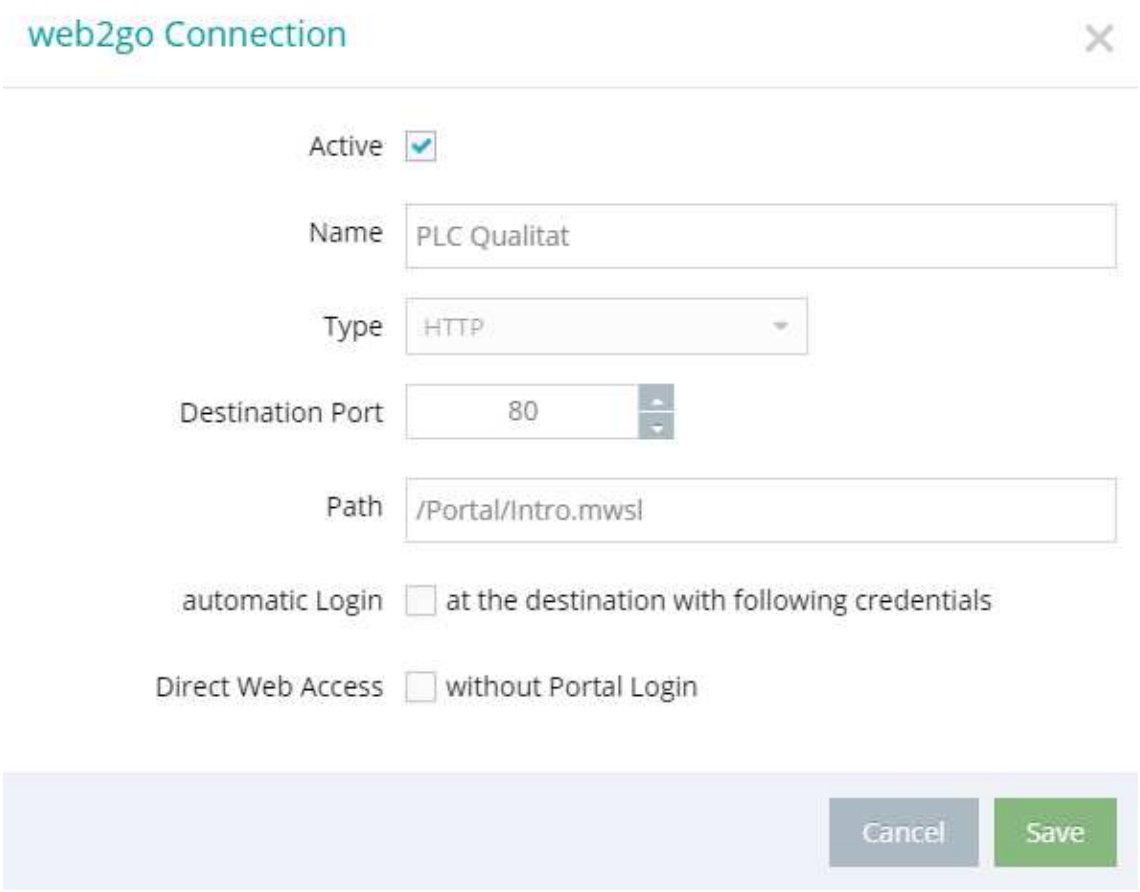


Figura 6.7 - Configuració web2go

Finalment, podem connectar-nos mitjançant el requadre de la connexió

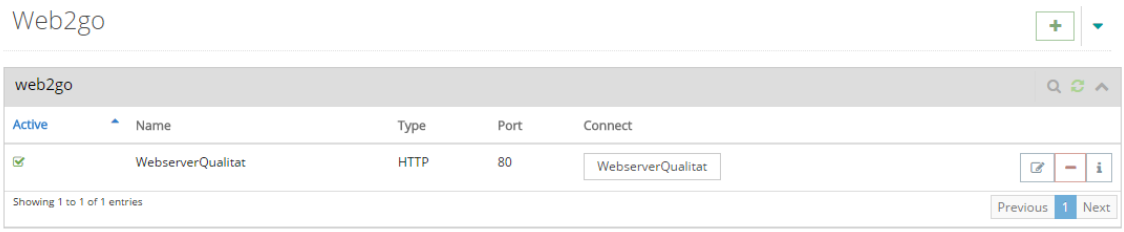


Figura 6.8 - Finalització de la configuració per a la connexió

O bé comprartir l'enllaç clickant al requadre d'informació

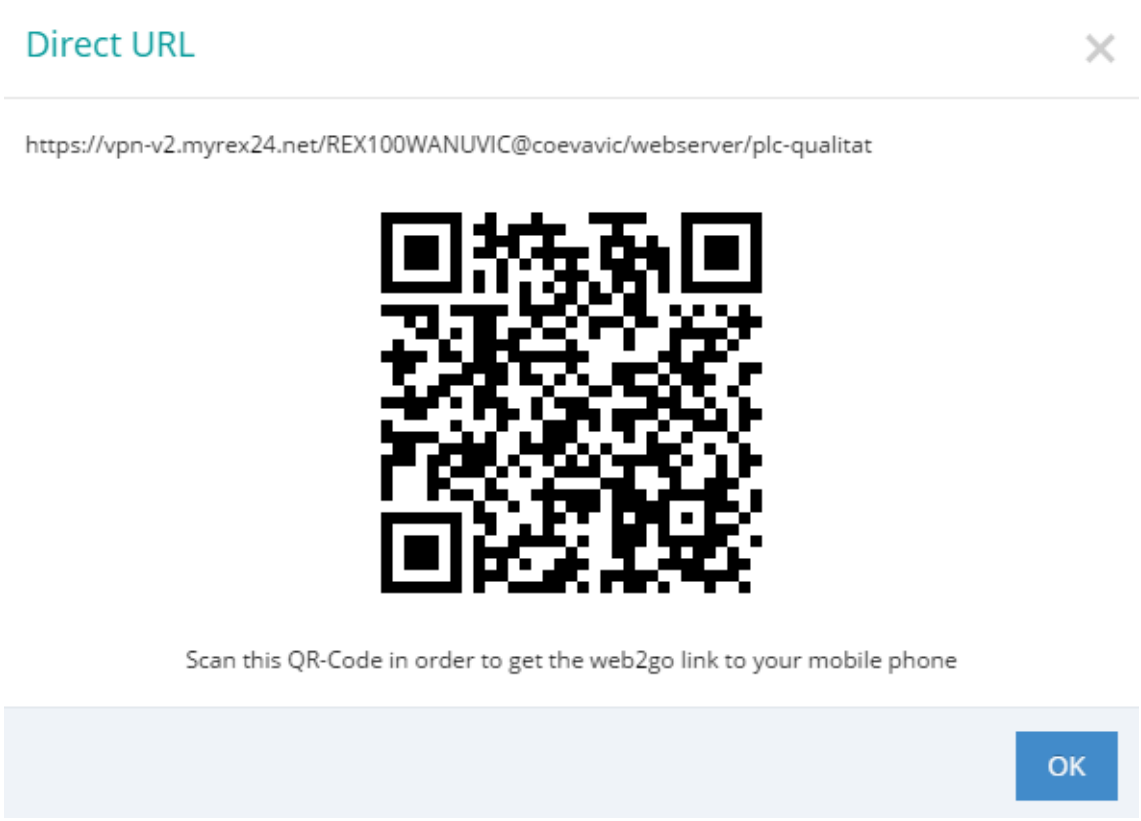


Figura 6.9 - Codi QR i enllaç per a l'accés remot

Aquest segon cas el tindrem disponible sempre que activem el “Direct Web Access”

Figura 6.10 - Activació de l'accés directe

Per tal de tenir accés a la pantalla tàctil, cal activar l’sm@rtServer al runtime del HMI

Figura 6.11 - Activació de l'Sm@artService