TP1 Cybersecurity TI - inherent PLC protections

Operational objectives:

- Understand the role and scope of the configuration of the M580 ePAC Central Unit's Ethernet security-related services (flat network vs. separate networks)
- Be able to define and modify this type of configuration, globally or selectively, and to explain its effectiveness, with supporting traces

Prerequisites:

- Have a general knowledge of the principles of Ethernet protocols and addressing (IPV4)
- Know how to change the IP address of a PC's local Ethernet port and specify a route for it
- Master the basic operations of Control Expert and Unity Loader
- Master the operations required to configure the CPU module and the Ethernet couplers of the ePAC M580 via Control Expert
- Be able to run Vijeo Designer in simulation mode
- Understand the basic structure of a Modbus frame and its main functions
- Be able to perform a Wireshark capture, and filter addresses and protocols

The problem posed:
Understand and deploy the inherent cybersecurity defenses of the ePAC M580

Resources:

- Manufacturer's documentation
  - Schneider Electric (website)
- Specific documentation (in ressources)
  - Architectures Maquette Cybersec_anglais.pptx
- Applications made available for this exercise:
  - M580 application (Control Expert): md1ae58ecyb.stu
  - HMI application (Vijeo Designer): MD1AE58ECYB
- Software provided, to be installed on the work PC (console) for the realization of this TP:
  - Control Expert (Schneider Electric) : Programming of Schneider Electric M340, M580, …
  - Unity Loader (Schneider Electric) [optional]: loading of M340/M580 PLC firmware
  - Vijeo Designer V6.2 SP8: Magelis HMI Application Design
  - (execution including in Simulation mode on the Workstation)
  - Web Gate Client (Schneider Electric): complement to Vijeo Designer [option]. (remote client of the Magelis HMI, running in an Internet browser)
  - Internet Explorer : Microsoft's Internet browser
  - Angry IP Scanner (angryip.org): check for accessible IP addresses in a given range [option].
  - Wireshark (Wireshark Foundation): observation of Ethernet frame details

- Evaluation criteria :

	😀	😐	😟
Understanding flat architecture vs. separate networks			
Interpretation/justification of the protocols considered (MB/TCP, HTTP, FTP)			
Implementation / justification of global control manipulations			
Implementation / justification of selective control manipulations			
Handling of tools (Control Expert / Loader, IE, VJD Simulation and Wireshark)			
Autonomy - Quality of work/restitution			

Time spent:	2h	Objective(s) :		Comment(s) :
Evaluation :	/ 20	Achieved	Not achieved	

TP1 - The intrinsic protections of the PLC (ePAC) in terms of Cybersecurity

The programmable logic controller, and in particular the Schneider Electric ePAC M580, provides a number of functionalities that can rightly be exploited as defensive measures in terms of cyber security.

These include, in particular, for entities with Ethernet connectivity (CPU or communication coupler):

- The ability to explicitly enable or disable the service of Ethernet communication protocols such as HTTP, FTP ... for example
- Filtering on IP addresses explicitly designated as eligible accessors (clients). This filtering will, for each designated IP address, validate/inhibit the service of such or such protocol (Modbus502, HTTP, FTP, ...)

This tutorial aims at highlighting these possibilities, solicited in a static way (i.e. by configuration)

NB: Dynamic filtering (i.e. by program) is beyond the scope of this course

NB: The implementation of the IPSec protocol is beyond the scope of this tutorial

—---

1. With the help of the documents provided (see Architectures Maquette Cybersec_anglais.pptx), identify and comment on the various components of the target architecture, in accordance with the Phase 1 architecture diagram.

2. The first step is to lay the Ethernet cables on the board, in accordance with this so-called Phase 1 architecture.

3. Load the M580 PLC using the default application program (md1ae58ecyb.stu), which does not involve filtering on services or filtering on the IP addresses of the accessors.

   NB: the HMI is the owner of the Vijeo Designer application program (MD1AE58ECYB)

   Check access to the drive speed setpoint modification, initially from the local HMI, and also from an Internet Browser requesting the HMI's IP address (Web Gate client).

   ---

4. Check the access to the drive speed setpoint modification, from the HMI application (Vijeo Designer) running in simulation mode on the Workstation.

   From an Internet Browser running on the Workstation, check access to the HTML pages served by the M580 CPU.

Try using the M580 PLC from the Workstation, using the Unity Loader utility to test the use of the FTP protocol

NB: The demonstration of Modbus/TCP, HTTP and FTP exchanges will be supported, if necessary, by a Wireshark trace (the service port of the CPU is configured in mirror mode, in order to restore all the traffic passing through the different Ethernet ports)

5. Sequentially test the persistence or not of the service of these protocols, depending on whether or not they are enabled/inhibited by the ePAC M580 configuration.

   NB: The demonstration of these behaviours will be supported by a Wireshark trace (the service port of the CPU is configured in mirror mode, to restore all the traffic transiting on the different Ethernet ports).

6. Set up IP address filtering in the configuration of the Ethernet communication on the idkétayCPU port. Check first that, when this filtering mode is activated, the Workstation is not able to operate anything on the ePAC if it is not on the list of declared accessors (whether it is an HTTP, FTP ... or simply Modbus/TCP access).

   Then check that if the IP address of the Workstation is recorded in the list of authorized accessors on the ePAC CPU, it now has full access to the ePAC.

   Next, examine the behavior of the Workstation if its IP address is present on the list of authorized accessors, even though the admissibility of the Modbus/TCP, HTTP and FTP protocols is successively invalidated.

   NB: Idem, support the demonstration of these behaviours with a Wireshark trace.

---

7. Now perform a test sequence identical to the one performed so far (points 4 to 6) considering the Phase 3 Architecture, i.e. by accessing the ePAC not directly via a CPU Ethernet (DIO) port, but via an Ethernet (DIO) port of the BME NOC 0321 coupler installed on the rack of this ePAC. (See document Architectures Maquette Cybersec_anglais.pptx)

   Note: The workstation (as well as the observation station) will be assigned a new IP address - see document Architectures Maquette Cybersec_anglais.pptx - which is supposed to correspond to the addressing domain of the 'Control Network', while the 'devices' will remain in the previous addressing domain, which is supposed to be that of the 'Device Network'. Consequently, the workstation (as well as the observation station) will have to be initialized with a route command to designate the 'internal' IP address of the NOC coupler to the PC as the access point to the 'Device Network'.

Bonus: Provide a short summary of the scope of the Modbus502, HTTP vs FTP clients, depending on whether the target IP address is the main port of the M580 CPU or the external address of the BME NOC 0321 coupler.

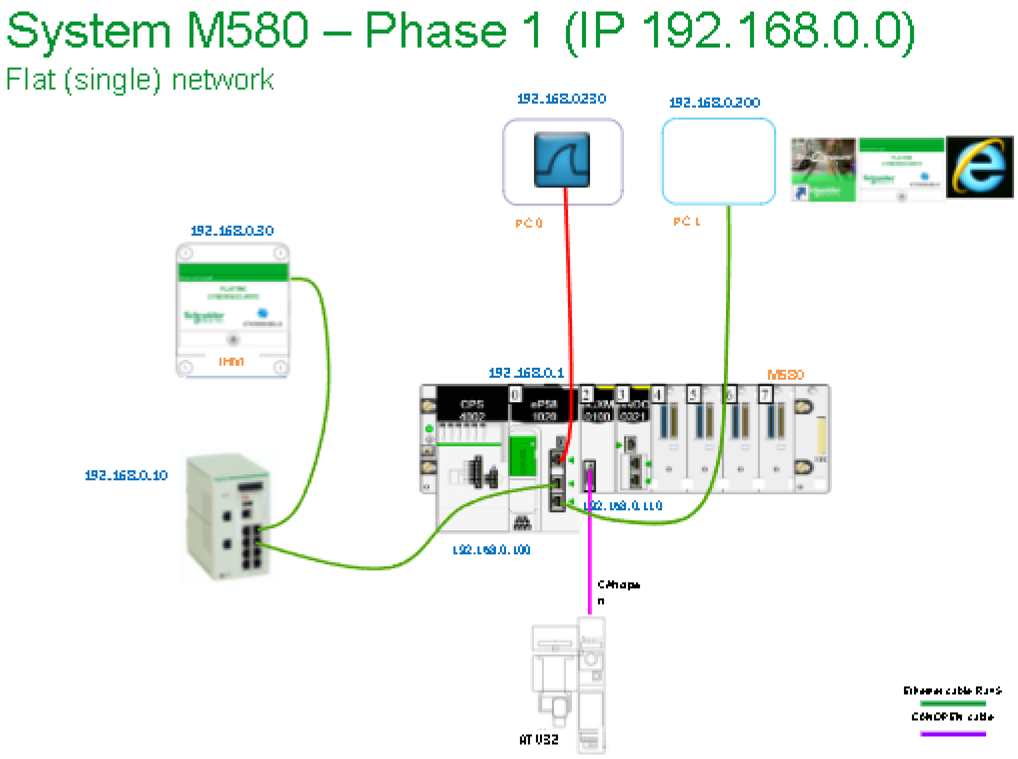
—---

Note: The BME coupler service port N0C 0321, as well as the M580 CPU service port, is configured in mirror mode by the M580 application program, to allow all traffic passing through the other coupler or CPU ports to be restored if required.

Details of expected operations

1. Architecture components Phase 1

- Identification and commentary on the components of the target architecture (Phase 1)



System M580 – Phase 1 (IP 192.168.0.0)

Flat (single) network

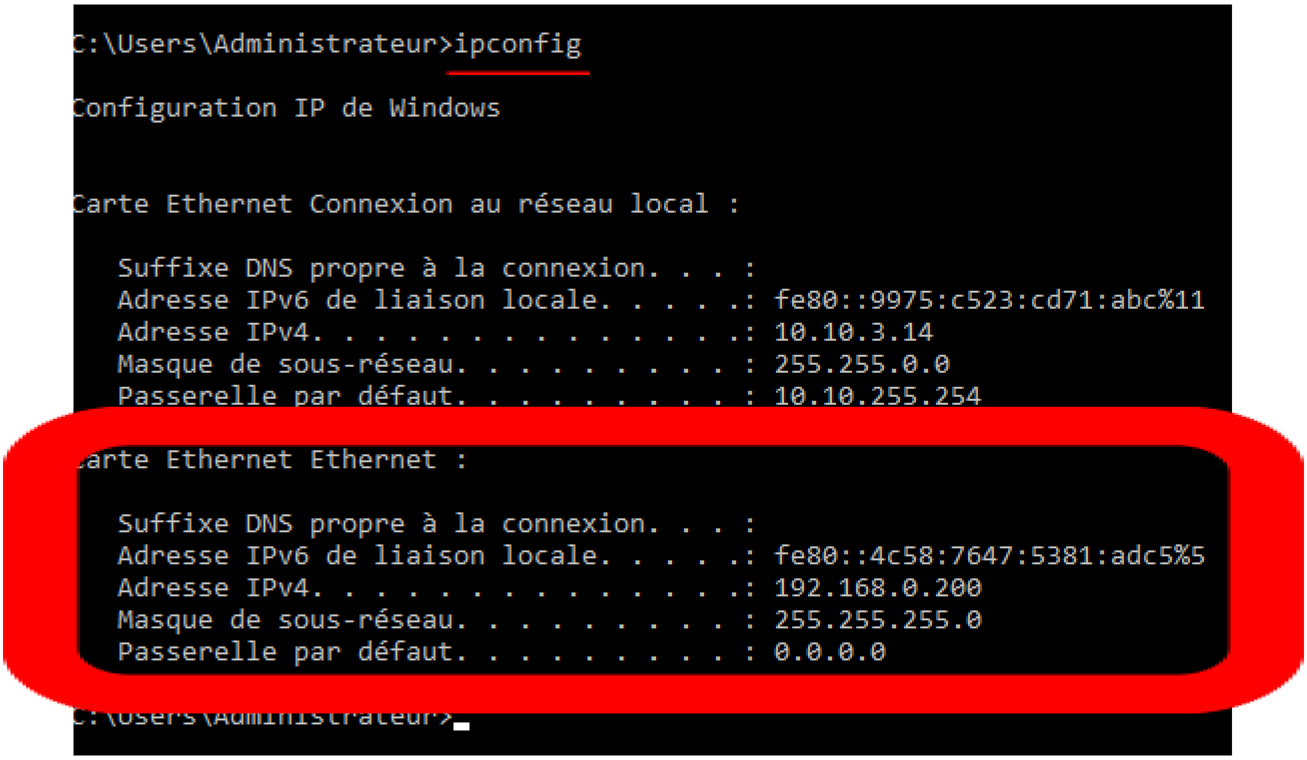
2. Installation of Ethernet cables according to the Phase 1 architecture

3. Loading the program with the default application (md1ae58ecyb.stu)

program to be open: **md1ae58ecyb.stu**

3.1. Checking the IP address of the workstation

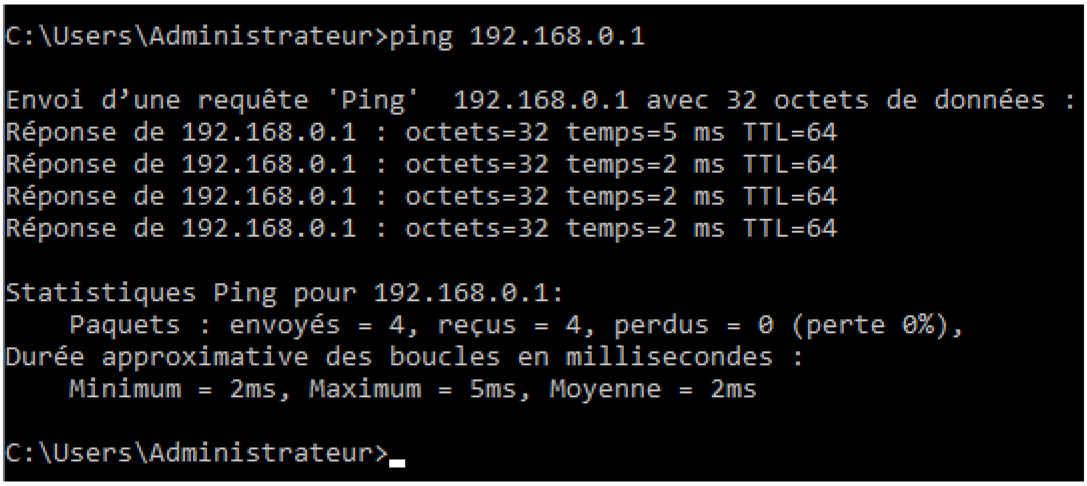
Make sure, as simply as possible by means of an **IPCONFIG**, of the IP address of your workstation, on your local (wired) network: **192.168.0.200**



```
C:\Users\Administrateur>ipconfig

Configuration IP de Windows


Carte Ethernet Connexion au réseau local :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::9975:c523:cd71:abc%11
   Adresse IPv4. . . . . . . . . . . . . .: 10.10.3.14
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 10.10.255.254

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::4c58:7647:5381:adc5%5
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.0.200
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 0.0.0.0

C:\Users\Administrateur>_
```

3.2. Checking the IP address of the M580 ePAC

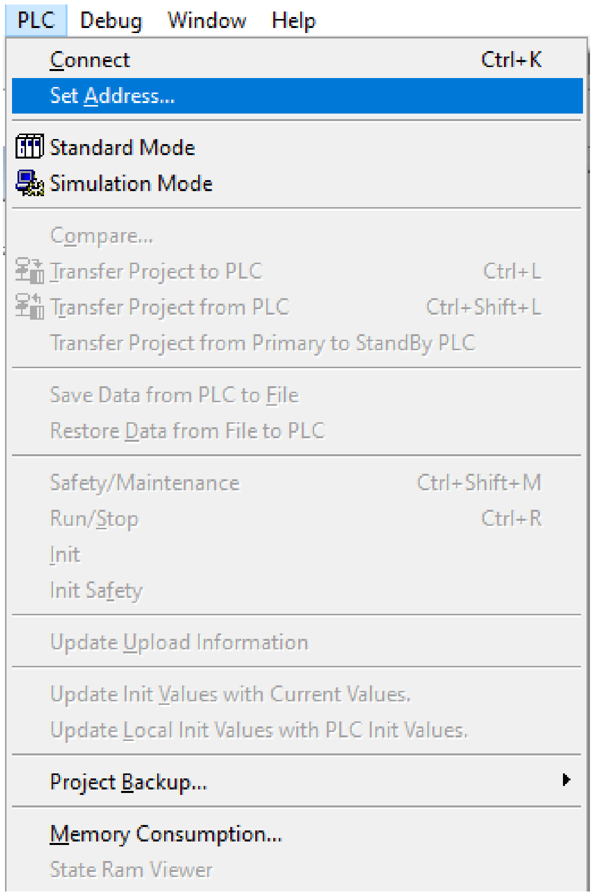
Before wiring the SNi40, make sure that the ePAC/M580 (main address **192.168.0.1**) is accessible by means of a PING

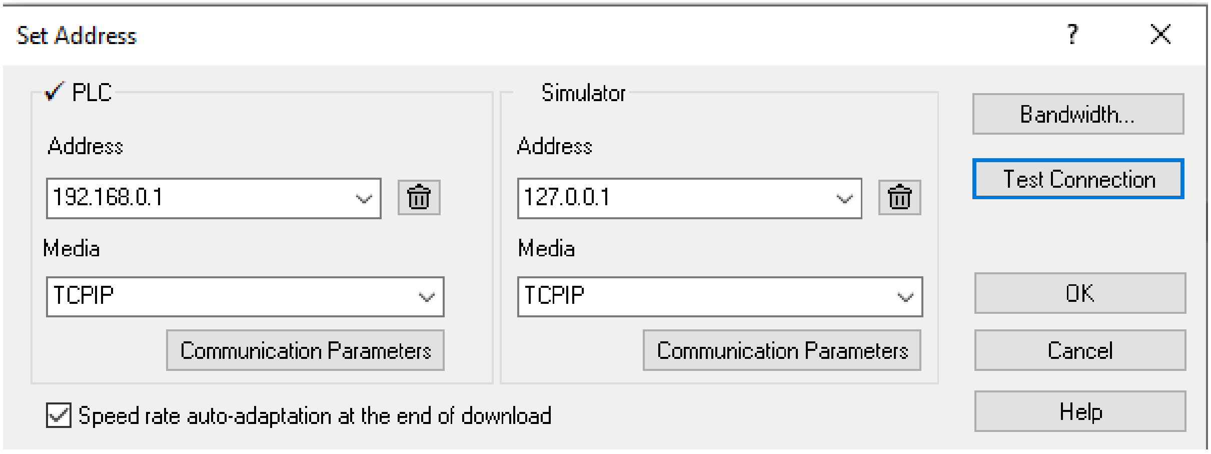


```
C:\Users\Administrateur>ping 192.168.0.1

Envoi d’une requête 'Ping'  192.168.0.1 avec 32 octets de données :
Réponse de 192.168.0.1 : octets=32 temps=5 ms TTL=64
Réponse de 192.168.0.1 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.0.1 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.0.1 : octets=32 temps=2 ms TTL=64

Statistiques Ping pour 192.168.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 5ms, Moyenne = 2ms

C:\Users\Administrateur>_
```

3.3. Reloading the PLC program (optional)

Using the Control Expert software, reload (if necessary) the ePAC M580 with the application program (**md1ae58ecyb.stu**), free of any protocol/service limitation and address filtering (using if possible the Ethernet link --- main address 192.168.0.1) or alternatively the USB link.

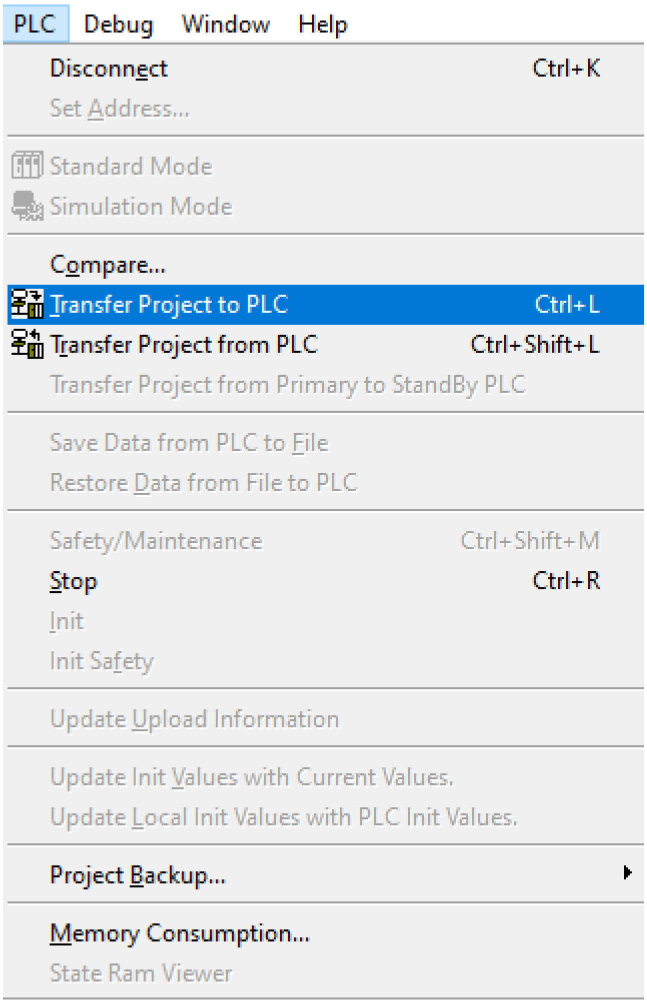

PLC
Debug
Window
Help
Connect Ctrl+K
Set Address...
Standard Mode
Simulation Mode
Compare...
Transfer Project to PLC Ctrl+L
Transfer Project from PLC Ctrl+Shift+L
Transfer Project from Primary to StandBy PLC
Save Data from PLC to File
Restore Data from File to PLC
Safety/Maintenance Ctrl+Shift+M
Run/Stop Ctrl+R
Init
Init Safety
Update Upload Information
Update Init Values with Current Values.
Update Local Init Values with PLC Init Values.
Project Backup...
Memory Consumption...
State Ram Viewer

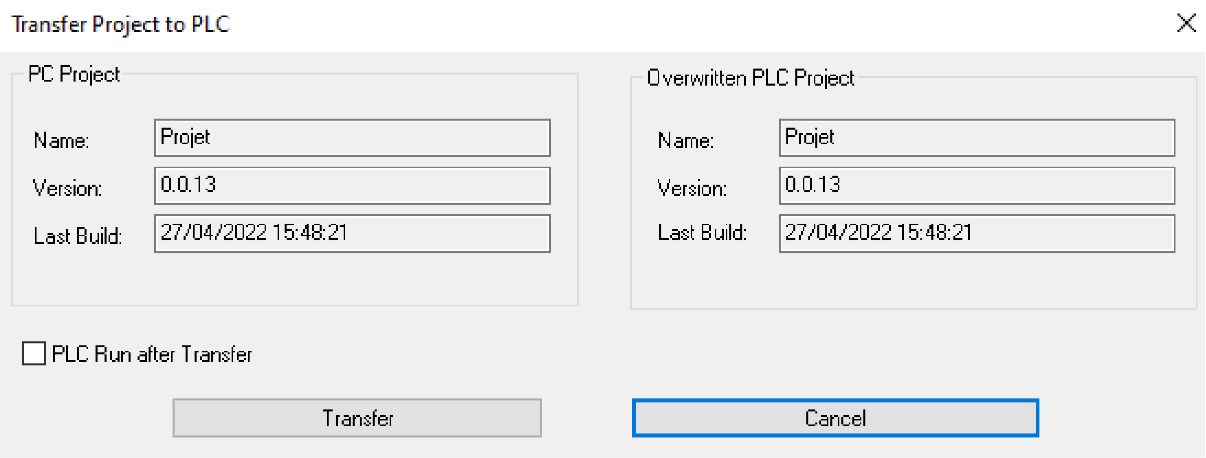


✓ PLC
Address: 192.168.0.1
Media: TCPIP

Simulator
Address: 127.0.0.1
Media: TCPIP

☑ Speed rate auto-adaptation at the end of download


PLC
Debug
Window
Help
Disconnect Ctrl+K
Set Address...
Standard Mode
Simulation Mode
Compare...
Transfer Project to PLC Ctrl+L
Transfer Project from PLC Ctrl+Shift+L
Transfer Project from Primary to StandBy PLC
Save Data from PLC to File
Restore Data from File to PLC
Safety/Maintenance Ctrl+Shift+M
Stop Ctrl+R
Init
Init Safety
Update Upload Information
Update Init Values with Current Values.
Update Local Init Values with PLC Init Values.
Project Backup...
Memory Consumption...
State Ram Viewer


Transfer Project to PLC

PC Project

Name: Projet
Version: 0.0.13
Last Build: 27/04/2022 15:48:21

Overwritten PLC Project

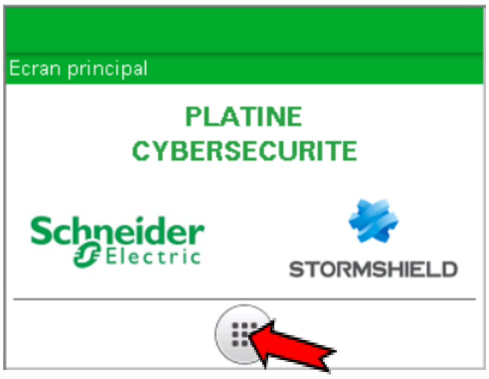
Name: Projet
Version: 0.0.13
Last Build: 27/04/2022 15:48:21

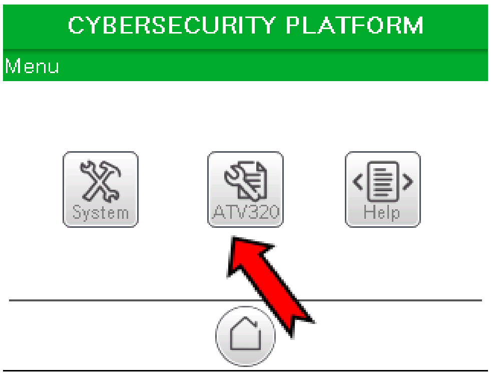
□ PLC Run after Transfer

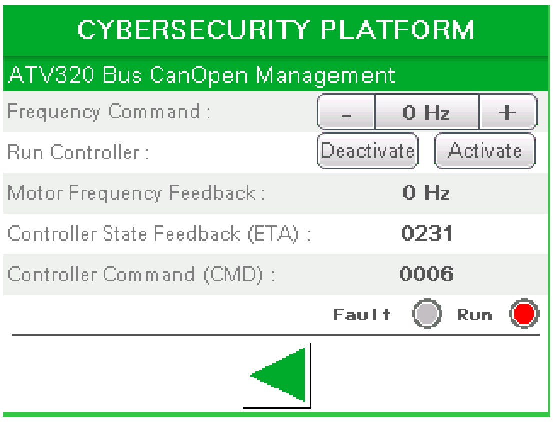
At the end of this loading, put the automaton in RUN.

3.4. Checking the accessibility of the ePAC for the HMI

- From the HMI, go to the speed controller control view







CYBERSECURITY PLATFORM

ATV320 Bus CanOpen Management

Frequency Command : - 0 Hz +

Run Controller : Deactivate Activate

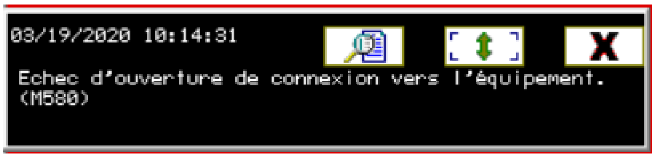
Motor Frequency Feedback : 0 Hz

Controller State Feedback (ETA) : 0231

Controller Command (CMD) : 0006

Fault ○ Run ●

NOTE: If the ePAC is inaccessible, the base of the HMI display will show a message like:

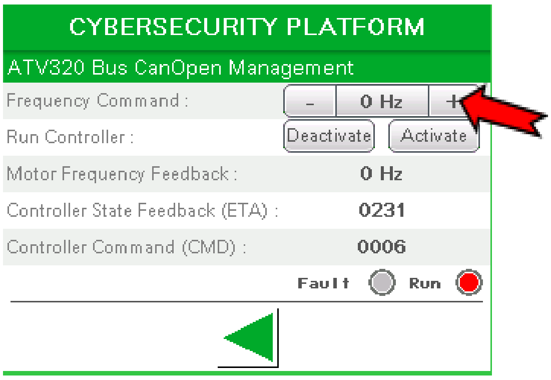


03/19/2020 10:14:31

Echec d'ouverture de connexion vers l'équipement. (M580)

If this error occurs, check the wiring. If necessary, check the HMI and ePAC applications.

- Changing the speed setpoint



CYBERSECURITY PLATFORM

ATV320 Bus CanOpen Management

Frequency Command : - 0 Hz +

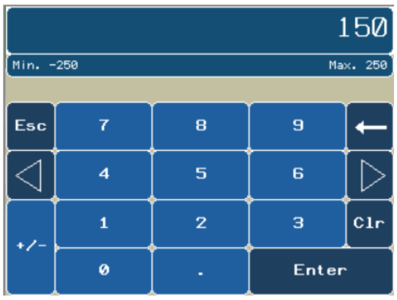
Run Controller : Deactivate Activate

Motor Frequency Feedback : 0 Hz

Controller State Feedback (ETA) : 0231

Controller Command (CMD) : 0006

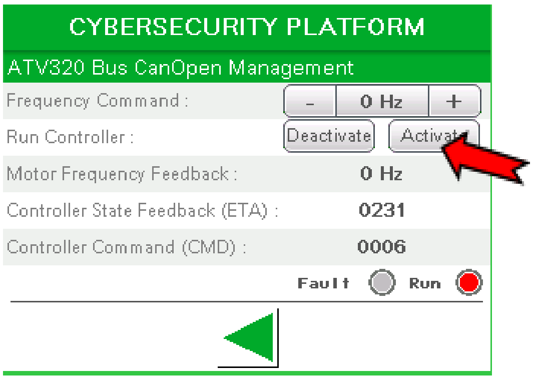
Fault ○ Run ●



150

Min. -250 Max. 250

- Start the engine by pressing the "Activate" button, and ensure that the engine is running.



CYBERSECURITY PLATFORM

ATV320 Bus CanOpen Management

Frequency Command : - 0 Hz +

Run Controller : Deactivate Activate

Motor Frequency Feedback : 0 Hz

Controller State Feedback (ETA) : 0231

Controller Command (CMD) : 0006

Fault ○ Run ●

Play with the speed setpoint and check that the motor speed matches the setpoint.

- Switch off the engine by pressing the "Disable" button, and ensure that the engine is stopped.

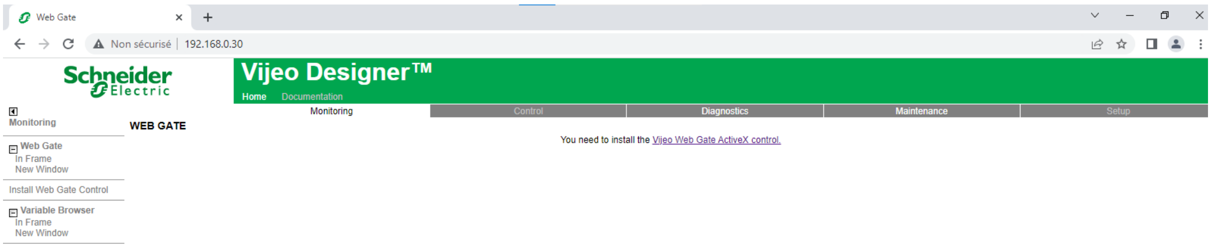
3.5. Verification of ePAC accessibility for the Web Gate replica of the HMI

Proceed in the same way, using a Web Gate access of the HMI on the workstation through an Internet Browser (Internet Explorer).

- Change the PC screen resolution to 800x600

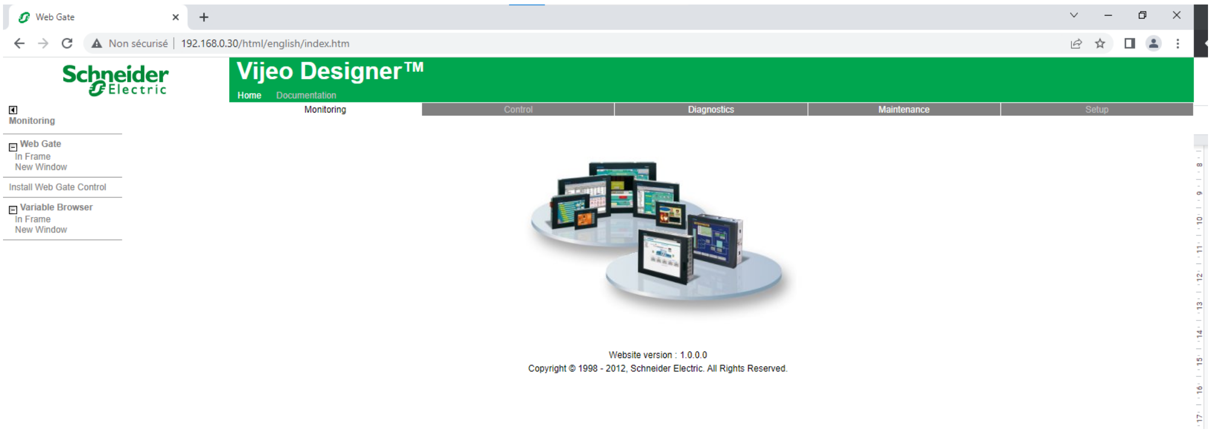
- Install "Web_Gate_Client_Files_6.2_SP8" available in the "Software" folder in 3Web Gate”

- Open Internet Explorer and enter the address of the HMI (192.168.0.30) in the address bar. Validate if necessary the Vijeo Web Gate add-on (Allow)



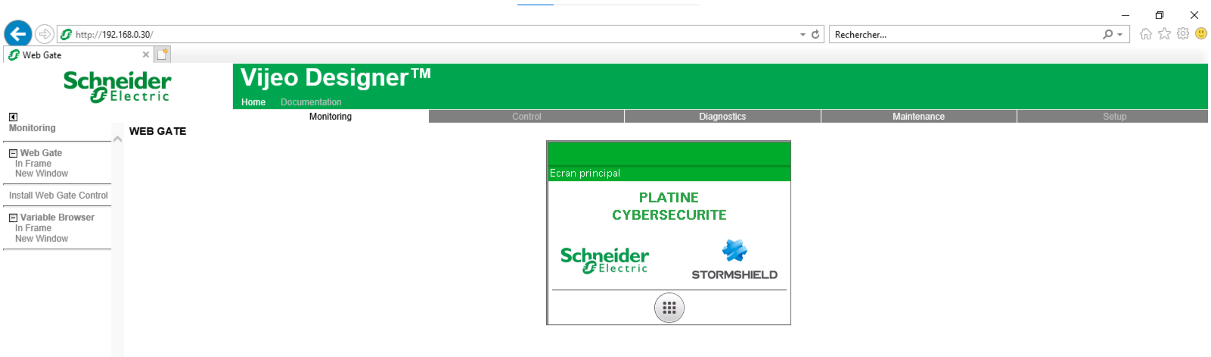
You need to install the Vijeo Web Gate ActiveX control.

- Select the English language

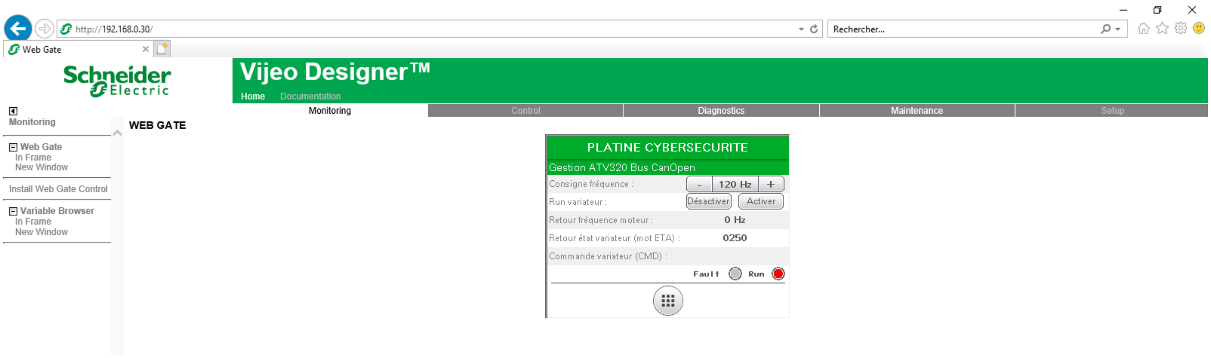


Website version : 1.0.0.0
Copyright © 1998 - 2012, Schneider Electric. All Rights Reserved.

- Then click on the Visualization tab and then on the entry Webgate | In Frame to display the HMI screens.



- Proceed as on the HMI to reach the drive control screen



PLATINE CYBERSECURITE

Gestion ATV320 Bus CanOpen

Consigne fréquence : - 120 Hz +

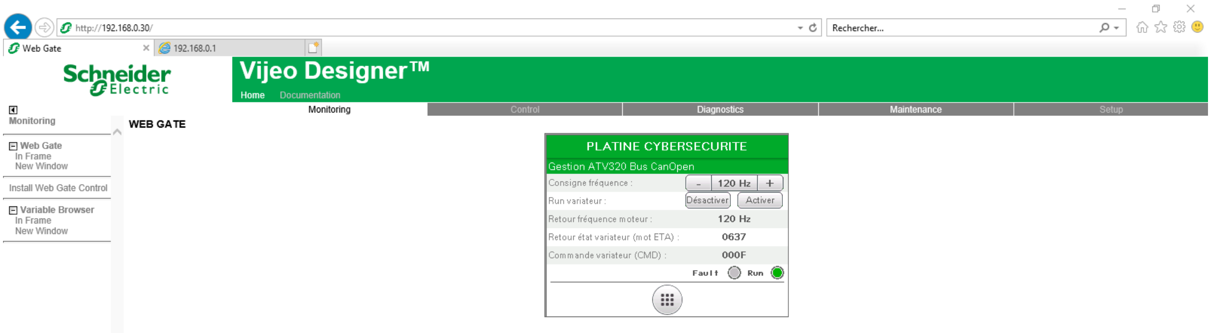
Run variateur : Désactiver Activer

Retour fréquence moteur : 0 Hz

Retour état variateur (mot ETA) : 0250

Commande variateur (CMD) :

Fault ○ Run ●



PLATINE CYBERSECURITE

Gestion ATV320 Bus CanOpen

Consigne fréquence : - 120 Hz +

Run variateur : Désactiver Activer

Retour fréquence moteur : 120 Hz

Retour état variateur (mot ETA) : 0637

Commande variateur (CMD) : 000F

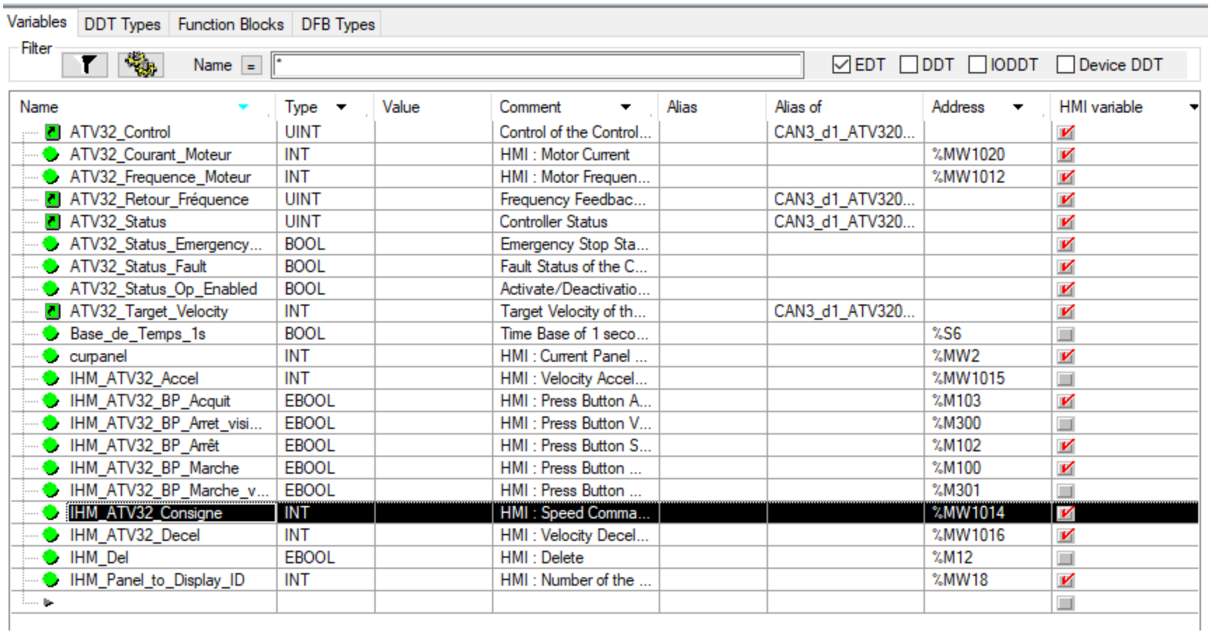
Fault ○ Run ●

NOTE: the commands operated from WebGate will, within the framework of this practical work, only be effectively taken into account if this view is simultaneously displayed on the HMI

4. Checking the availability of the Modbus/TCP, HTTP and FTP protocols by the M580 Central Unit

4.1. Verification of ePAC accessibility for Modbus/TCP requests requests issued by Vijeo Designer in Simulation Mode

- First check with Control Expert, through an Animation Table, the possibility to read/write the speed setpoint value of the drive, i.e. the possibility to read/write the variable **IHM_ATV32_Consigne** (%MW1014)



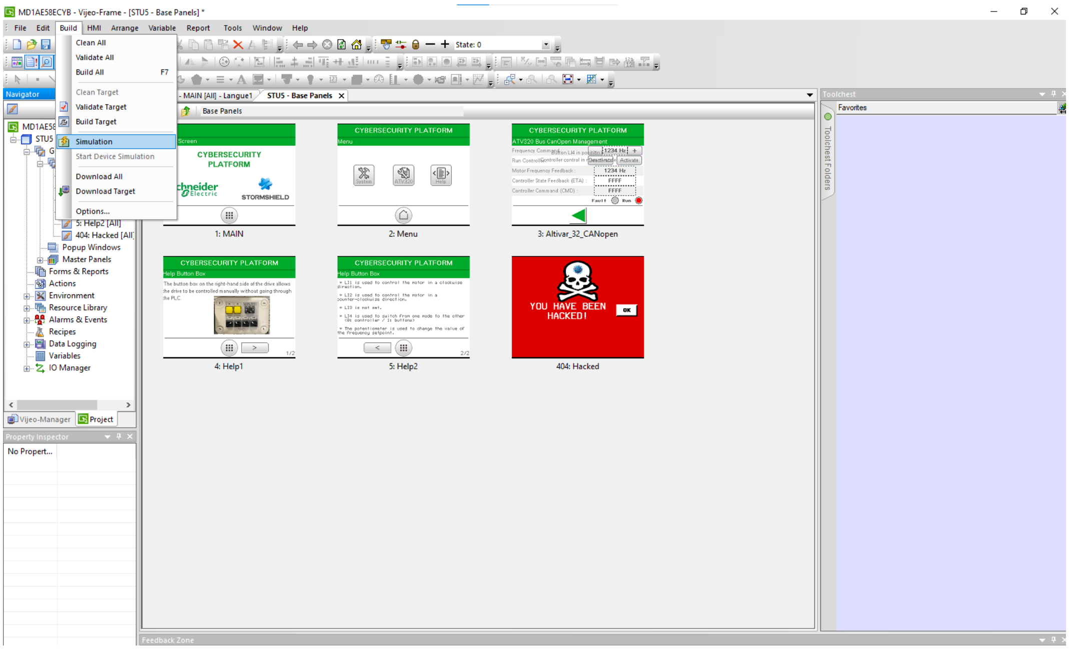
Variables | DDT Types | Function Blocks | DFB Types

Filter Name = * ☑ EDT □ DDT □ IODDT □ Device DDT

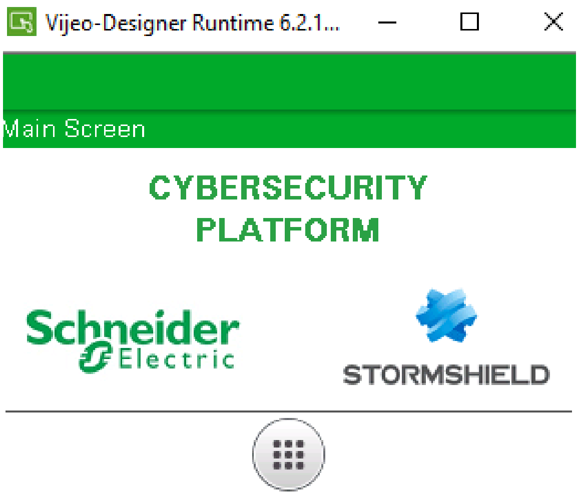
Name	Type	Value	Comment	Alias	Alias of	Address	HMI variable
ATV32_Control	UINT		Control of the Control...		CAN3_d1_ATV320...		☑
ATV32_Courant_Moteur	INT		HMI : Motor Current			%MW1020	☑
ATV32_Frequence_Moteur	INT		HMI : Motor Frequen...			%MW1012	☑
ATV32_Retour_Fréquence	UINT		Frequency Feedbac...		CAN3_d1_ATV320...		☑
ATV32_Status	UINT		Controller Status		CAN3_d1_ATV320...		☑
ATV32_Status_Emergency...	BOOL		Emergency Stop Sta...				☑
ATV32_Status_Fault	BOOL		Fault Status of the C...				☑
ATV32_Status_Op_Enabled	BOOL		Activate/Deactivatio...				☑
ATV32_Target_Velocity	INT		Target Velocity of th...		CAN3_d1_ATV320...		☑
Base_de_Temps_1s	BOOL		Time Base of 1 seco...			%S6	□
curpanel	INT		HMI : Current Panel ...			%MW2	☑
IHM_ATV32_Accel	INT		HMI : Velocity Accel...			%MW1015	□
IHM_ATV32_BP_Acquit	EBOOL		HMI : Press Button A...			%M103	☑
IHM_ATV32_BP_Arret_visi...	EBOOL		HMI : Press Button V...			%M300	□
IHM_ATV32_BP_Arrêt	EBOOL		HMI : Press Button S...			%M102	☑
IHM_ATV32_BP_Marche	EBOOL		HMI : Press Button ...			%M100	☑
IHM_ATV32_BP_Marche_v...	EBOOL		HMI : Press Button ...			%M301	□
IHM_ATV32_Consigne	INT		HMI : Speed Comma...			%MW1014	☑
IHM_ATV32_Decel	INT		HMI : Velocity Decel...			%MW1016	☑
IHM_Del	EBOOL		HMI : Delete			%M12	□
IHM_Panel_to_Display_ID	INT		HMI : Number of the ...			%MW18	☑
							□

- Also, ensure that the ePAC (main address 192.168.0.1) is accessible via a Modbus request. Check that a read access on the word %MW1014 (which corresponds to the drive speed setpoint address) gives the same value as the one identified via Control Expert.

Use the Vijeo Designer application, running in Simulation mode on the working PC



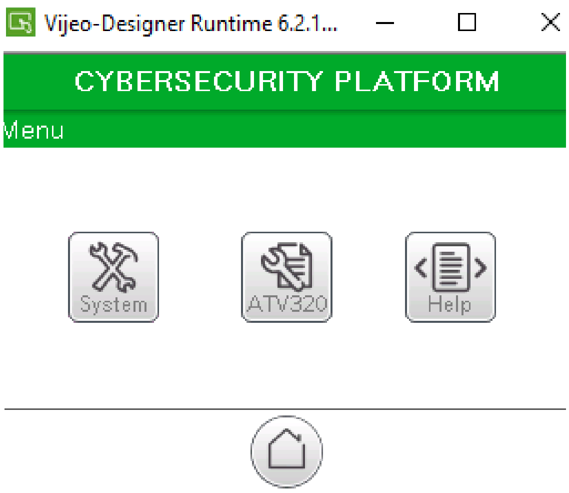
- The welcome screen displayed by the simulator is as follows:



Vijeo-Designer Runtime 6.2.1...

Main Screen

CYBERSECURITY PLATFORM



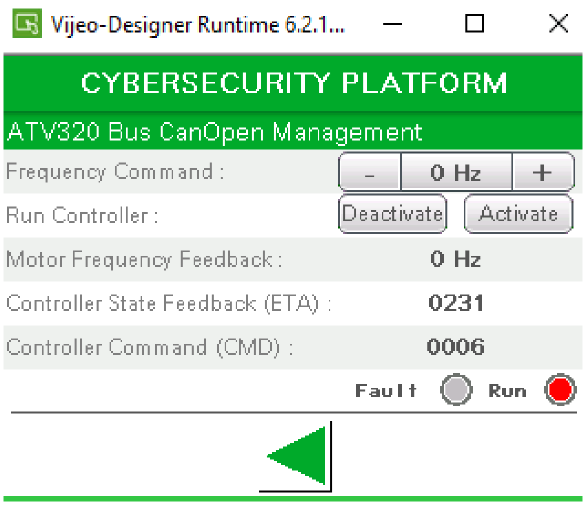
Vijeo-Designer Runtime 6.2.1...

CYBERSECURITY PLATFORM

Menu

- Click on the **ATV32** button.

  Proceed as on the HMI to control the drive



Vijeo-Designer Runtime 6.2.1...

CYBERSECURITY PLATFORM

ATV320 Bus CanOpen Management

Frequency Command : - 0 Hz +

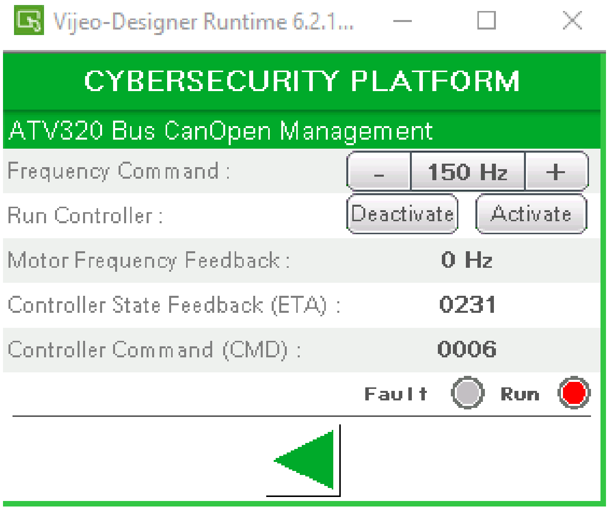
Run Controller : Deactivate Activate

Motor Frequency Feedback : 0 Hz

Controller State Feedback (ETA) : 0231

Controller Command (CMD) : 0006

Fault ○ Run ●



Vijeo-Designer Runtime 6.2.1...

CYBERSECURITY PLATFORM

ATV320 Bus CanOpen Management

Frequency Command : - 150 Hz +

Run Controller : Deactivate Activate

Motor Frequency Feedback : 0 Hz

Controller State Feedback (ETA) : 0231

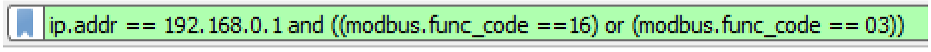
Controller Command (CMD) : 0006

Fault ○ Run ●

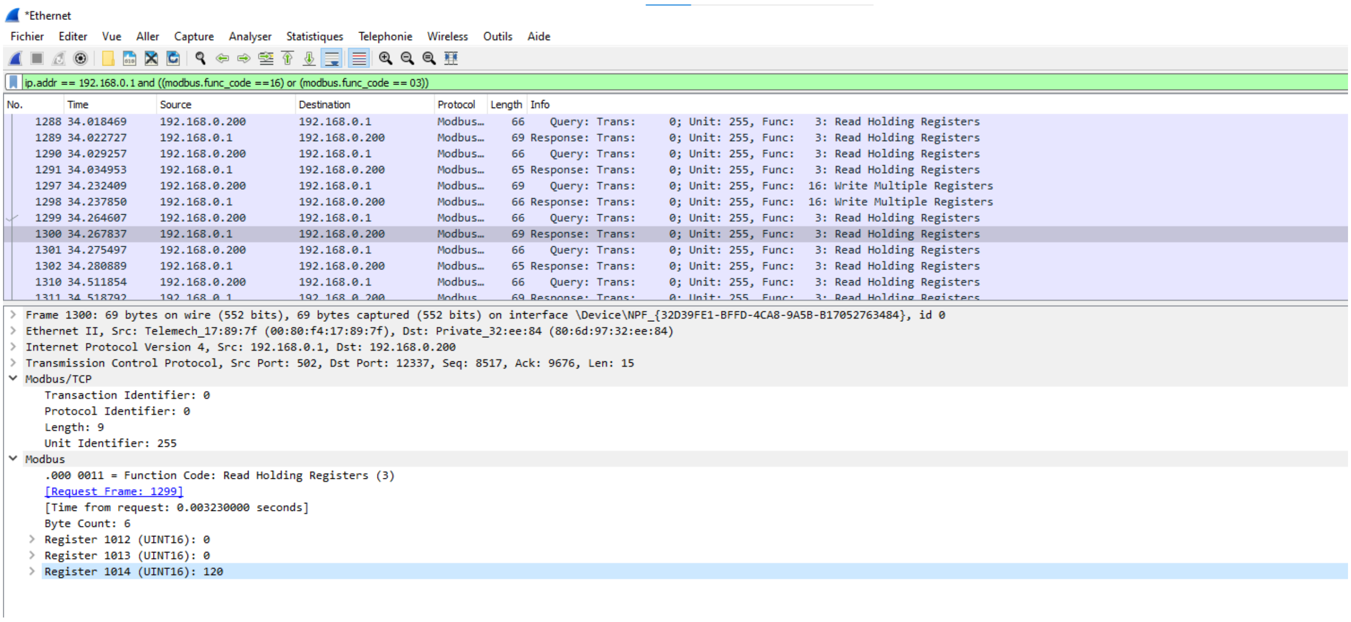
- Check via Wireshark, that Modbus/TCP frames are exchanged between My Computer and the M580 CPU.

  We are going to filter all the frames captured by this expression:

  ip.addr == 192.168.0.1 and ((modbus.func_code ==16) or (modbus.func_code == 03))



ip.addr == 192.168.0.1 and ((modbus.func_code ==16) or (modbus.func_code == 03))



```
ip.addr == 192.168.0.1 and ((modbus.func_code ==16) or (modbus.func_code == 03))

No.  Time          Source          Destination     Protocol  Length Info
1288 34.018469     192.168.0.200   192.168.0.1     Modbus…   66    Query: Trans:    0; Unit: 255, Func:  3: Read Holding Registers
1289 34.022727     192.168.0.1     192.168.0.200   Modbus…   69 Response: Trans:    0; Unit: 255, Func:  3: Read Holding Registers
1290 34.029257     192.168.0.200   192.168.0.1     Modbus…   66    Query: Trans:    0; Unit: 255, Func:  3: Read Holding Registers
1291 34.034953     192.168.0.1     192.168.0.200   Modbus…   65 Response: Trans:    0; Unit: 255, Func:  3: Read Holding Registers
1297 34.232409     192.168.0.200   192.168.0.1     Modbus…   69    Query: Trans:    0; Unit: 255, Func: 16: Write Multiple Registers
1298 34.237850     192.168.0.1     192.168.0.200   Modbus…   66 Response: Trans:    0; Unit: 255, Func: 16: Write Multiple Registers
1299 34.264607     192.168.0.200   192.168.0.1     Modbus…   66    Query: Trans:    0; Unit: 255, Func:  3: Read Holding Registers
1300 34.267837     192.168.0.1     192.168.0.200   Modbus…   69 Response: Trans:    0; Unit: 255, Func:  3: Read Holding Registers
1301 34.275497     192.168.0.200   192.168.0.1     Modbus…   66    Query: Trans:    0; Unit: 255, Func:  3: Read Holding Registers
1302 34.280889     192.168.0.1     192.168.0.200   Modbus…   65 Response: Trans:    0; Unit: 255, Func:  3: Read Holding Registers
1310 34.511854     192.168.0.200   192.168.0.1     Modbus…   66    Query: Trans:    0; Unit: 255, Func:  3: Read Holding Registers
1311 34.518792     192.168.0.1     192.168.0.200   Modbus…   69 Response: Trans:    0; Unit: 255, Func:  3: Read Holding Registers

> Frame 1300: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Telemech_17:89:7f (00:80:f4:17:89:7f), Dst: Private_32:ee:84 (80:6d:97:32:ee:84)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.200
> Transmission Control Protocol, Src Port: 502, Dst Port: 12337, Seq: 8517, Ack: 9676, Len: 15
v Modbus/TCP
    Transaction Identifier: 0
    Protocol Identifier: 0
    Length: 9
    Unit Identifier: 255
v Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    [Request Frame: 1299]
    [Time from request: 0.003230000 seconds]
    Byte Count: 6
  > Register 1012 (UINT16): 0
  > Register 1013 (UINT16): 0
  > Register 1014 (UINT16): 120
```

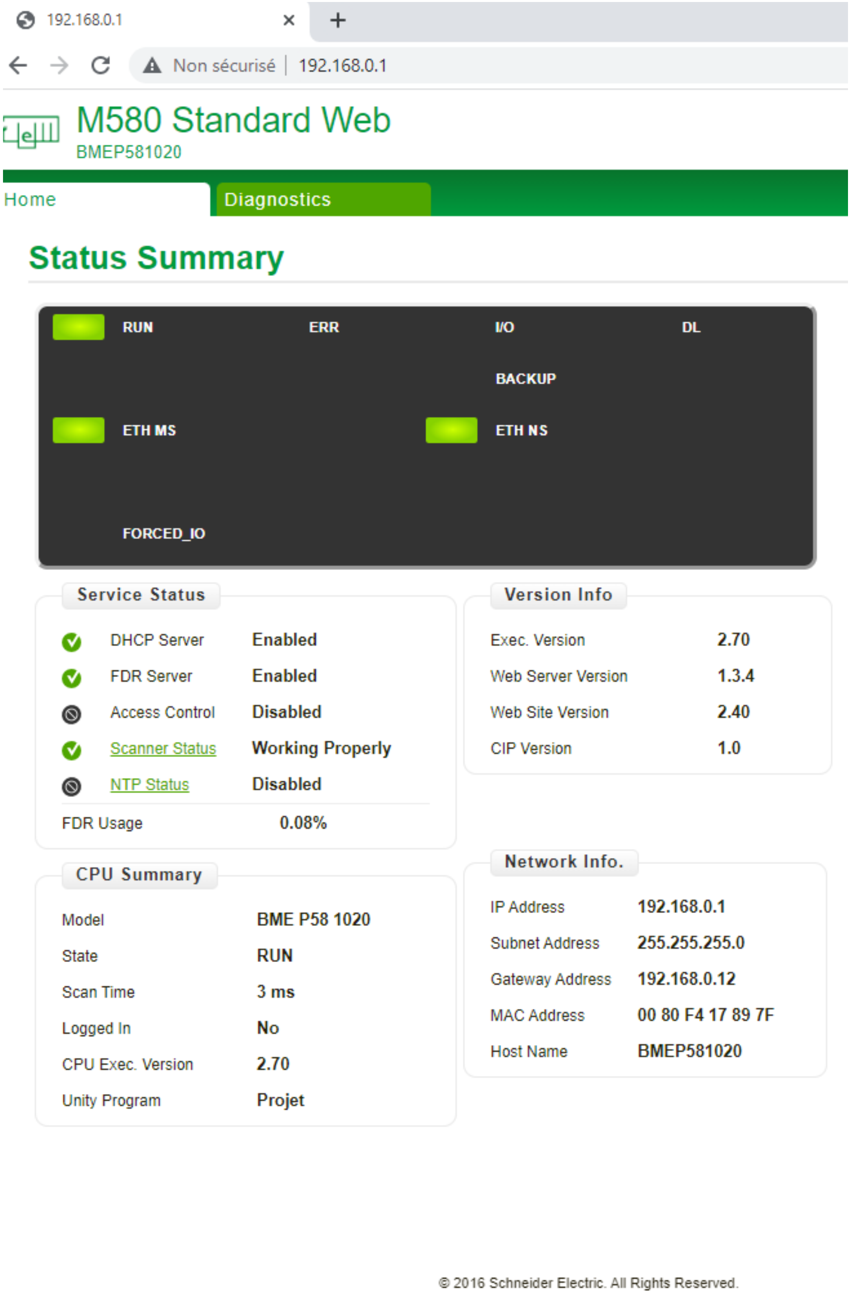
Example: Cyclic multiple register read frame (function code 03) and specific multiple register write frame (function code 16)

- Discontinue the Vijeo Designer Simulation after use.

4.2. Access to HTML pages served by the M580 CPU (HTTP protocol)

- From Internet Explorer (the Internet browser of choice for web servers built into Schneider Electric PLCs), enter the IP address of the main CPU port.

Check that the machine responds, and allows browsing of the HTML pages served.



M580 Standard Web
BMEP581020

Status Summary

🟩 RUN	ERR	I/O	DL
		BACKUP	
🟩 ETH MS		🟩 ETH NS	
FORCED_IO			

Service Status

✓	DHCP Server	Enabled
✓	FDR Server	Enabled
⊘	Access Control	Disabled
✓	Scanner Status	Working Properly
⊘	NTP Status	Disabled
	FDR Usage	0.08%

Version Info

Exec. Version	2.70
Web Server Version	1.3.4
Web Site Version	2.40
CIP Version	1.0

CPU Summary

Model	BME P58 1020
State	RUN
Scan Time	3 ms
Logged In	No
CPU Exec. Version	2.70
Unity Program	Projet

Network Info.

IP Address	192.168.0.1
Subnet Address	255.255.255.0
Gateway Address	192.168.0.12
MAC Address	00 80 F4 17 89 7F
Host Name	BMEP581020

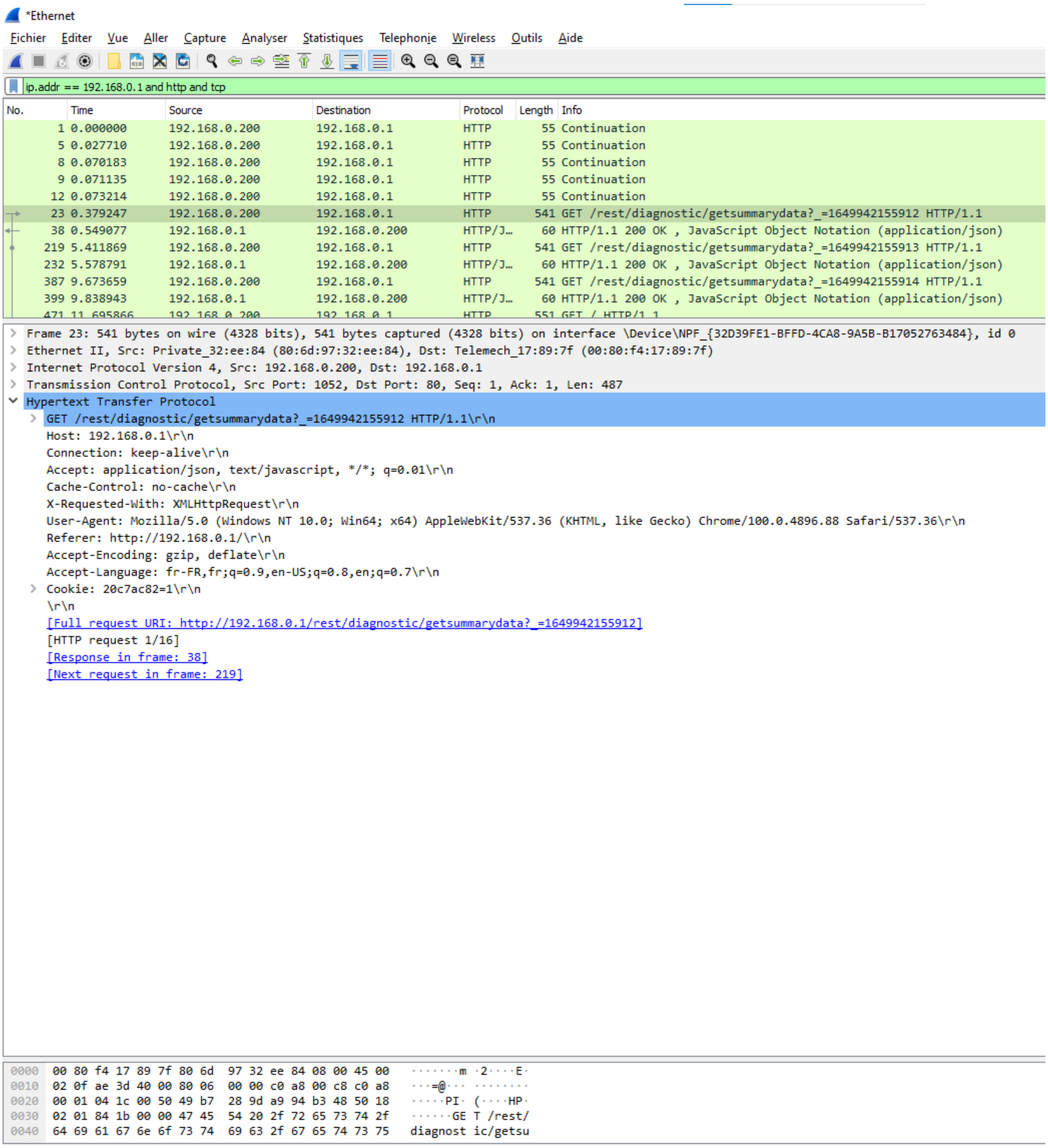
© 2016 Schneider Electric. All Rights Reserved.

- Check via Wireshark, that HHTP frames are exchanged between Workstation and M580 CPU.

  We are going to filter by the following expression:

  ip.addr == 192.168.0.1 and http and tcp

ip.addr == 192.168.0.1 and http and tcp


*Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

```
ip.addr == 192.168.0.1 and http and tcp
```

```
No.   Time      Source         Destination    Protocol Length Info
    1 0.000000  192.168.0.200  192.168.0.1    HTTP       55 Continuation
    5 0.027710  192.168.0.200  192.168.0.1    HTTP       55 Continuation
    8 0.070183  192.168.0.200  192.168.0.1    HTTP       55 Continuation
    9 0.071135  192.168.0.200  192.168.0.1    HTTP       55 Continuation
   12 0.073214  192.168.0.200  192.168.0.1    HTTP       55 Continuation
   23 0.379247  192.168.0.200  192.168.0.1    HTTP      541 GET /rest/diagnostic/getsummarydata?_=1649942155912 HTTP/1.1
   38 0.549077  192.168.0.1    192.168.0.200  HTTP/J…    60 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
  219 5.411869  192.168.0.200  192.168.0.1    HTTP      541 GET /rest/diagnostic/getsummarydata?_=1649942155913 HTTP/1.1
  232 5.578791  192.168.0.1    192.168.0.200  HTTP/J…    60 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
  387 9.673659  192.168.0.200  192.168.0.1    HTTP      541 GET /rest/diagnostic/getsummarydata?_=1649942155914 HTTP/1.1
  399 9.838943  192.168.0.1    192.168.0.200  HTTP/J…    60 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
  471 11.695866 192.168.0.200  192.168.0.1    HTTP      551 GET / HTTP/1.1
```

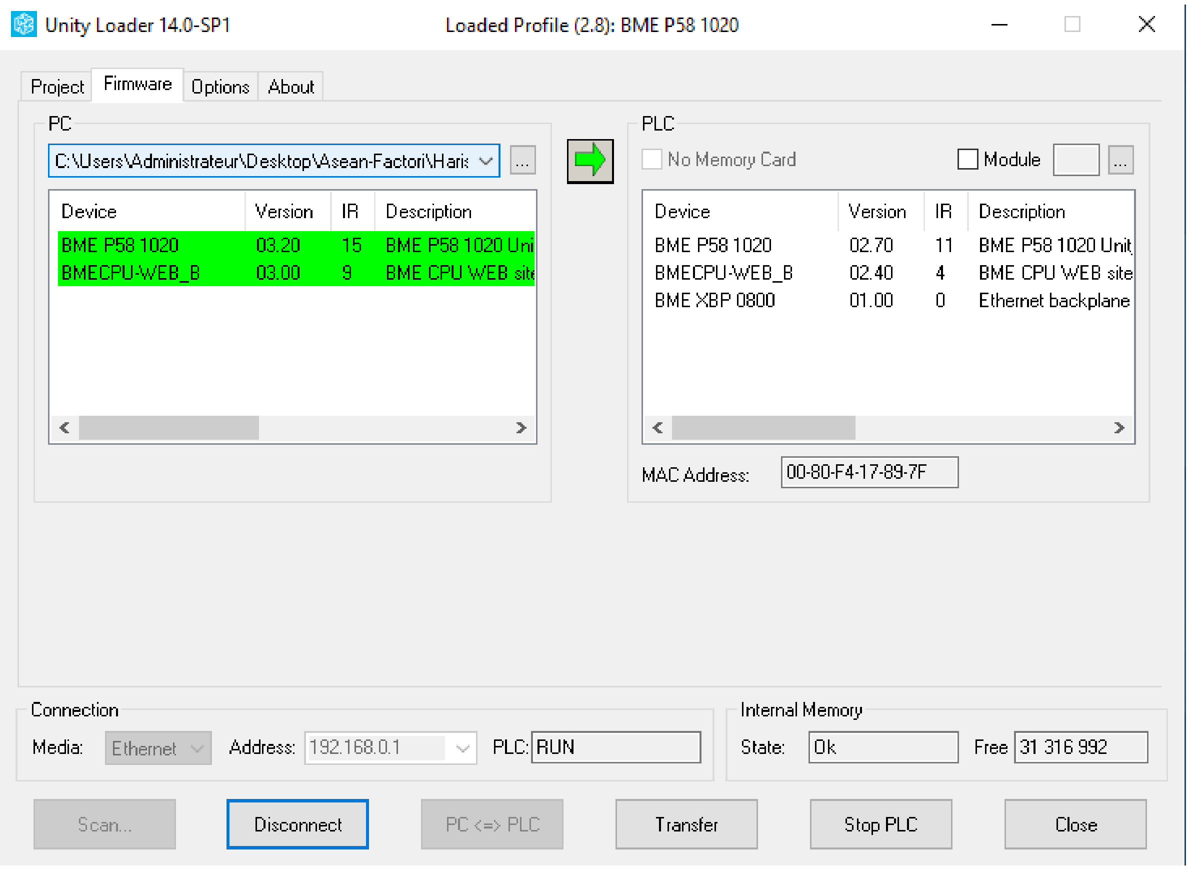
```
> Frame 23: 541 bytes on wire (4328 bits), 541 bytes captured (4328 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Private_32:ee:84 (80:6d:97:32:ee:84), Dst: Telemech_17:89:7f (00:80:f4:17:89:7f)
> Internet Protocol Version 4, Src: 192.168.0.200, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 1052, Dst Port: 80, Seq: 1, Ack: 1, Len: 487
v Hypertext Transfer Protocol
  > GET /rest/diagnostic/getsummarydata?_=1649942155912 HTTP/1.1\r\n
    Host: 192.168.0.1\r\n
    Connection: keep-alive\r\n
    Accept: application/json, text/javascript, */*; q=0.01\r\n
    Cache-Control: no-cache\r\n
    X-Requested-With: XMLHttpRequest\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.88 Safari/537.36\r\n
    Referer: http://192.168.0.1/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7\r\n
  > Cookie: 20c7ac82=1\r\n
    \r\n
    [Full request URI: http://192.168.0.1/rest/diagnostic/getsummarydata?_=1649942155912]
    [HTTP request 1/16]
    [Response in frame: 38]
    [Next request in frame: 219]
```

```
0000  00 80 f4 17 89 7f 80 6d  97 32 ee 84 08 00 45 00   ·······m ·2····E·
0010  02 0f ae 3d 40 00 80 06  00 00 c0 a8 00 c8 c0 a8   ···=@··· ········
0020  00 01 04 1c 00 50 49 b7  28 9d a9 94 b3 48 50 18   ·····PI· (····HP·
0030  02 01 84 1b 00 00 47 45  54 20 2f 72 65 73 74 2f   ······GE T /rest/
0040  64 69 61 67 6e 6f 73 74  69 63 2f 67 65 74 73 75   diagnost ic/getsu
```

- Quit the browser after use.

4.3. Access to the M580 CPU firmware download service (FTP protocol)

- Launch Unity Loader, go to the second tab (Firmware) and connect to the M580 CPU via Ethernet.



Unity Loader 14.0-SP1 Loaded Profile (2.8): BME P58 1020

PC

C:\Users\Administrateur\Desktop\Asean-Factori\Haris

Device	Version	IR	Description
BME P58 1020	03.20	15	BME P58 1020 Uni
BMECPU-WEB_B	03.00	9	BME CPU WEB site

PLC

□ No Memory Card □ Module

Device	Version	IR	Description
BME P58 1020	02.70	11	BME P58 1020 Unit
BMECPU-WEB_B	02.40	4	BME CPU WEB site
BME XBP 0800	01.00	0	Ethernet backplane

MAC Address: 00-80-F4-17-89-7F

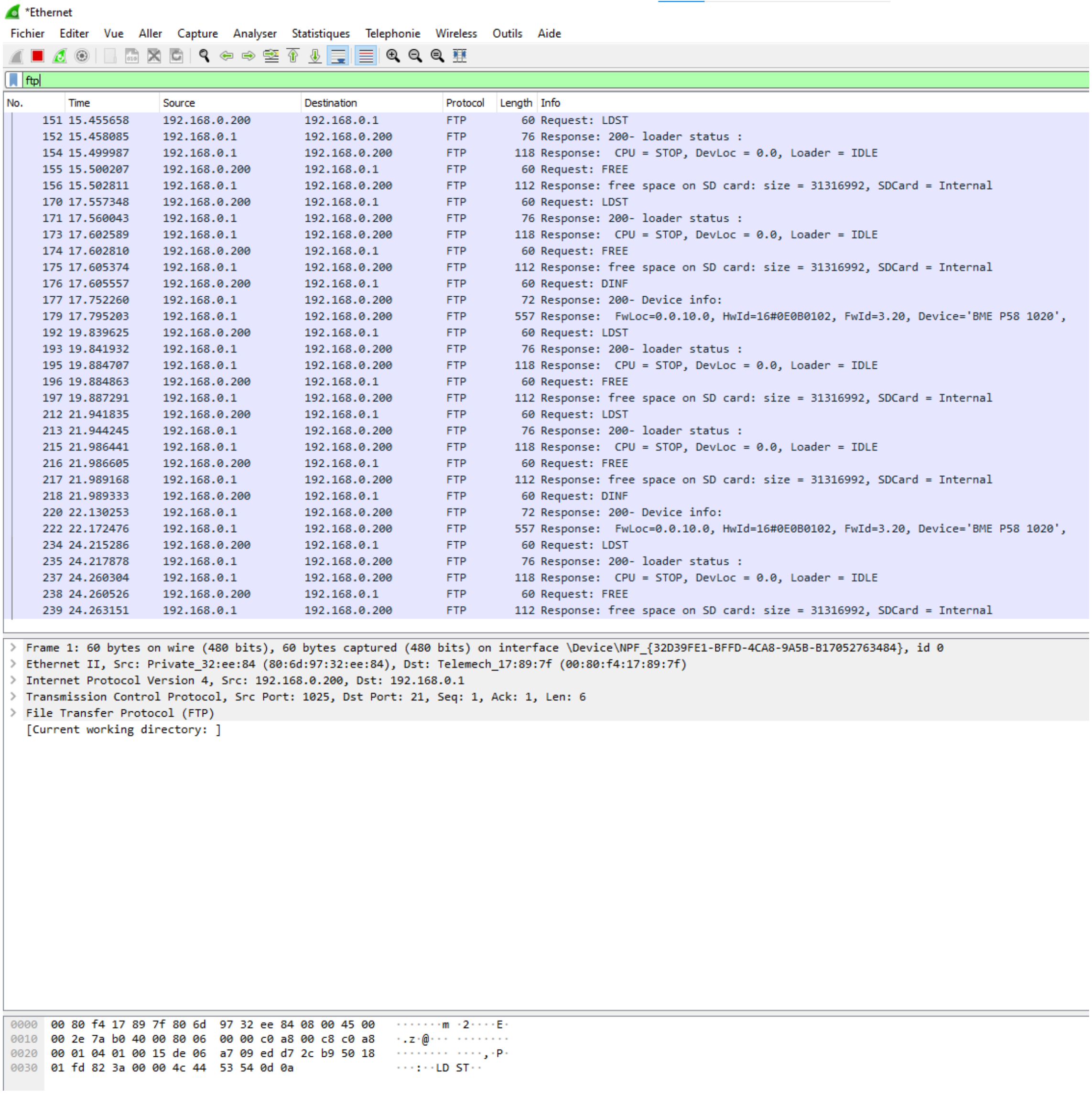
Connection

Media: Ethernet Address: 192.168.0.1 PLC: RUN

Internal Memory

State: Ok Free 31 316 992

- Check via Wireshark, that FTP frames are exchanged between My Computer and M580 CPU.



```
ftp
```

```
No.   Time       Source         Destination    Protocol Length Info
  151 15.455658  192.168.0.200  192.168.0.1    FTP        60 Request: LDST
  152 15.458085  192.168.0.1    192.168.0.200  FTP        76 Response: 200- loader status :
  154 15.499987  192.168.0.1    192.168.0.200  FTP       118 Response:  CPU = STOP, DevLoc = 0.0, Loader = IDLE
  155 15.500207  192.168.0.200  192.168.0.1    FTP        60 Request: FREE
  156 15.502811  192.168.0.1    192.168.0.200  FTP       112 Response: free space on SD card: size = 31316992, SDCard = Internal
  170 17.557348  192.168.0.200  192.168.0.1    FTP        60 Request: LDST
  171 17.560043  192.168.0.1    192.168.0.200  FTP        76 Response: 200- loader status :
  173 17.602589  192.168.0.1    192.168.0.200  FTP       118 Response:  CPU = STOP, DevLoc = 0.0, Loader = IDLE
  174 17.602810  192.168.0.200  192.168.0.1    FTP        60 Request: FREE
  175 17.605374  192.168.0.1    192.168.0.200  FTP       112 Response: free space on SD card: size = 31316992, SDCard = Internal
  176 17.605557  192.168.0.200  192.168.0.1    FTP        60 Request: DINF
  177 17.752260  192.168.0.1    192.168.0.200  FTP        72 Response: 200- Device info:
  179 17.795203  192.168.0.1    192.168.0.200  FTP       557 Response:  FwLoc=0.0.10.0, HwId=16#0E0B0102, FwId=3.20, Device='BME P58 1020',
  192 19.839625  192.168.0.200  192.168.0.1    FTP        60 Request: LDST
  193 19.841932  192.168.0.1    192.168.0.200  FTP        76 Response: 200- loader status :
  195 19.884707  192.168.0.1    192.168.0.200  FTP       118 Response:  CPU = STOP, DevLoc = 0.0, Loader = IDLE
  196 19.884863  192.168.0.200  192.168.0.1    FTP        60 Request: FREE
  197 19.887291  192.168.0.1    192.168.0.200  FTP       112 Response: free space on SD card: size = 31316992, SDCard = Internal
  212 21.941835  192.168.0.200  192.168.0.1    FTP        60 Request: LDST
  213 21.944245  192.168.0.1    192.168.0.200  FTP        76 Response: 200- loader status :
  215 21.986441  192.168.0.1    192.168.0.200  FTP       118 Response:  CPU = STOP, DevLoc = 0.0, Loader = IDLE
  216 21.986605  192.168.0.200  192.168.0.1    FTP        60 Request: FREE
  217 21.989168  192.168.0.1    192.168.0.200  FTP       112 Response: free space on SD card: size = 31316992, SDCard = Internal
  218 21.989333  192.168.0.200  192.168.0.1    FTP        60 Request: DINF
  220 22.130253  192.168.0.1    192.168.0.200  FTP        72 Response: 200- Device info:
  222 22.172476  192.168.0.1    192.168.0.200  FTP       557 Response:  FwLoc=0.0.10.0, HwId=16#0E0B0102, FwId=3.20, Device='BME P58 1020',
  234 24.215286  192.168.0.200  192.168.0.1    FTP        60 Request: LDST
  235 24.217878  192.168.0.1    192.168.0.200  FTP        76 Response: 200- loader status :
  237 24.260304  192.168.0.1    192.168.0.200  FTP       118 Response:  CPU = STOP, DevLoc = 0.0, Loader = IDLE
  238 24.260526  192.168.0.200  192.168.0.1    FTP        60 Request: FREE
  239 24.263151  192.168.0.1    192.168.0.200  FTP       112 Response: free space on SD card: size = 31316992, SDCard = Internal
```

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Private_32:ee:84 (80:6d:97:32:ee:84), Dst: Telemech_17:89:7f (00:80:f4:17:89:7f)
> Internet Protocol Version 4, Src: 192.168.0.200, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 1025, Dst Port: 21, Seq: 1, Ack: 1, Len: 6
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  00 80 f4 17 89 7f 80 6d  97 32 ee 84 08 00 45 00   ·······m ·2····E·
0010  00 2e 7a b0 40 00 80 06  00 00 c0 a8 00 c8 c0 a8   ·.z·@··· ········
0020  00 01 04 01 00 15 de 06  a7 09 ed d7 2c b9 50 18   ········ ····,·P·
0030  01 fd 82 3a 00 00 4c 44  53 54 0d 0a               ···:··LD ST··
```

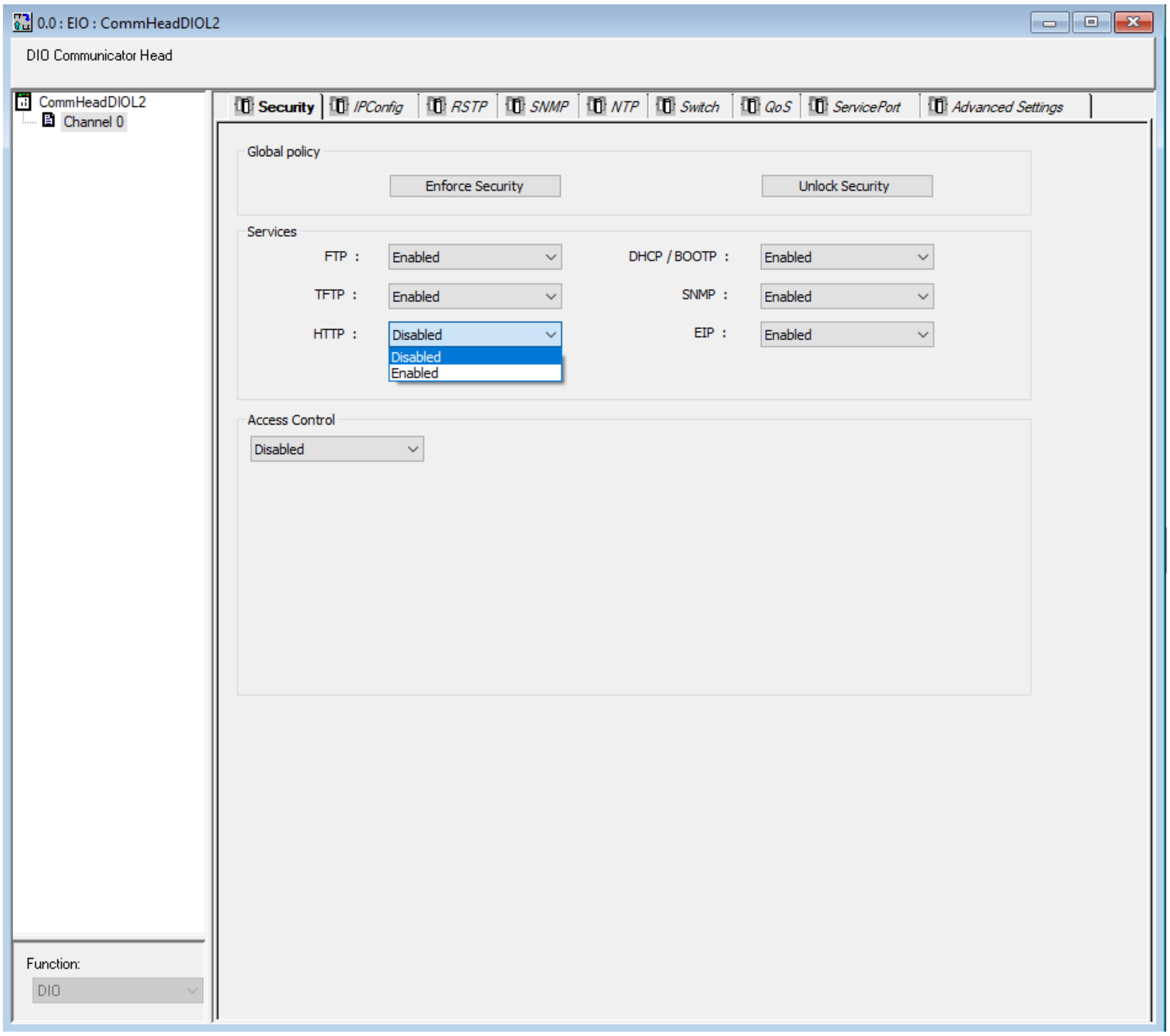
Disconnect from the M580 CPU after use.

5. Selective inhibition, by configuration, of the HTTP and FTP services of the Central Unit

5.1. Access to HTML pages served by the M580 CPU (HTTP protocol)

- With Control Expert, in off-line mode, in the M580 CPU configuration, and open the section presenting itself as the EIO Bus configuration section.

Disable the HTTP protocol service



FTP : Enabled

TFTP : Enabled

HTTP : Disabled

DHCP / BOOTP : Enabled

SNMP : Enabled

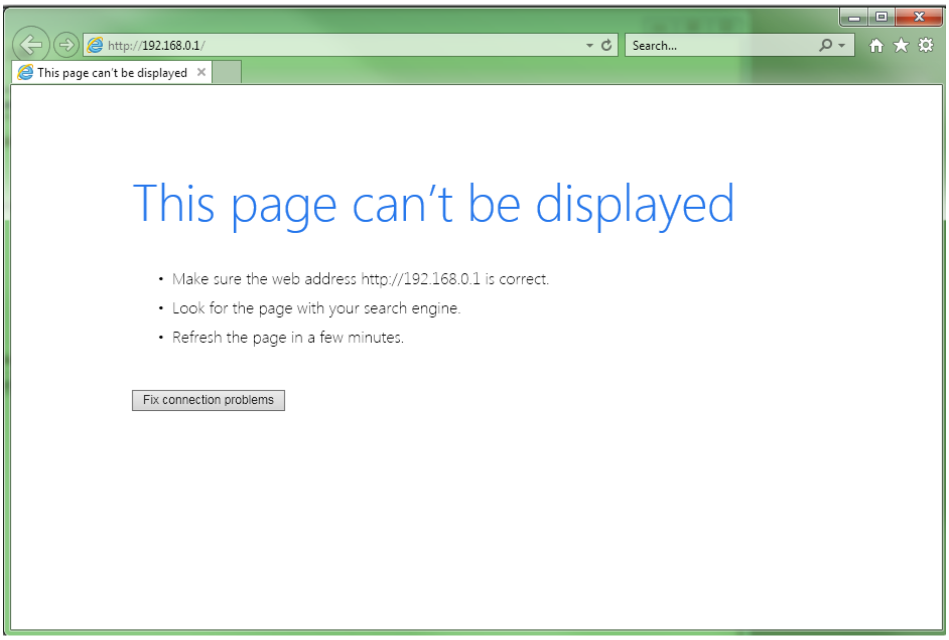
EIP : Enabled

Access Control: Disabled

Validate this configuration modification (Ctrl-W), generate, load the PLC and put it in run.

- From Internet Explorer, enter the IP address of the main CPU port.

  Check that, under these conditions, the PLC CPU does not allow browsing its HTML pages.

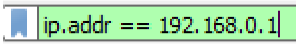


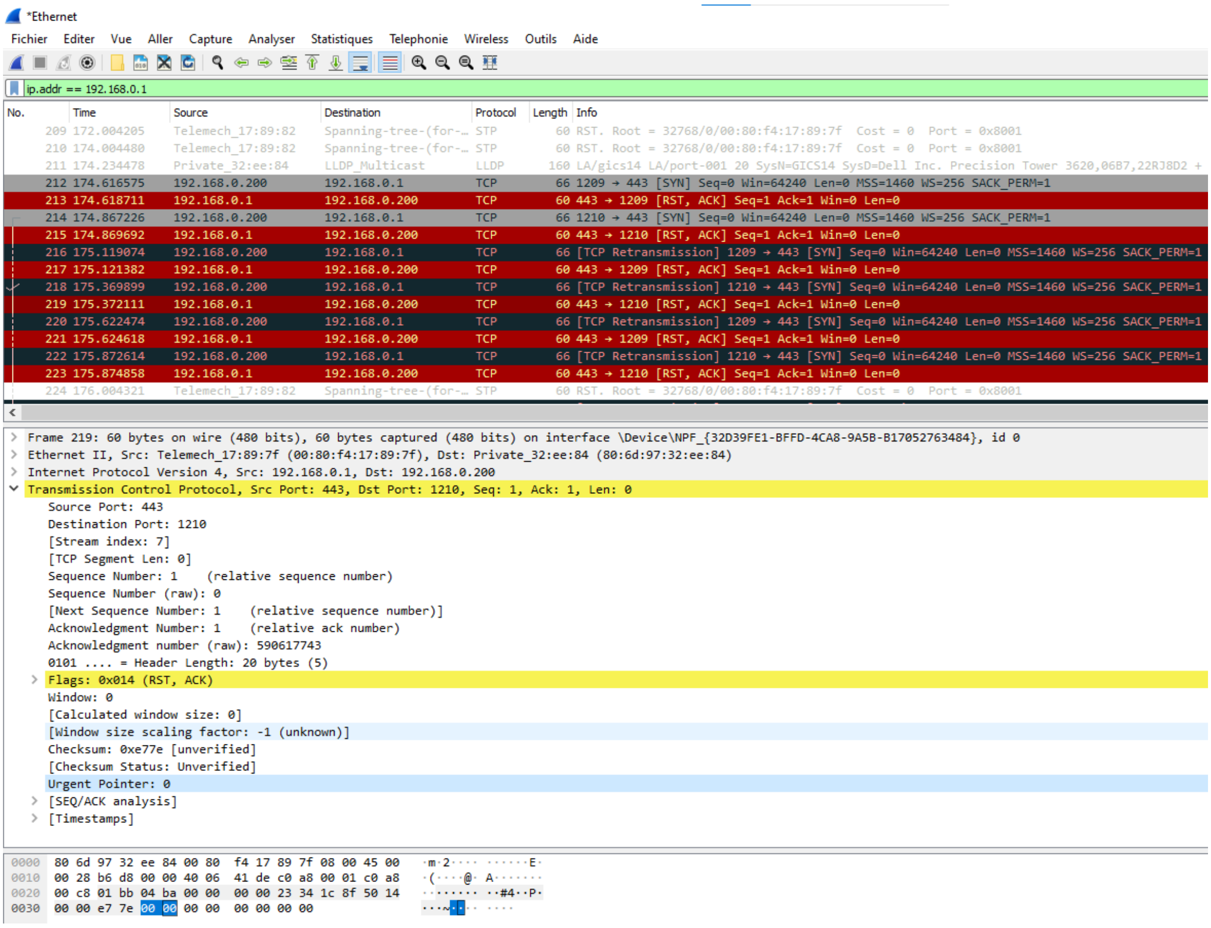
This page can't be displayed

- Make sure the web address http://192.168.0.1 is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

- Check via Wireshark that, given the current configuration of the Ethernet port of the M580 CPU, there are no HTTP frame exchanges with the workstation

Filter the results by: **ip.addr == 192.168.0.1**


ip.addr == 192.168.0.1


*Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

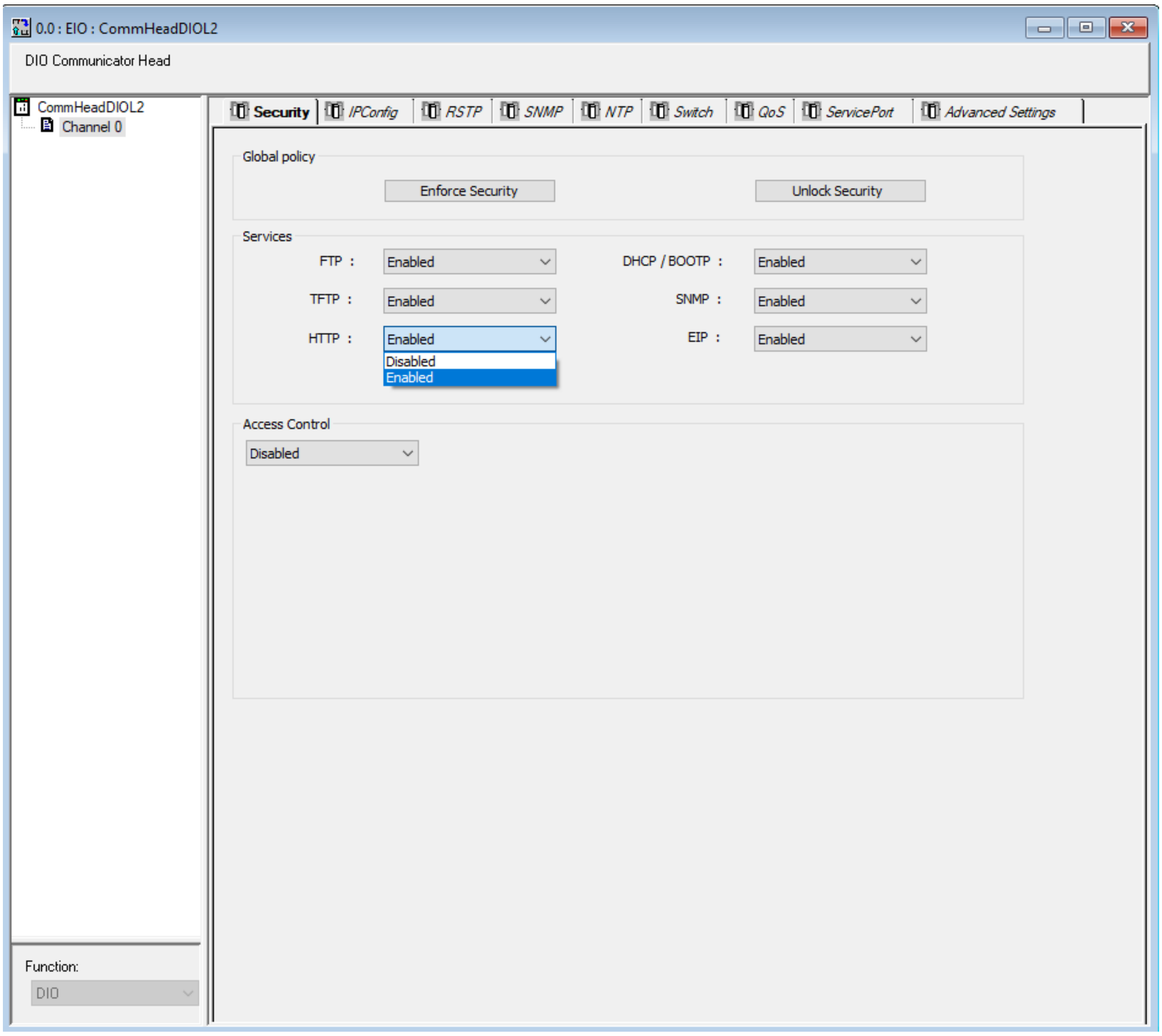
```
ip.addr == 192.168.0.1

No.   Time        Source             Destination          Protocol Length Info
  209 172.004205  Telemech_17:89:82  Spanning-tree-(for-… STP      60 RST. Root = 32768/0/00:80:f4:17:89:7f  Cost = 0  Port = 0x8001
  210 174.004480  Telemech_17:89:82  Spanning-tree-(for-… STP      60 RST. Root = 32768/0/00:80:f4:17:89:7f  Cost = 0  Port = 0x8001
  211 174.234478  Private_32:ee:84   LLDP_Multicast       LLDP    160 LA/gics14 LA/port-001 20 SysN=GICS14 SysD=Dell Inc. Precision Tower 3620,06B7,22RJ8D2 +
  212 174.616575  192.168.0.200      192.168.0.1          TCP      66 1209 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  213 174.618711  192.168.0.1        192.168.0.200        TCP      60 443 → 1209 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  214 174.867226  192.168.0.200      192.168.0.1          TCP      66 1210 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  215 174.869692  192.168.0.1        192.168.0.200        TCP      60 443 → 1210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  216 175.119074  192.168.0.200      192.168.0.1          TCP      66 [TCP Retransmission] 1209 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  217 175.121382  192.168.0.1        192.168.0.200        TCP      60 443 → 1209 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  218 175.369899  192.168.0.200      192.168.0.1          TCP      66 [TCP Retransmission] 1210 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  219 175.372111  192.168.0.1        192.168.0.200        TCP      60 443 → 1210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  220 175.622474  192.168.0.200      192.168.0.1          TCP      66 [TCP Retransmission] 1209 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  221 175.624618  192.168.0.1        192.168.0.200        TCP      60 443 → 1209 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  222 175.872614  192.168.0.200      192.168.0.1          TCP      66 [TCP Retransmission] 1210 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  223 175.874858  192.168.0.1        192.168.0.200        TCP      60 443 → 1210 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  224 176.004321  Telemech_17:89:82  Spanning-tree-(for-… STP      60 RST. Root = 32768/0/00:80:f4:17:89:7f  Cost = 0  Port = 0x8001
```

```
> Frame 219: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Telemech_17:89:7f (00:80:f4:17:89:7f), Dst: Private_32:ee:84 (80:6d:97:32:ee:84)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.200
v Transmission Control Protocol, Src Port: 443, Dst Port: 1210, Seq: 1, Ack: 1, Len: 0
    Source Port: 443
    Destination Port: 1210
    [Stream index: 7]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 0
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 590617743
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x014 (RST, ACK)
    Window: 0
    [Calculated window size: 0]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xe77e [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
```

```
0000  80 6d 97 32 ee 84 00 80  f4 17 89 7f 08 00 45 00   ·m·2···· ······E·
0010  00 28 b6 d8 00 00 40 06  41 de c0 a8 00 01 c0 a8   ·(····@· A·······
0020  00 c8 01 bb 04 ba 00 00  00 00 23 34 1c 8f 50 14   ········ ··#4··P·
0030  00 00 e7 7e 00 00 00 00  00 00 00 00               ···~···· ····
```

It can be seen that the ePAC M580 systematically rejects the attempts made by the Workstation with a reset request

- Re-enable the HTTP protocol service.

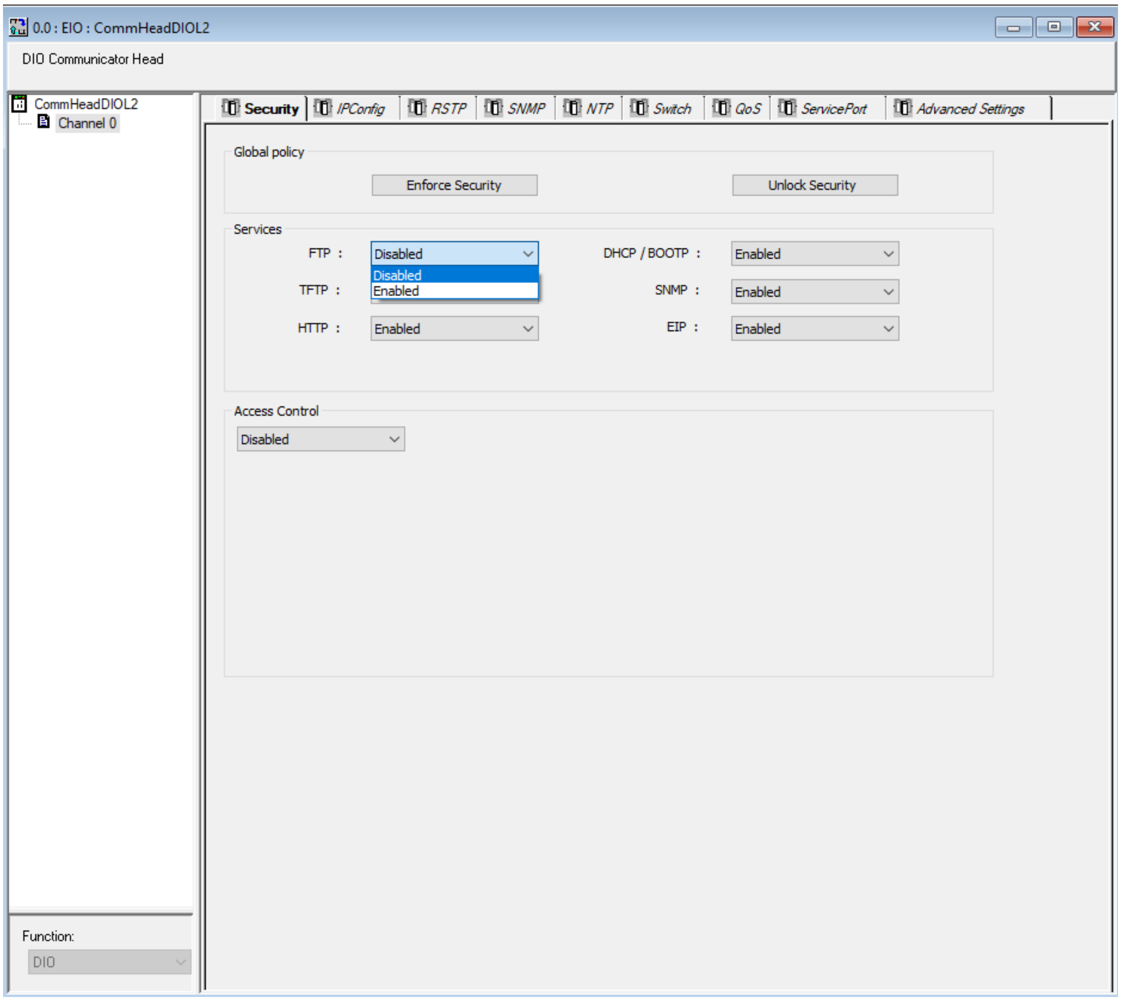


FTP : Enabled
TFTP : Enabled
HTTP : Enabled
DHCP / BOOTP : Enabled
SNMP : Enabled
EIP : Enabled
Access Control: Disabled

5.2. Access to the M580 CPU firmware download service (FTP protocol)

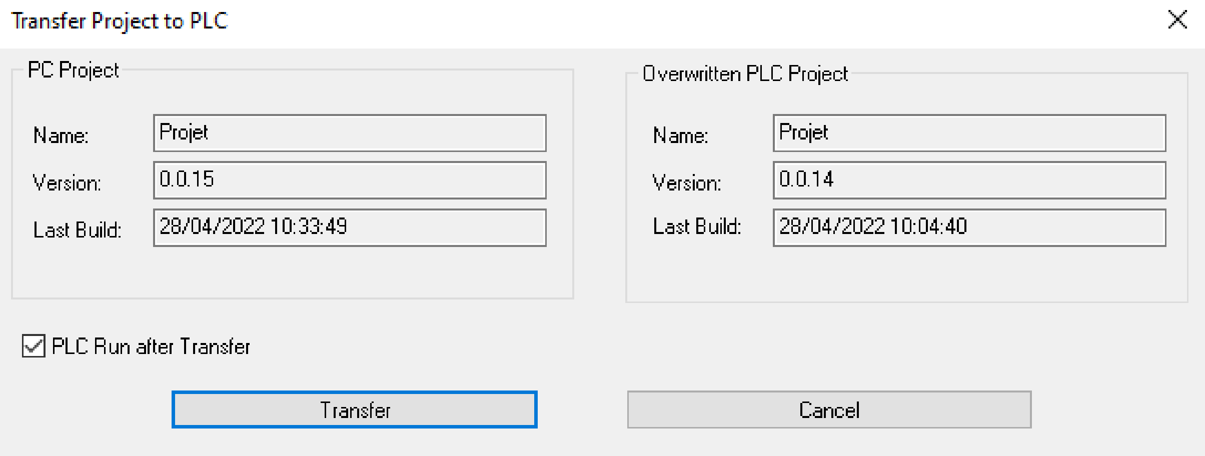
- Continuing with Unity, still in off-line mode, in the M580 CPU configuration, open the section presenting itself as the EIO Bus configuration section.

Disable the FTP protocol service.



FTP : Disabled (Disabled / Enabled)
TFTP :
HTTP : Enabled
DHCP / BOOTP : Enabled
SNMP : Enabled
EIP : Enabled
Access Control: Disabled

Validate this configuration modification (Ctrl-W), generate, load the PLC and put it in run.

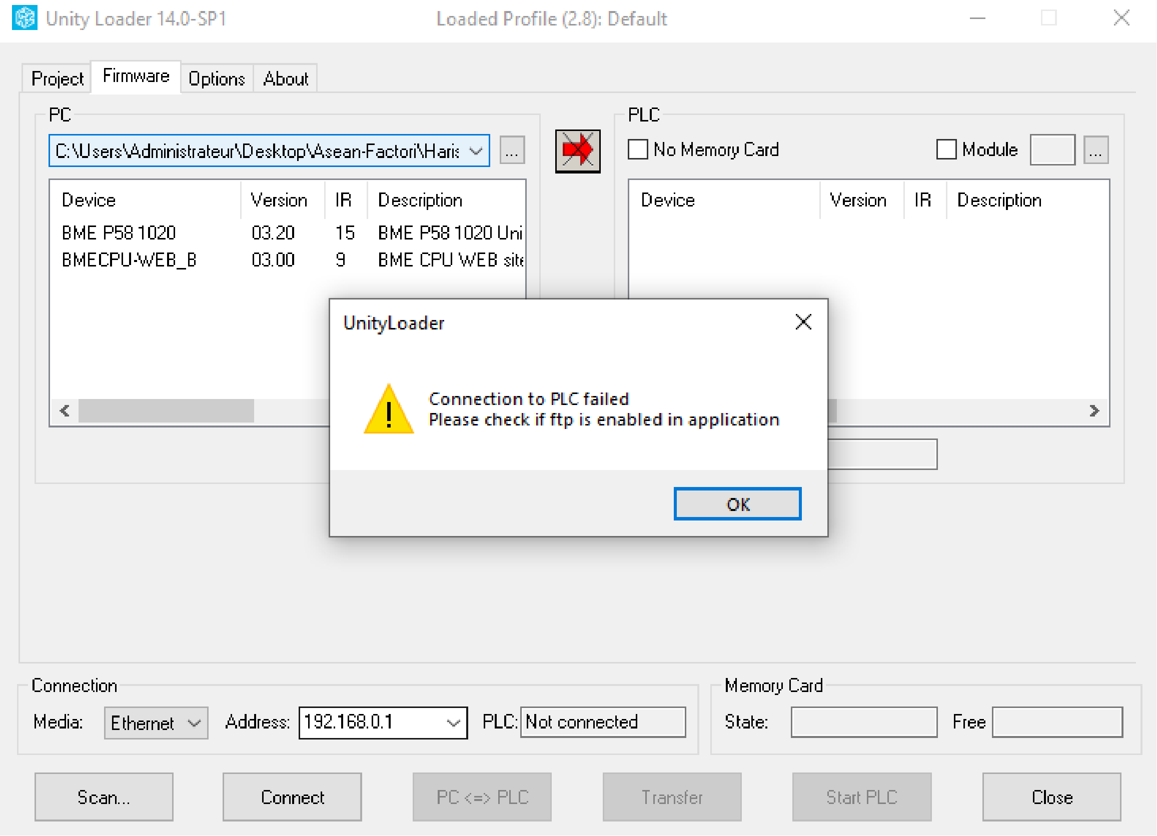


PC Project		Overwritten PLC Project	
Name:	Projet	Name:	Projet
Version:	0.0.15	Version:	0.0.14
Last Build:	28/04/2022 10:33:49	Last Build:	28/04/2022 10:04:40

☑ PLC Run after Transfer

Launch Unity Loader, go to the second tab (Firmware) and connect to the M580 CPU via Ethernet.

Check that, under these conditions, the PLC CPU does not allow any manipulation on the firmware side (neither read nor write).



C:\Users\Administrateur\Desktop\Asean-Factori\Haris

☐ No Memory Card ☐ Module

Device	Version	IR	Description
BME P58 1020	03.20	15	BME P58 1020 Uni
BMECPU-WEB_B	03.00	9	BME CPU WEB site

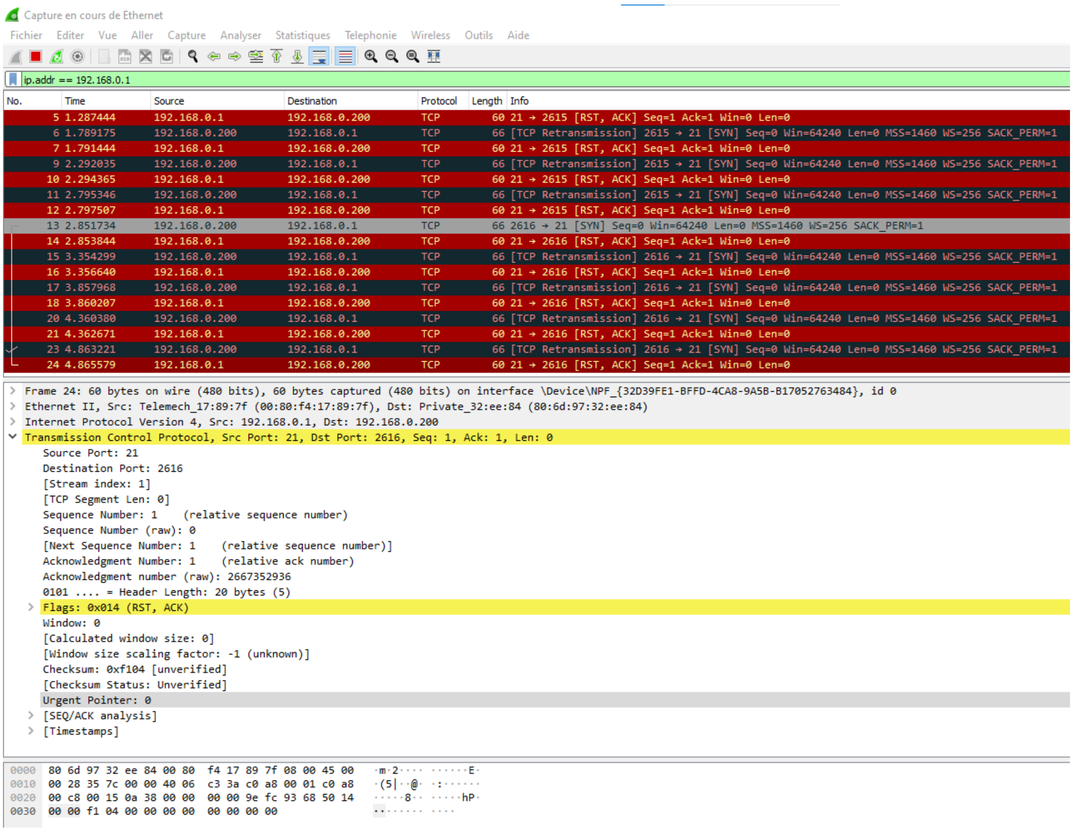
UnityLoader

Connection to PLC failed
Please check if ftp is enabled in application

Connection — Media: Ethernet Address: 192.168.0.1 PLC: Not connected

Memory Card — State: Free:

- Check via Wireshark that, given the current configuration of the Ethernet port of the M580 CPU, there are no FTP frame exchanges with the workstation


Capture en cours de Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

```
ip.addr == 192.168.0.1
```

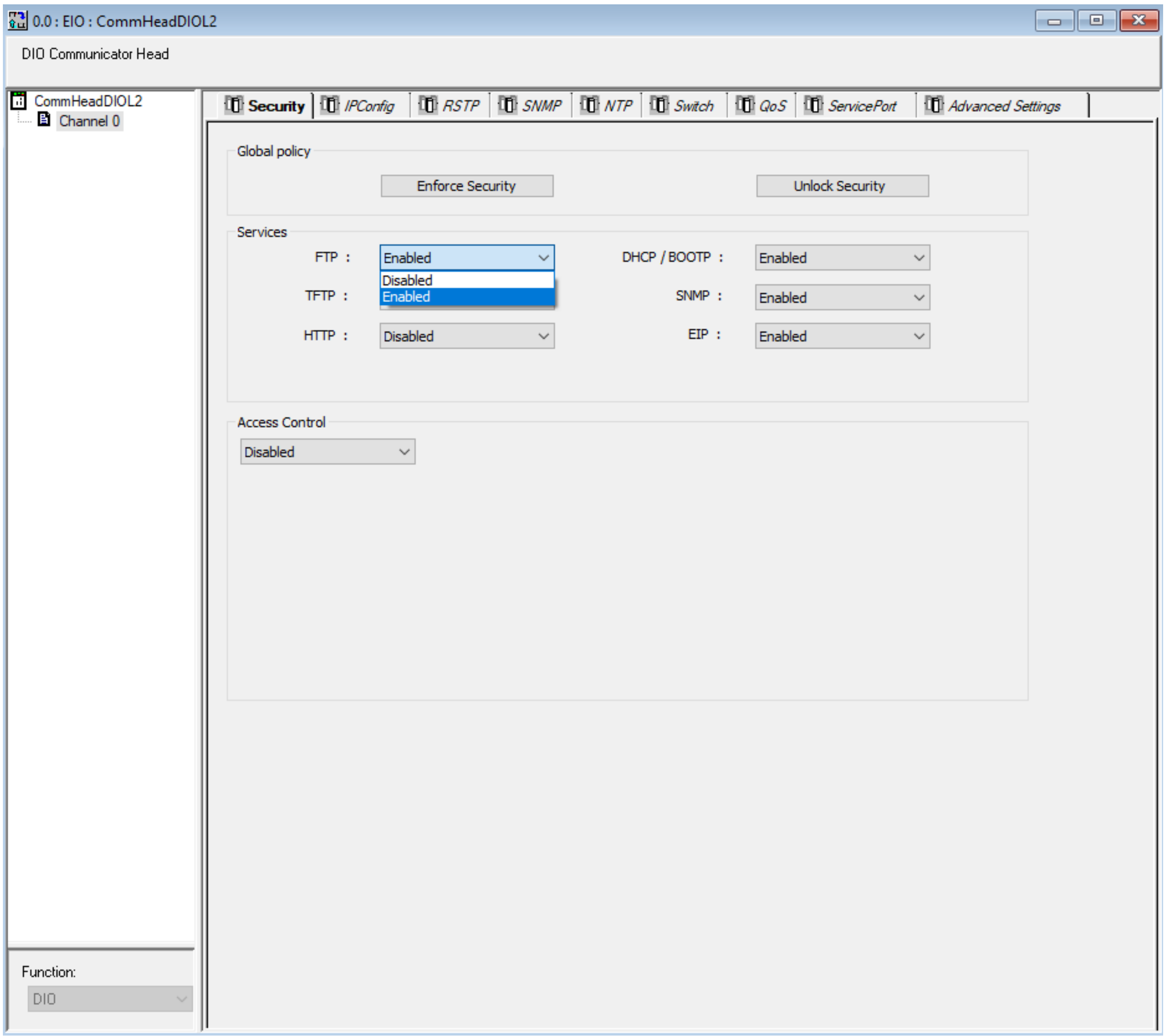
```
No.  Time       Source         Destination    Protocol Length Info
   5 1.287444   192.168.0.1    192.168.0.200  TCP      60 21 → 2615 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   6 1.789175   192.168.0.200  192.168.0.1    TCP      66 [TCP Retransmission] 2615 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   7 1.791444   192.168.0.1    192.168.0.200  TCP      60 21 → 2615 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   9 2.292035   192.168.0.200  192.168.0.1    TCP      66 [TCP Retransmission] 2615 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  10 2.294365   192.168.0.1    192.168.0.200  TCP      60 21 → 2615 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  11 2.795346   192.168.0.200  192.168.0.1    TCP      66 [TCP Retransmission] 2615 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  12 2.797507   192.168.0.1    192.168.0.200  TCP      60 21 → 2615 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  13 2.851734   192.168.0.200  192.168.0.1    TCP      66 2616 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  14 2.853844   192.168.0.1    192.168.0.200  TCP      60 21 → 2616 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  15 3.354299   192.168.0.200  192.168.0.1    TCP      66 [TCP Retransmission] 2616 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  16 3.356640   192.168.0.1    192.168.0.200  TCP      60 21 → 2616 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  17 3.857968   192.168.0.200  192.168.0.1    TCP      66 [TCP Retransmission] 2616 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  18 3.860207   192.168.0.1    192.168.0.200  TCP      60 21 → 2616 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  20 4.360380   192.168.0.200  192.168.0.1    TCP      66 [TCP Retransmission] 2616 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  21 4.362671   192.168.0.1    192.168.0.200  TCP      60 21 → 2616 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  23 4.863221   192.168.0.200  192.168.0.1    TCP      66 [TCP Retransmission] 2616 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  24 4.865579   192.168.0.1    192.168.0.200  TCP      60 21 → 2616 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
> Frame 24: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Telemech_17:89:7f (00:80:f4:17:89:7f), Dst: Private_32:ee:84 (80:6d:97:32:ee:84)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.200
v Transmission Control Protocol, Src Port: 21, Dst Port: 2616, Seq: 1, Ack: 1, Len: 0
    Source Port: 21
    Destination Port: 2616
    [Stream index: 1]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 0
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 2667352936
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x014 (RST, ACK)
    Window: 0
    [Calculated window size: 0]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0xf104 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
```

```
0000  80 6d 97 32 ee 84 00 80  f4 17 89 7f 08 00 45 00   ·m·2···· ······E·
0010  00 28 35 7c 00 00 40 06  c3 3a c0 a8 00 01 c0 a8   ·(5|··@· ·:······
0020  00 c8 00 15 0a 38 00 00  00 00 9e fc 93 68 50 14   ·····8·· ·····hP·
0030  00 00 f1 04 00 00 00 00  00 00 00 00               ········ ····
```

It can be seen that the ePAC M580 systematically rejects the attempts made by the Workstation with a reset request

- Reactivate the FTP protocol service.



Services

FTP : Enabled

TFTP :

HTTP : Disabled

DHCP / BOOTP : Enabled

SNMP : Enabled

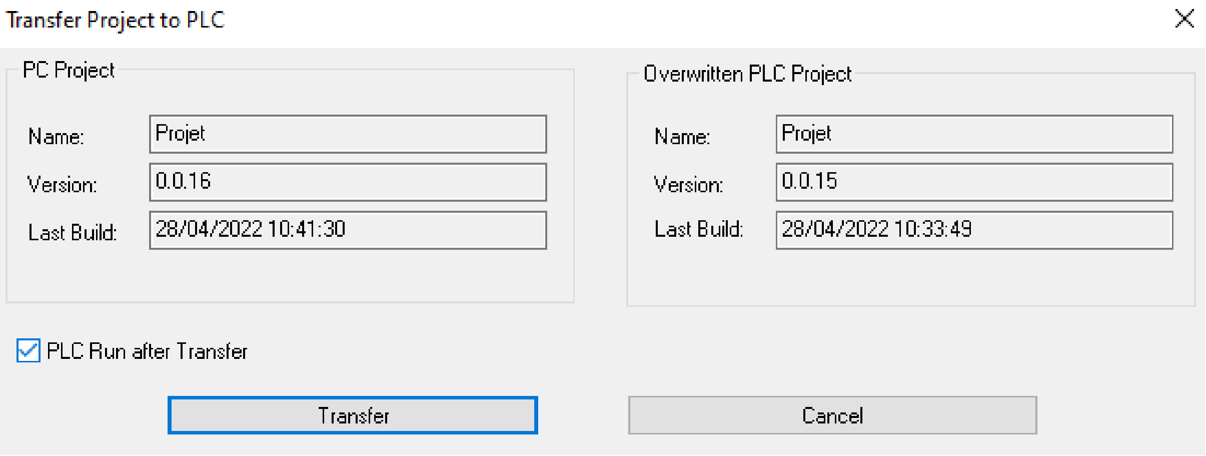
EIP : Enabled

Access Control

Disabled

Function: DIO

Validate this configuration modification (Ctrl-W), generate, load the PLC and put it in run.



Transfer Project to PLC

PC Project

Name: Projet
Version: 0.0.16
Last Build: 28/04/2022 10:41:30

Overwritten PLC Project

Name: Projet
Version: 0.0.15
Last Build: 28/04/2022 10:33:49

☑ PLC Run after Transfer

6. IP Address Filtering: M580 CPU Access Control

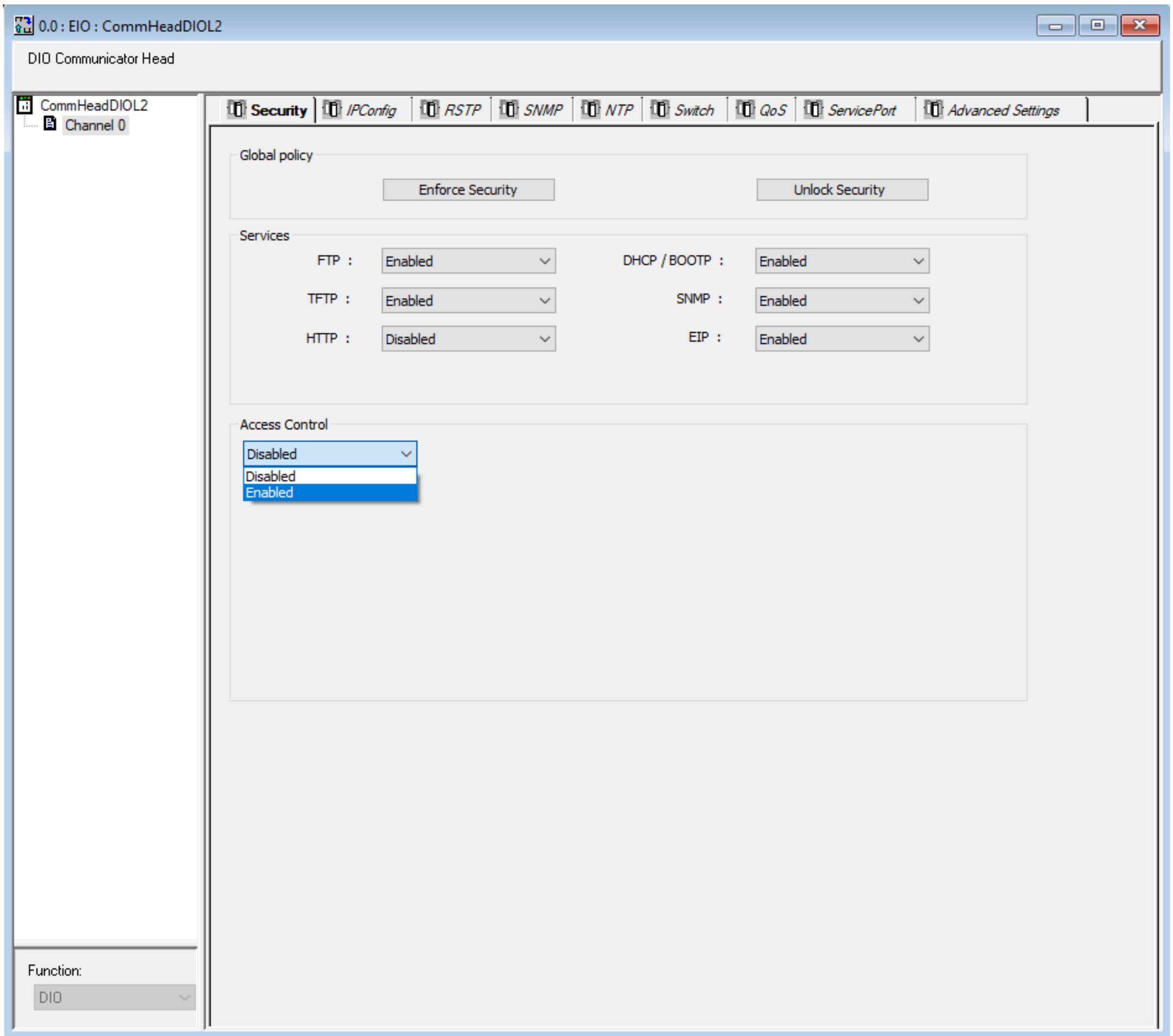
When this IP address filtering (Access Control) is disabled, no filtering is performed on the IP addresses of clients accessing the port in question (in this case the CPU Ethernet port).

On the other hand, when this filtering is activated, only those whose IP addresses have been logged will be recognised as legitimate clients. Thus, for a logged address, the admissibility of the protocols corresponding to the Modbus/TCP, HTTP, FTP, TFTP, SNMP and EIP services will be checked individually for each designated accessor.

6.1. IP address filtering in the Ethernet configuration on the CPU port

- With Unity, go (in off-line mode) to the M580 CPU configuration, and open the section presenting itself as the EIO Bus configuration section.

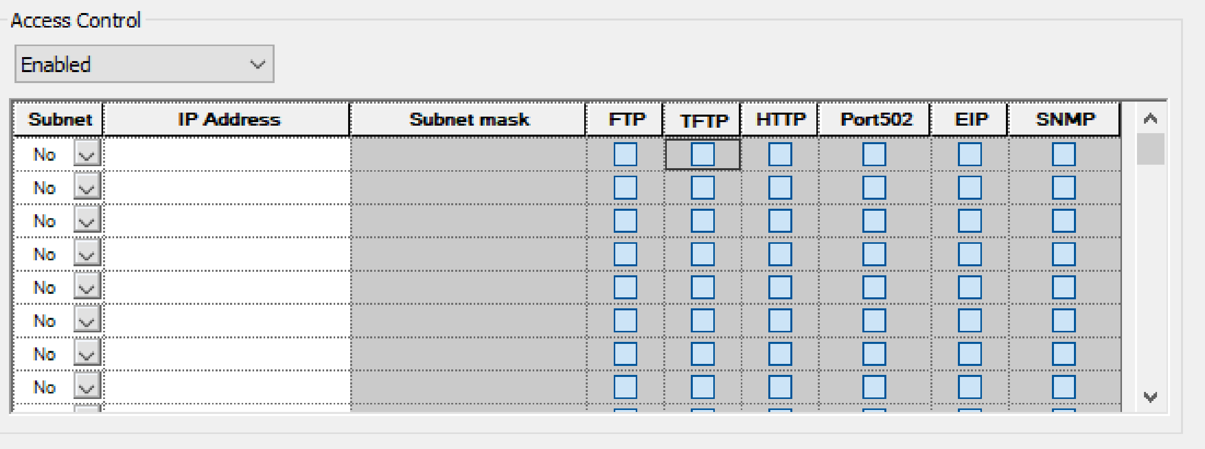
Enable Access Control i.e. filtering on the addresses of the accessors (clients) to the services managed by the CPU



FTP : Enabled
TFTP : Enabled
HTTP : Disabled
DHCP / BOOTP : Enabled
SNMP : Enabled
EIP : Enabled
Access Control: Disabled
Function: DIO

6.2. IP filtering enabled in the Ethernet configuration on the CPU port, without designated accessor

- Firstly, ensure that the filtering log table does not indicate any authorized accessors

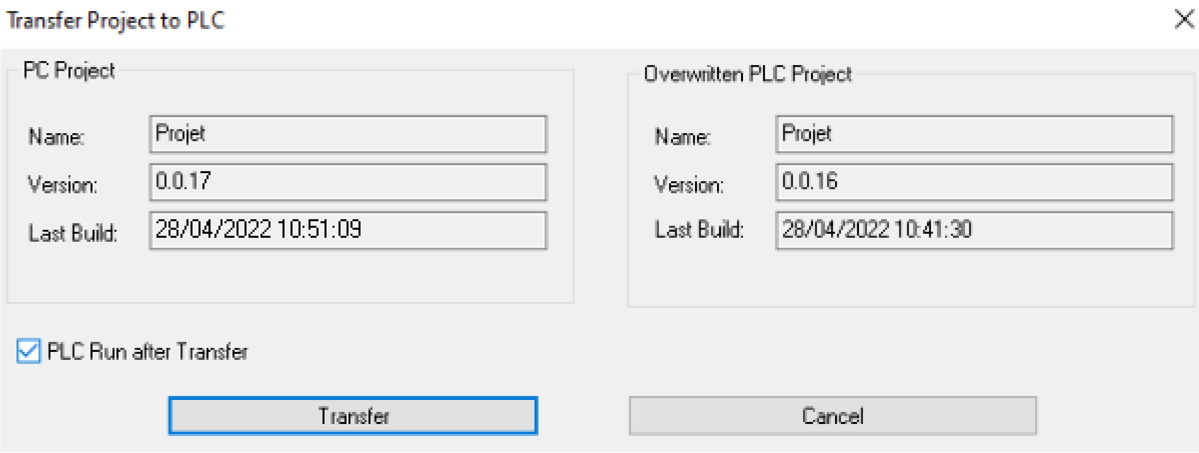


Access Control

Enabled

Subnet	IP Address	Subnet mask	FTP	TFTP	HTTP	Port502	EIP	SNMP
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□

If necessary, comply with this configuration, validate (Ctrl-W), generate, load the PLC and run.



Transfer Project to PLC

PC Project

Name: Projet

Version: 0.0.17

Last Build: 28/04/2022 10:51:09

Overwritten PLC Project

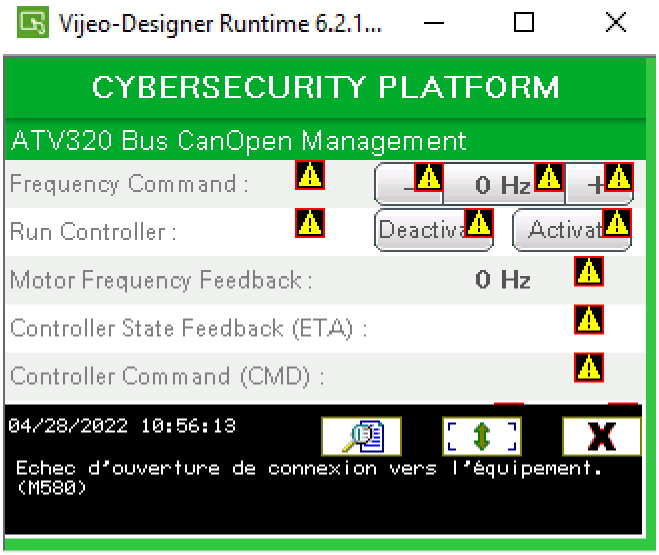
Name: Projet

Version: 0.0.16

Last Build: 28/04/2022 10:41:30

☑ PLC Run after Transfer

- Under these conditions, check that the workstation is no longer able to operate a Modbus access (via the Vijeo Designer simulation)



Vijeo-Designer Runtime 6.2.1...

CYBERSECURITY PLATFORM

ATV320 Bus CanOpen Management

Frequency Command : 0 Hz

Run Controller :

Motor Frequency Feedback : 0 Hz

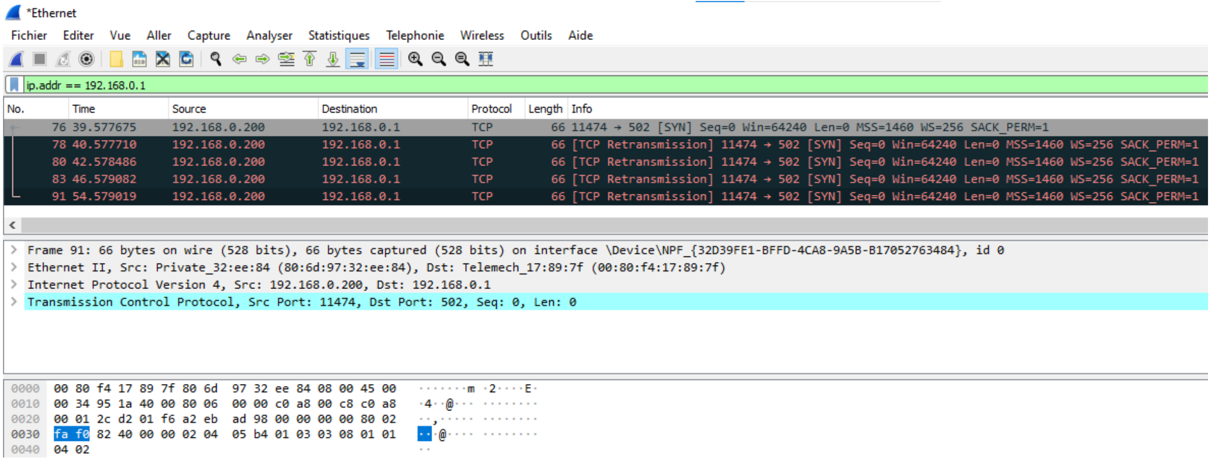
Controller State Feedback (ETA) :

Controller Command (CMD) :

04/28/2022 10:56:13

Echec d'ouverture de connexion vers l'équipement.
(M580)

Example of a Wireshark trace with cyclic readings and speed setpoint modification



*Ethernet

ip.addr == 192.168.0.1

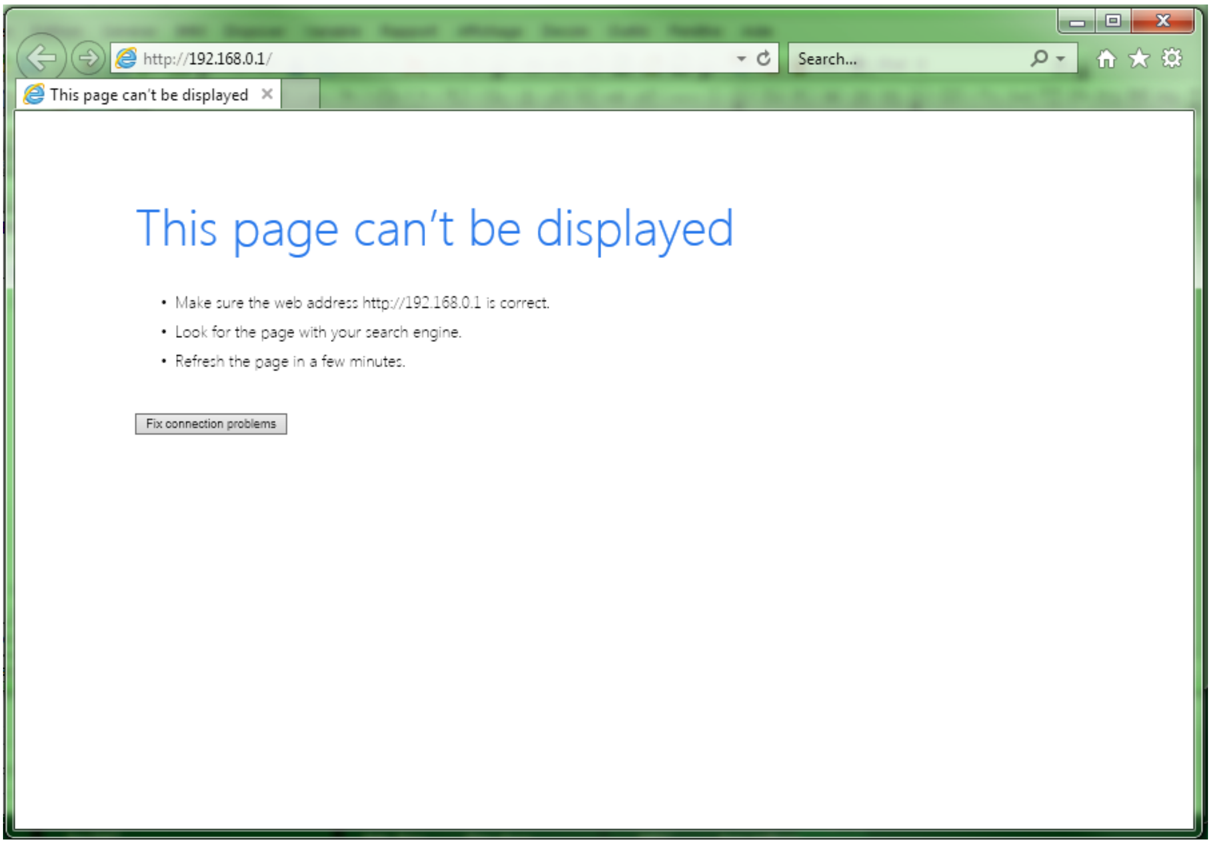
```
No.   Time        Source          Destination     Protocol  Length Info
   76 39.577675   192.168.0.200   192.168.0.1     TCP       66 11474 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   78 40.577710   192.168.0.200   192.168.0.1     TCP       66 [TCP Retransmission] 11474 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   80 42.578486   192.168.0.200   192.168.0.1     TCP       66 [TCP Retransmission] 11474 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   83 46.579082   192.168.0.200   192.168.0.1     TCP       66 [TCP Retransmission] 11474 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   91 54.579019   192.168.0.200   192.168.0.1     TCP       66 [TCP Retransmission] 11474 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

```
> Frame 91: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Private_32:ee:84 (80:6d:97:32:ee:84), Dst: Telemech_17:89:7f (00:80:f4:17:89:7f)
> Internet Protocol Version 4, Src: 192.168.0.200, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 11474, Dst Port: 502, Seq: 0, Len: 0
```

```
0000  00 80 f4 17 89 7f 80 6d  97 32 ee 84 08 00 45 00   ·······m ·2····E·
0010  00 34 95 1a 40 00 80 06  00 00 c0 a8 00 c8 c0 a8   ·4··@··· ········
0020  00 01 2c d2 01 f6 a2 eb  ad 98 00 00 00 00 80 02   ··,····· ········
0030  fa f0 82 40 00 00 02 04  05 b4 01 03 03 08 01 01   ···@···· ········
0040  04 02                                              ··
```

We check that we oscillate between requests for retransmission and synchronization issued by the Workstation; but that the automaton does not respond to these requests.

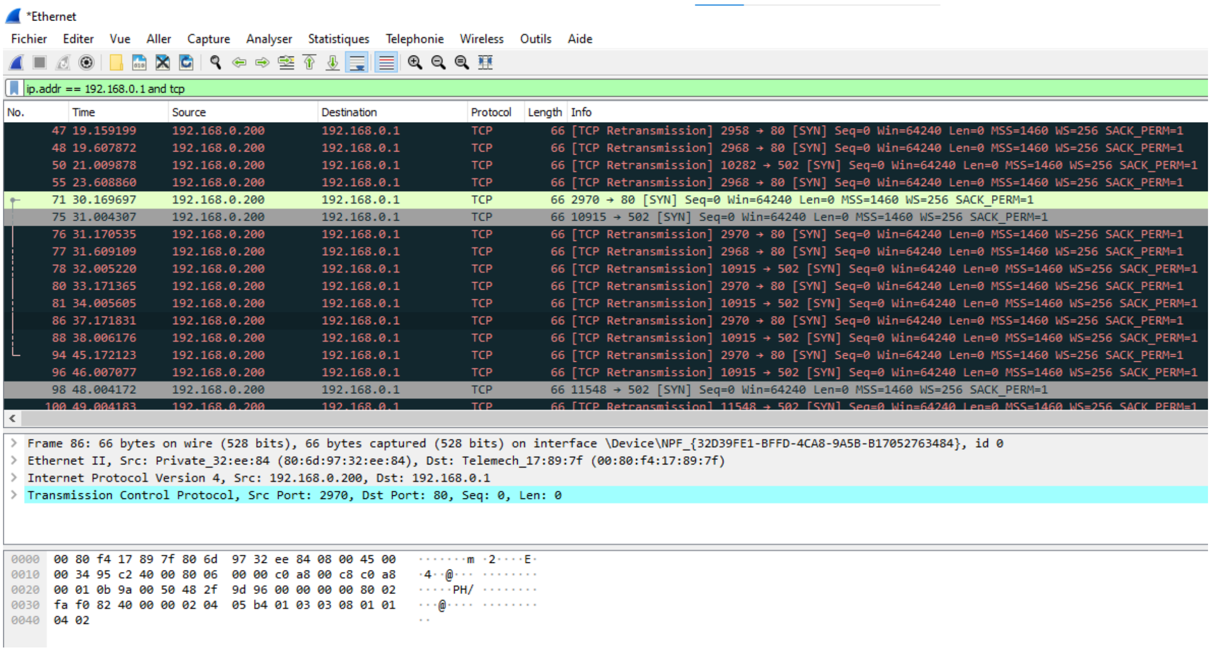
- Also check that, under these conditions, it is no longer possible to access the M580 CPU web pages from the Workstation.



This page can't be displayed

- Make sure the web address http://192.168.0.1 is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

Example of a Wireshark trace


*Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

ip.addr == 192.168.0.1 and tcp

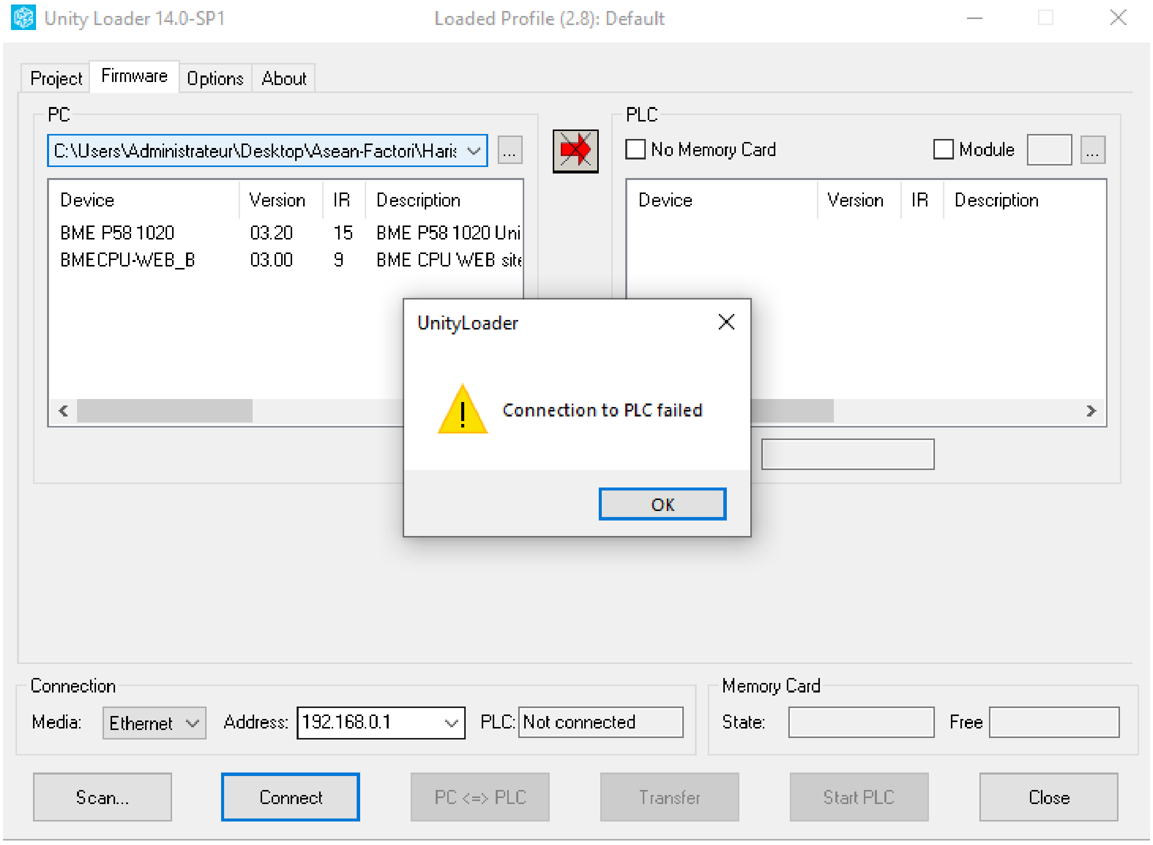
```
No.  Time       Source         Destination  Protocol Length Info
  47 19.159199  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 2958 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  48 19.607872  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 2968 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  50 21.009878  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 10282 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  55 23.608860  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 2968 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  71 30.169697  192.168.0.200  192.168.0.1  TCP      66 2970 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  75 31.004307  192.168.0.200  192.168.0.1  TCP      66 10915 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  76 31.170535  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 2970 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  77 31.609109  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 2968 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  78 32.005220  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 10915 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  80 33.171365  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 2970 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  81 34.005605  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 10915 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  86 37.171831  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 2970 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  88 38.006176  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 10915 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  94 45.172123  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 2970 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  96 46.007077  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 10915 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  98 48.004172  192.168.0.200  192.168.0.1  TCP      66 11548 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
 100 49.004183  192.168.0.200  192.168.0.1  TCP      66 [TCP Retransmission] 11548 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

```
> Frame 86: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Private_32:ee:84 (80:6d:97:32:ee:84), Dst: Telemech_17:89:7f (00:80:f4:17:89:7f)
> Internet Protocol Version 4, Src: 192.168.0.200, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 2970, Dst Port: 80, Seq: 0, Len: 0
```

```
0000  00 80 f4 17 89 7f 80 6d  97 32 ee 84 08 00 45 00   ·······m ·2····E·
0010  00 34 95 c2 40 00 80 06  00 00 c0 a8 00 c8 c0 a8   ·4··@··· ········
0020  00 01 0b 9a 00 50 48 2f  9d 96 00 00 00 00 80 02   ·····PH/ ········
0030  fa f0 82 40 00 00 02 04  05 b4 01 03 03 08 01 01   ···@···· ········
0040  04 02                                              ··
```

We check that we oscillate between requests for synchronization and retransmission before abandonment, by the Workstation; but that the automaton does not respond to these requests.

- Finally, check that, under these conditions, it is no longer possible to connect to the M580 CPU from the Workstation via Unity Loader.



PC: C:\Users\Administrateur\Desktop\Asean-Factori\Haris

Device	Version	IR	Description
BME P58 1020	03.20	15	BME P58 1020 Uni
BMECPU-WEB_B	03.00	9	BME CPU WEB site

PLC: ☐ No Memory Card ☐ Module

Device	Version	IR	Description

UnityLoader

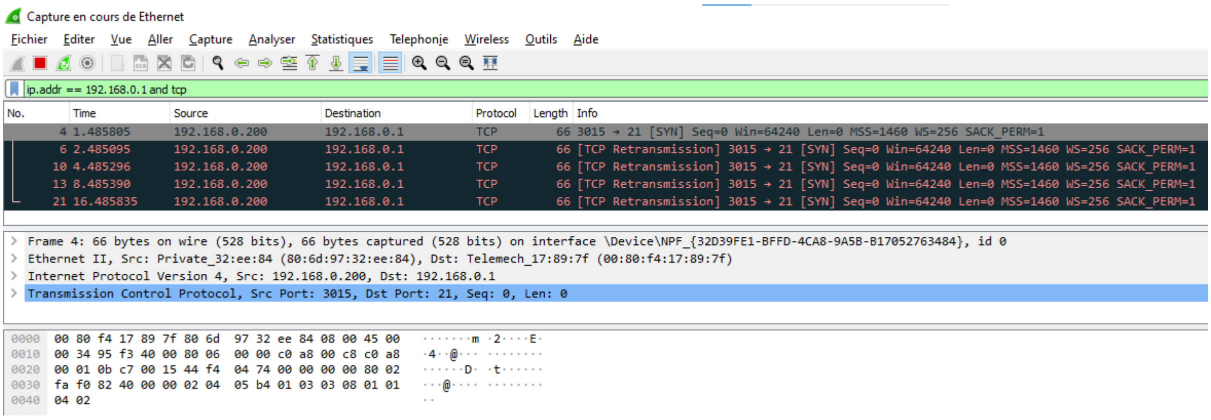
Connection to PLC failed

OK

Connection
Media: Ethernet Address: 192.168.0.1 PLC: Not connected

Memory Card
State: Free

Example of a Wireshark trace


Capture en cours de Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

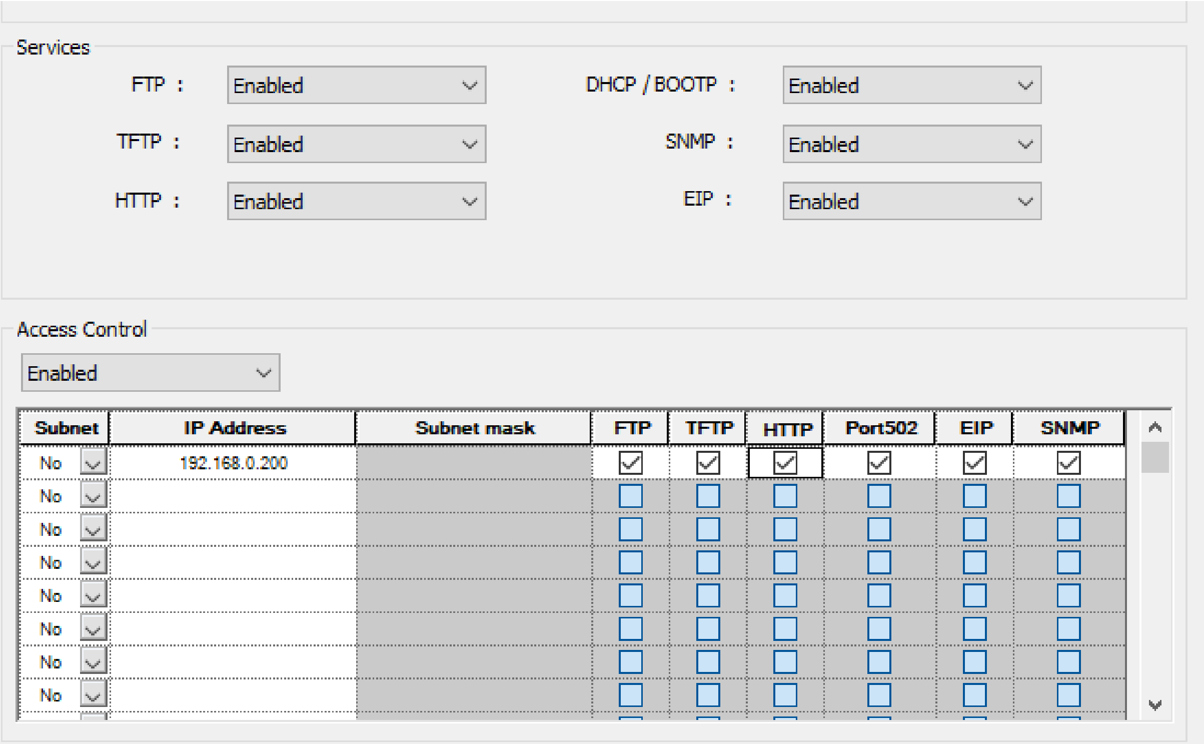
ip.addr == 192.168.0.1 and tcp

```
No.   Time         Source          Destination   Protocol  Length  Info
    4 1.485805     192.168.0.200   192.168.0.1   TCP       66 3015 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
    6 2.485095     192.168.0.200   192.168.0.1   TCP       66 [TCP Retransmission] 3015 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   10 4.485296     192.168.0.200   192.168.0.1   TCP       66 [TCP Retransmission] 3015 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   13 8.485390     192.168.0.200   192.168.0.1   TCP       66 [TCP Retransmission] 3015 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   21 16.485835    192.168.0.200   192.168.0.1   TCP       66 [TCP Retransmission] 3015 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Private_32:ee:84 (80:6d:97:32:ee:84), Dst: Telemech_17:89:7f (00:80:f4:17:89:7f)
> Internet Protocol Version 4, Src: 192.168.0.200, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 3015, Dst Port: 21, Seq: 0, Len: 0

0000  00 80 f4 17 89 7f 80 6d  97 32 ee 84 08 00 45 00   ·······m ·2····E·
0010  00 34 95 f3 40 00 80 06  00 00 c0 a8 00 c8 c0 a8   ·4··@··· ········
0020  00 01 0b c7 00 15 44 f4  04 74 00 00 00 00 80 02   ······D· ·t······
0030  fa f0 82 40 00 00 02 04  05 b4 01 03 03 08 01 01   ···@···· ········
0040  04 02                                              ··
```

We check that we oscillate between requests for synchronization and retransmission before abandonment, by the Workstation; but that the automaton does not respond to these requests.

6.3. Validated IP filtering in the Ethernet configuration on the CPU port, with designated accessor and all validated protocols

- Ensure that the filtering log table now designates the Workstation as an authorized user, by validating each of the FTP, TFTP, HTTP, Port502 (Modbus), EIP and SNMP protocols



Services

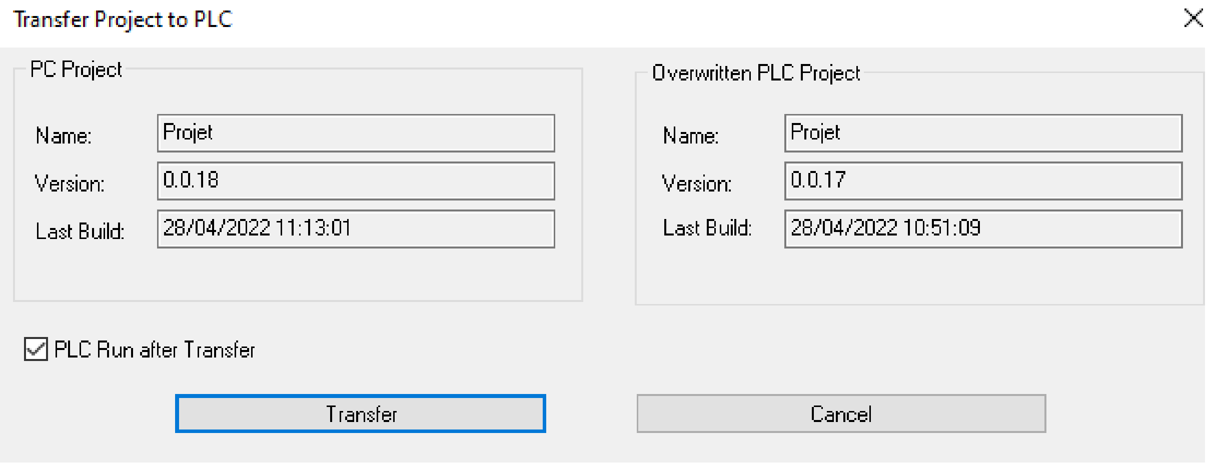
FTP :	Enabled	DHCP / BOOTP :	Enabled
TFTP :	Enabled	SNMP :	Enabled
HTTP :	Enabled	EIP :	Enabled

Access Control

Enabled

Subnet	IP Address	Subnet mask	FTP	TFTP	HTTP	Port502	EIP	SNMP
No	192.168.0.200		☑	☑	☑	☑	☑	☑
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐
No			☐	☐	☐	☐	☐	☐

If necessary, comply with this configuration, validate (Ctrl-W), generate, and load the PLC and run if necessary.



Transfer Project to PLC

PC Project

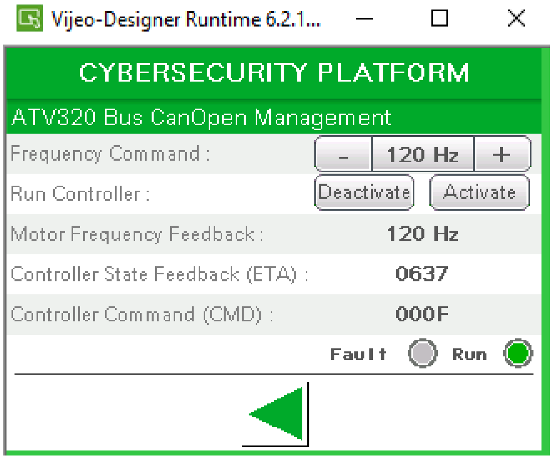
Name: Projet
Version: 0.0.18
Last Build: 28/04/2022 11:13:01

Overwritten PLC Project

Name: Projet
Version: 0.0.17
Last Build: 28/04/2022 10:51:09

☑ PLC Run after Transfer

- In these conditions, check that the workstation is able to operate a Modbus access (via the Vijeo Designer Simulation) (read or even write)

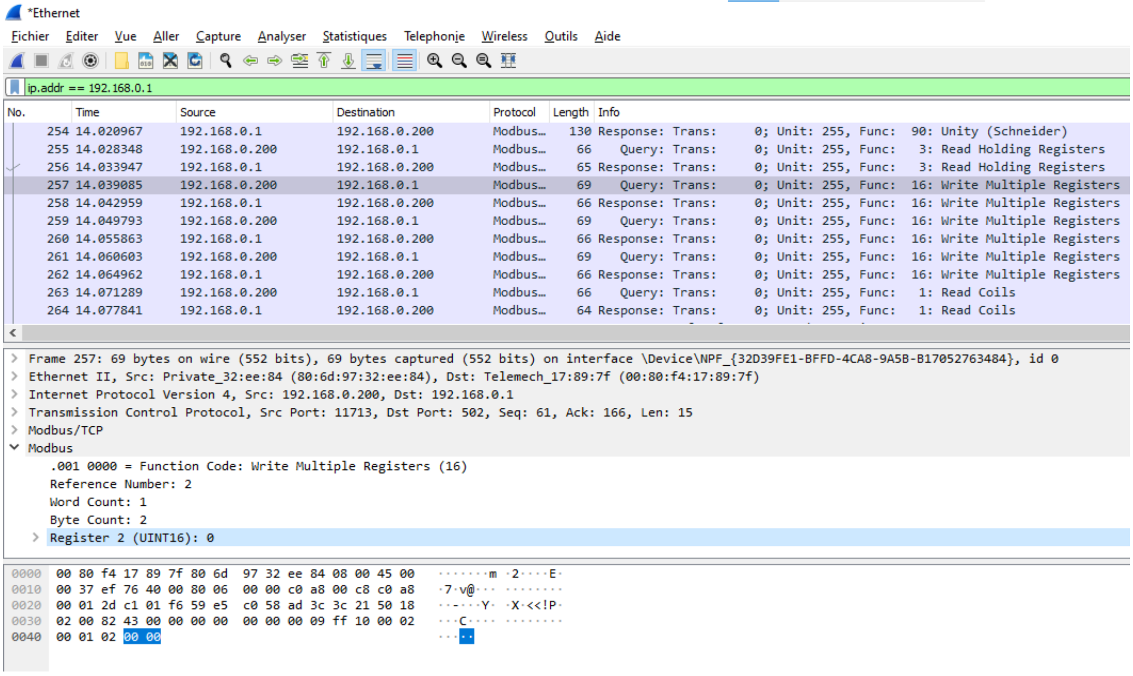


CYBERSECURITY PLATFORM

ATV320 Bus CanOpen Management

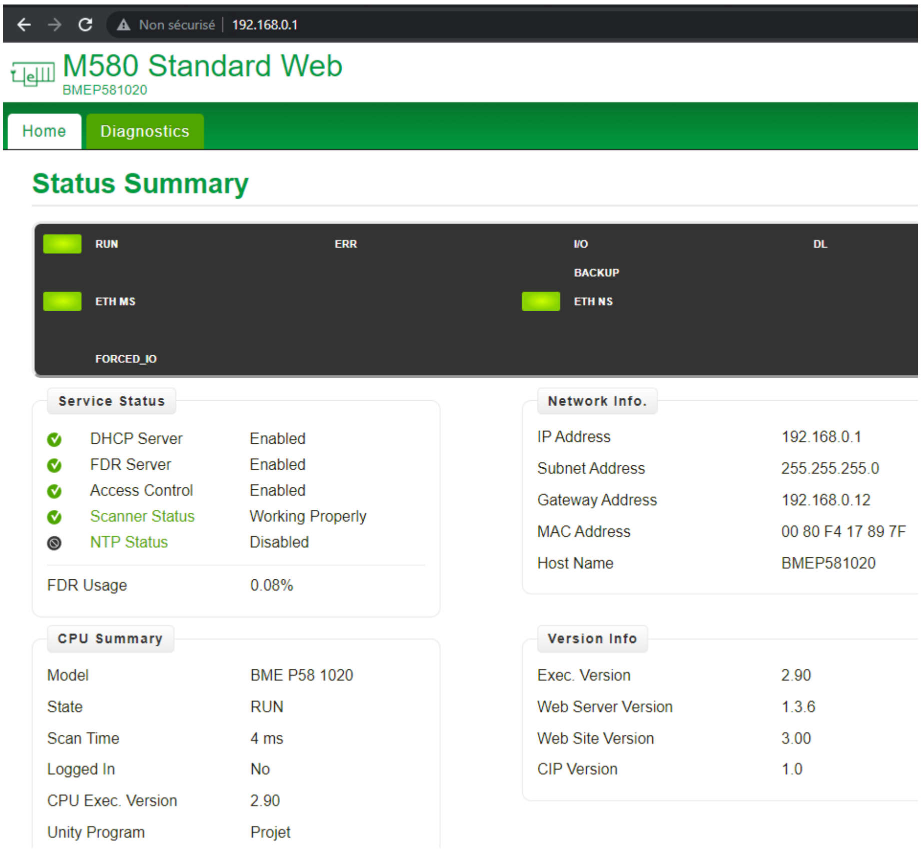
Frequency Command : - 120 Hz +
Run Controller : Deactivate Activate
Motor Frequency Feedback : 120 Hz
Controller State Feedback (ETA) : 0637
Controller Command (CMD) : 000F

Example of a Wireshark trace with cyclic readings and speed setpoint modification


*Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

```
ip.addr == 192.168.0.1

No.   Time        Source         Destination    Protocol  Length Info
  254 14.020967   192.168.0.1    192.168.0.200  Modbus…   130 Response: Trans:    0; Unit: 255, Func:  90: Unity (Schneider)
  255 14.028348   192.168.0.200  192.168.0.1    Modbus…   66     Query: Trans:    0; Unit: 255, Func:   3: Read Holding Registers
  256 14.033947   192.168.0.1    192.168.0.200  Modbus…   65 Response: Trans:    0; Unit: 255, Func:   3: Read Holding Registers
  257 14.039085   192.168.0.200  192.168.0.1    Modbus…   69     Query: Trans:    0; Unit: 255, Func:  16: Write Multiple Registers
  258 14.042959   192.168.0.1    192.168.0.200  Modbus…   66 Response: Trans:    0; Unit: 255, Func:  16: Write Multiple Registers
  259 14.049793   192.168.0.200  192.168.0.1    Modbus…   69     Query: Trans:    0; Unit: 255, Func:  16: Write Multiple Registers
  260 14.055863   192.168.0.1    192.168.0.200  Modbus…   66 Response: Trans:    0; Unit: 255, Func:  16: Write Multiple Registers
  261 14.060603   192.168.0.200  192.168.0.1    Modbus…   69     Query: Trans:    0; Unit: 255, Func:  16: Write Multiple Registers
  262 14.064962   192.168.0.1    192.168.0.200  Modbus…   66 Response: Trans:    0; Unit: 255, Func:  16: Write Multiple Registers
  263 14.071289   192.168.0.200  192.168.0.1    Modbus…   66     Query: Trans:    0; Unit: 255, Func:   1: Read Coils
  264 14.077841   192.168.0.1    192.168.0.200  Modbus…   64 Response: Trans:    0; Unit: 255, Func:   1: Read Coils

> Frame 257: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Private_32:ee:84 (80:6d:97:32:ee:84), Dst: Telemech_17:89:7f (00:80:f4:17:89:7f)
> Internet Protocol Version 4, Src: 192.168.0.200, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 11713, Dst Port: 502, Seq: 61, Ack: 166, Len: 15
> Modbus/TCP
v Modbus
    .001 0000 = Function Code: Write Multiple Registers (16)
    Reference Number: 2
    Word Count: 1
    Byte Count: 2
  > Register 2 (UINT16): 0

0000  00 80 f4 17 89 7f 80 6d  97 32 ee 84 08 00 45 00   ·······m ·2····E·
0010  00 37 ef 76 40 00 80 06  00 00 c0 a8 00 c8 c0 a8   ·7·v@··· ········
0020  00 01 2d c1 01 f6 59 e5  c0 58 ad 3c 3c 21 50 18   ··-···Y· ·X·<<!P·
0030  02 00 82 43 00 00 00 00  00 00 00 09 ff 10 00 02   ···C···· ········
0040  00 01 02 00 00                                     ···..
```

- Also check that the M580 CPU web pages can still be accessed from the Workstation



Status Summary

Service Status

✓	DHCP Server	Enabled
✓	FDR Server	Enabled
✓	Access Control	Enabled
✓	Scanner Status	Working Properly
⊘	NTP Status	Disabled
	FDR Usage	0.08%

Network Info.

IP Address	192.168.0.1
Subnet Address	255.255.255.0
Gateway Address	192.168.0.12
MAC Address	00 80 F4 17 89 7F
Host Name	BMEP581020

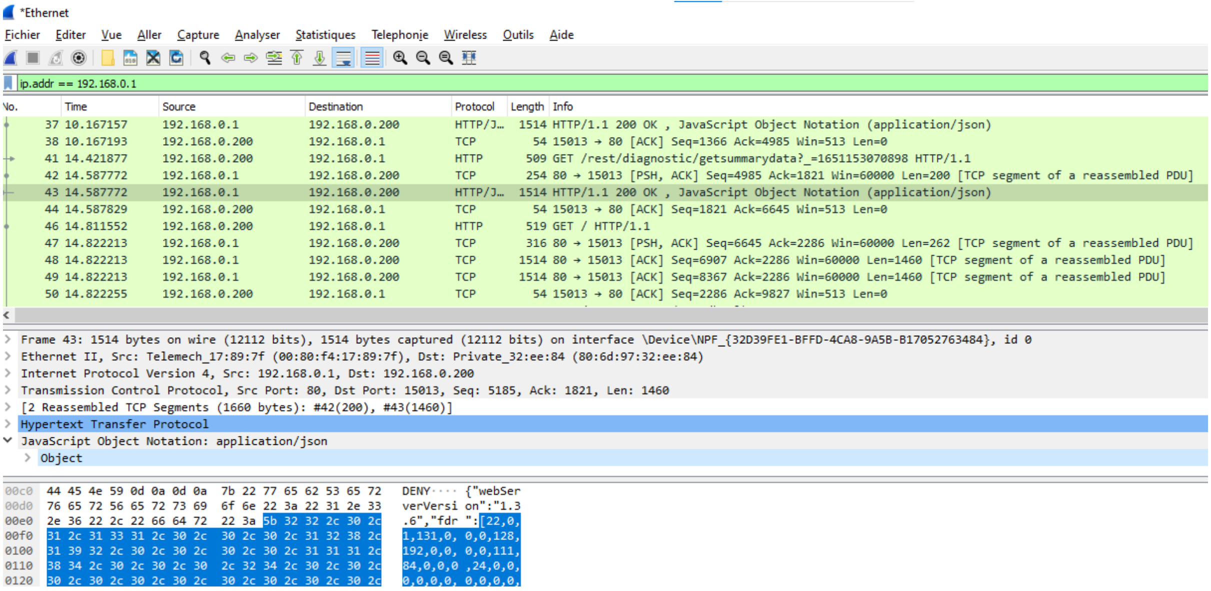
CPU Summary

Model	BME P58 1020
State	RUN
Scan Time	4 ms
Logged In	No
CPU Exec. Version	2.90
Unity Program	Projet

Version Info

Exec. Version	2.90
Web Server Version	1.3.6
Web Site Version	3.00
CIP Version	1.0

Example of a Wireshark trace


*Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

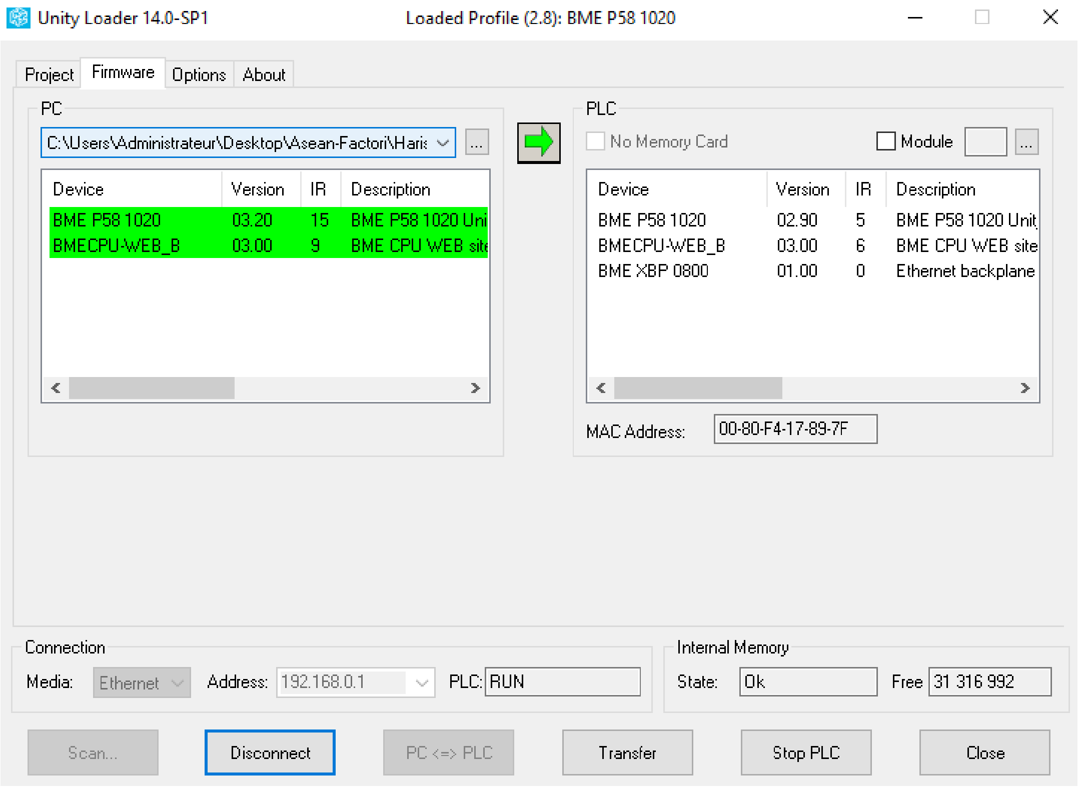
```
ip.addr == 192.168.0.1
```

```
No.  Time       Source         Destination    Protocol Length Info
  37 10.167157  192.168.0.1    192.168.0.200  HTTP/J…   1514 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
  38 10.167193  192.168.0.200  192.168.0.1    TCP         54 15013 → 80 [ACK] Seq=1366 Ack=4985 Win=513 Len=0
  41 14.421877  192.168.0.200  192.168.0.1    HTTP       509 GET /rest/diagnostic/getsummarydata?_=1651153070898 HTTP/1.1
  42 14.587772  192.168.0.1    192.168.0.200  TCP        254 80 → 15013 [PSH, ACK] Seq=4985 Ack=1821 Win=60000 Len=200 [TCP segment of a reassembled PDU]
  43 14.587772  192.168.0.1    192.168.0.200  HTTP/J…   1514 HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
  44 14.587829  192.168.0.200  192.168.0.1    TCP         54 15013 → 80 [ACK] Seq=1821 Ack=6645 Win=513 Len=0
  46 14.811552  192.168.0.200  192.168.0.1    HTTP       519 GET / HTTP/1.1
  47 14.822213  192.168.0.1    192.168.0.200  TCP        316 80 → 15013 [PSH, ACK] Seq=6645 Ack=2286 Win=60000 Len=262 [TCP segment of a reassembled PDU]
  48 14.822213  192.168.0.1    192.168.0.200  TCP       1514 80 → 15013 [ACK] Seq=6907 Ack=2286 Win=60000 Len=1460 [TCP segment of a reassembled PDU]
  49 14.822213  192.168.0.1    192.168.0.200  TCP       1514 80 → 15013 [ACK] Seq=8367 Ack=2286 Win=60000 Len=1460 [TCP segment of a reassembled PDU]
  50 14.822255  192.168.0.200  192.168.0.1    TCP         54 15013 → 80 [ACK] Seq=2286 Ack=9827 Win=513 Len=0
```

```
> Frame 43: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Telemech_17:89:7f (00:80:f4:17:89:7f), Dst: Private_32:ee:84 (80:6d:97:32:ee:84)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.200
> Transmission Control Protocol, Src Port: 80, Dst Port: 15013, Seq: 5185, Ack: 1821, Len: 1460
> [2 Reassembled TCP Segments (1660 bytes): #42(200), #43(1460)]
> Hypertext Transfer Protocol
v JavaScript Object Notation: application/json
  > Object
```

```
00c0  44 45 4e 59 0d 0a 0d 0a  7b 22 77 65 62 53 65 72   DENY···· {"webSer
00d0  76 65 72 56 65 72 73 69  6f 6e 22 3a 22 31 2e 33   verVersi on":"1.3
00e0  2e 36 22 2c 22 66 64 72  22 3a 5b 32 32 2c 30 2c   .6","fdr ":[22,0,
00f0  31 2c 31 33 31 2c 30 2c  30 2c 30 2c 31 32 38 2c   1,131,0, 0,0,128,
0100  31 39 32 2c 30 2c 30 2c  30 2c 30 2c 31 31 31 2c   192,0,0, 0,0,111,
0110  38 34 2c 30 2c 30 2c 30  2c 32 34 2c 30 2c 30 2c   84,0,0,0 ,24,0,0,
0120  30 2c 30 2c 30 2c 30 2c  30 2c 30 2c 30 2c 30 2c   0,0,0,0, 0,0,0,0,
```

- Finally, check that you can still connect to the M580 CPU from the Workstation via Unity Loader.



PC: C:\Users\Administrateur\Desktop\Asean-Factori\Haris

Device	Version	IR	Description
BME P58 1020	03.20	15	BME P58 1020 Uni
BMECPU-WEB_B	03.00	9	BME CPU WEB site

PLC: □ No Memory Card □ Module

Device	Version	IR	Description
BME P58 1020	02.90	5	BME P58 1020 Unit
BMECPU-WEB_B	03.00	6	BME CPU WEB site
BME XBP 0800	01.00	0	Ethernet backplane

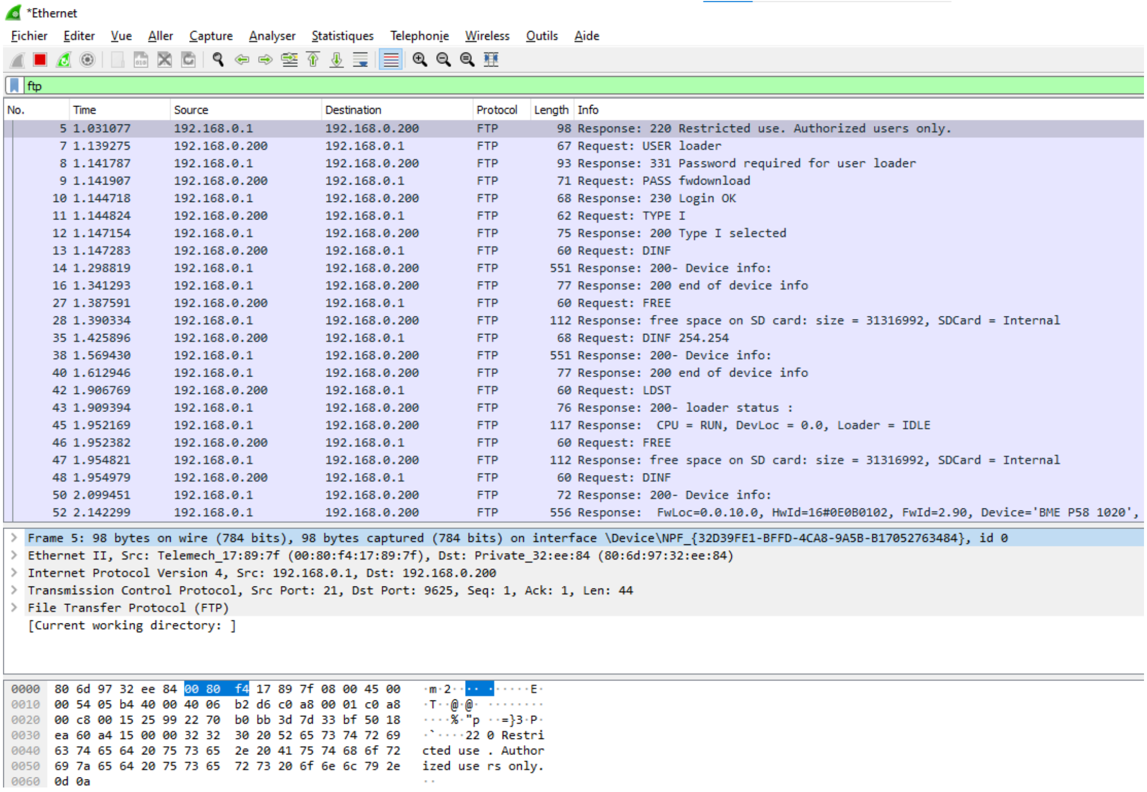
MAC Address: 00-80-F4-17-89-7F

Connection
Media: Ethernet Address: 192.168.0.1 PLC: RUN

Internal Memory
State: Ok Free 31 316 992

Example of a Wireshark trace

filter by: ftp


*Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
ftp

```
No.  Time        Source         Destination    Protocol Length Info
   5 1.031077    192.168.0.1    192.168.0.200  FTP       98 Response: 220 Restricted use. Authorized users only.
   7 1.139275    192.168.0.200  192.168.0.1    FTP       67 Request: USER loader
   8 1.141787    192.168.0.1    192.168.0.200  FTP       93 Response: 331 Password required for user loader
   9 1.141907    192.168.0.200  192.168.0.1    FTP       71 Request: PASS fwdownload
  10 1.144718    192.168.0.1    192.168.0.200  FTP       68 Response: 230 Login OK
  11 1.144824    192.168.0.200  192.168.0.1    FTP       62 Request: TYPE I
  12 1.147154    192.168.0.1    192.168.0.200  FTP       75 Response: 200 Type I selected
  13 1.147283    192.168.0.200  192.168.0.1    FTP       60 Request: DINF
  14 1.298819    192.168.0.1    192.168.0.200  FTP      551 Response: 200- Device info:
  16 1.341293    192.168.0.1    192.168.0.200  FTP       77 Response: 200 end of device info
  27 1.387591    192.168.0.200  192.168.0.1    FTP       60 Request: FREE
  28 1.390334    192.168.0.1    192.168.0.200  FTP      112 Response: free space on SD card: size = 31316992, SDCard = Internal
  35 1.425896    192.168.0.200  192.168.0.1    FTP       68 Request: DINF 254.254
  38 1.569430    192.168.0.1    192.168.0.200  FTP      551 Response: 200- Device info:
  40 1.612946    192.168.0.1    192.168.0.200  FTP       77 Response: 200 end of device info
  42 1.906769    192.168.0.200  192.168.0.1    FTP       60 Request: LDST
  43 1.909394    192.168.0.1    192.168.0.200  FTP       76 Response: 200- loader status :
  45 1.952169    192.168.0.1    192.168.0.200  FTP      117 Response:  CPU = RUN, DevLoc = 0.0, Loader = IDLE
  46 1.952382    192.168.0.200  192.168.0.1    FTP       60 Request: FREE
  47 1.954821    192.168.0.1    192.168.0.200  FTP      112 Response: free space on SD card: size = 31316992, SDCard = Internal
  48 1.954979    192.168.0.200  192.168.0.1    FTP       60 Request: DINF
  50 2.099451    192.168.0.1    192.168.0.200  FTP       72 Response: 200- Device info:
  52 2.142299    192.168.0.1    192.168.0.200  FTP      556 Response:  FwLoc=0.0.10.0, HwId=16#0E0B0102, FwId=2.90, Device='BME P58 1020',

> Frame 5: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Telemech_17:89:7f (00:80:f4:17:89:7f), Dst: Private_32:ee:84 (80:6d:97:32:ee:84)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.200
> Transmission Control Protocol, Src Port: 21, Dst Port: 9625, Seq: 1, Ack: 1, Len: 44
> File Transfer Protocol (FTP)
  [Current working directory: ]

0000  80 6d 97 32 ee 84 00 80  f4 17 89 7f 08 00 45 00   ·m·2·········E·
0010  00 54 05 b4 40 00 40 06  b2 d6 c0 a8 00 01 c0 a8   ·T··@·@· ········
0020  00 c8 00 15 25 99 22 70  b0 bb 3d 7d 33 bf 50 18   ····%·"p ··=}3·P·
0030  ea 60 a4 15 00 00 32 32  30 20 52 65 73 74 72 69   ·`····22 0 Restri
0040  63 74 65 64 20 75 73 65  2e 20 41 75 74 68 6f 72   cted use . Author
0050  69 7a 65 64 20 75 73 65  72 73 20 6f 6e 6c 79 2e   ized use rs only.
0060  0d 0a                                              ··
```

6.4. IP filtering enabled in the Ethernet configuration on the CPU port, with designated accessor with selective protocol disabling.

Now ensure that the filtering log table designates the Workstation as an authorized user, but by successively and alternately disabling the Port502 (Modbus) protocol, then HTTP, and finally FTP.

6.4.1. Modbus protocol disabling

As we are enabling the access control for the PLC, we need to mention all the host addresses and protocols they will be allowed to use, so the platform could work properly.

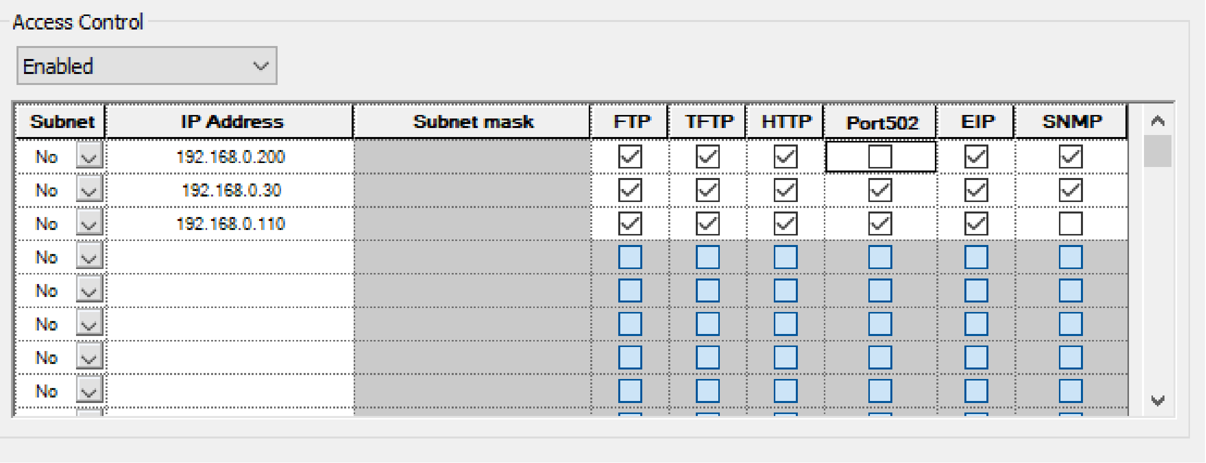
We have added in this order the following addresses:

PC address: 192.168.0.200

HMI address: 192.168.0.30

CAN address: 192.168.0.110

- Disable Modbus protocol (Port502) against IP address 192.168.0.200

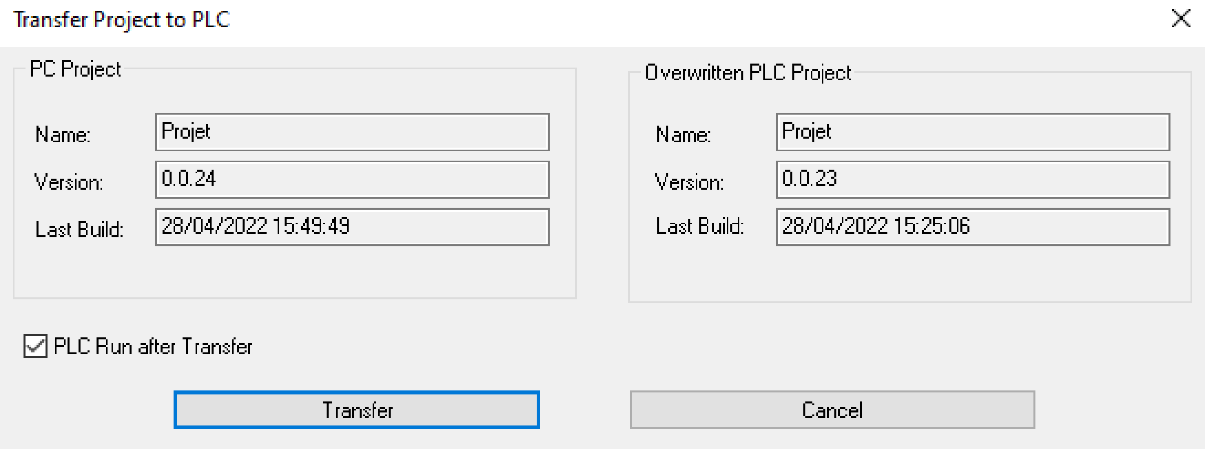


Access Control

Enabled

Subnet	IP Address	Subnet mask	FTP	TFTP	HTTP	Port502	EIP	SNMP
No	192.168.0.200		☑	☑	☑	□	☑	☑
No	192.168.0.30		☑	☑	☑	☑	☑	☑
No	192.168.0.110		☑	☑	☑	☑	☑	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□

If necessary, comply with this configuration, validate (Ctrl-W), generate, and load the PLC and run if necessary.



Transfer Project to PLC

PC Project

Name: Projet

Version: 0.0.24

Last Build: 28/04/2022 15:49:49

Overwritten PLC Project

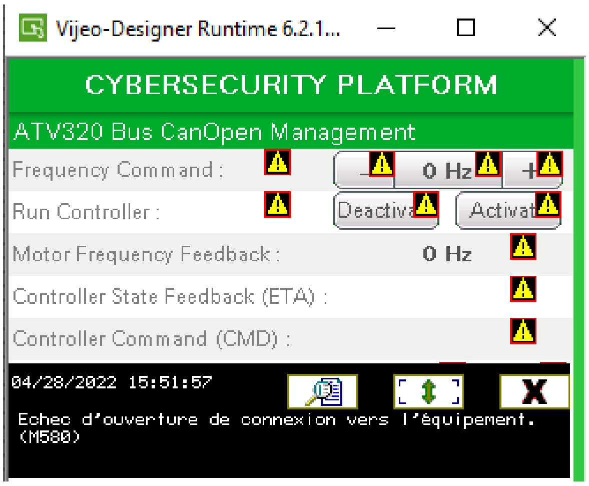
Name: Projet

Version: 0.0.23

Last Build: 28/04/2022 15:25:06

☑ PLC Run after Transfer

- If this is the case, check that the workstation is no longer able to access Modbus (via the Vijeo Designer simulation) (reading or even writing)



CYBERSECURITY PLATFORM

ATV320 Bus CanOpen Management

Frequency Command : 0 Hz

Run Controller :

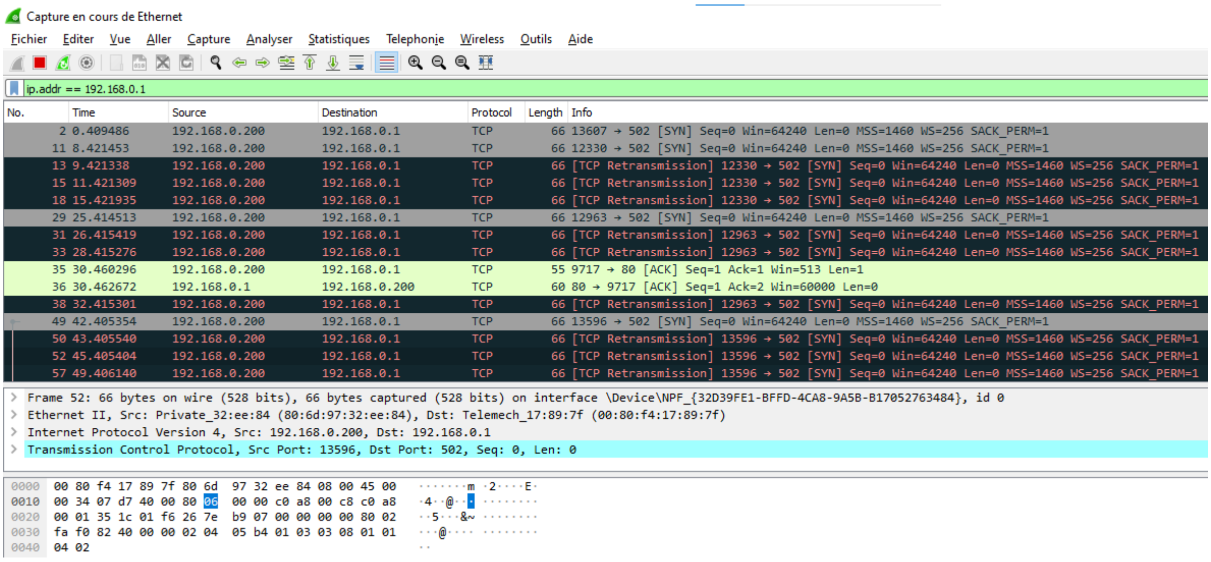
Motor Frequency Feedback : 0 Hz

Controller State Feedback (ETA) :

Controller Command (CMD) :

```
04/28/2022 15:51:57
Echec d'ouverture de connexion vers l'équipement.
(M580)
```

- Example of a Wireshark trace


Capture en cours de Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

```
ip.addr == 192.168.0.1
```

```
No.  Time       Source          Destination     Protocol Length Info
   2 0.409486   192.168.0.200   192.168.0.1     TCP      66 13607 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  11 8.421453   192.168.0.200   192.168.0.1     TCP      66 12330 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  13 9.421338   192.168.0.200   192.168.0.1     TCP      66 [TCP Retransmission] 12330 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  15 11.421309  192.168.0.200   192.168.0.1     TCP      66 [TCP Retransmission] 12330 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  18 15.421935  192.168.0.200   192.168.0.1     TCP      66 [TCP Retransmission] 12330 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  29 25.414513  192.168.0.200   192.168.0.1     TCP      66 12963 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  31 26.415419  192.168.0.200   192.168.0.1     TCP      66 [TCP Retransmission] 12963 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  33 28.415276  192.168.0.200   192.168.0.1     TCP      66 [TCP Retransmission] 12963 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  35 30.460296  192.168.0.200   192.168.0.1     TCP      55 9717 → 80 [ACK] Seq=1 Ack=1 Win=513 Len=1
  36 30.462672  192.168.0.1     192.168.0.200   TCP      60 80 → 9717 [ACK] Seq=1 Ack=2 Win=60000 Len=0
  38 32.415301  192.168.0.200   192.168.0.1     TCP      66 [TCP Retransmission] 12963 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  49 42.405354  192.168.0.200   192.168.0.1     TCP      66 13596 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  50 43.405540  192.168.0.200   192.168.0.1     TCP      66 [TCP Retransmission] 13596 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  52 45.405404  192.168.0.200   192.168.0.1     TCP      66 [TCP Retransmission] 13596 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  57 49.406140  192.168.0.200   192.168.0.1     TCP      66 [TCP Retransmission] 13596 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
```

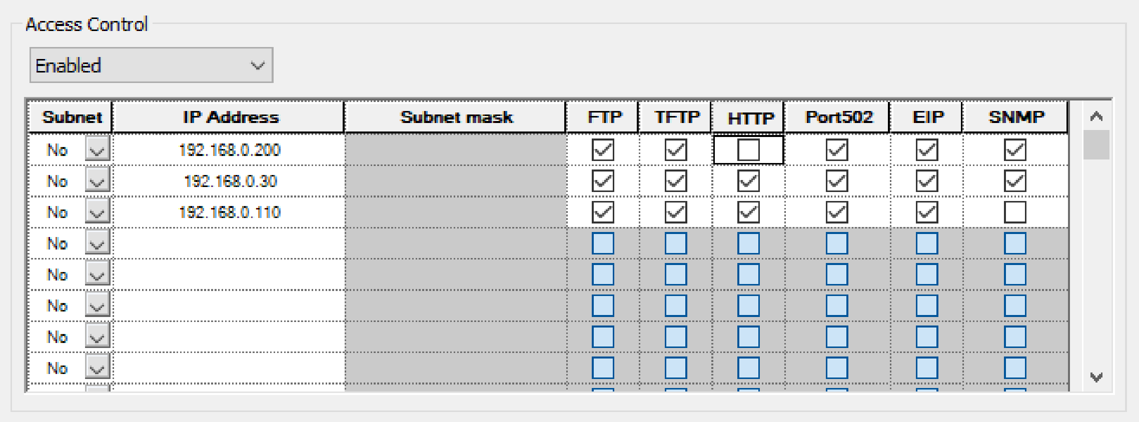
```
> Frame 52: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Private_32:ee:84 (80:6d:97:32:ee:84), Dst: Telemech_17:89:7f (00:80:f4:17:89:7f)
> Internet Protocol Version 4, Src: 192.168.0.200, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 13596, Dst Port: 502, Seq: 0, Len: 0
```

```
0000  00 80 f4 17 89 7f 80 6d  97 32 ee 84 08 00 45 00   ·······m ·2····E·
0010  00 34 07 d7 40 00 80 06  00 00 c0 a8 00 c8 c0 a8   ·4··@··· ········
0020  00 01 35 1c 01 f6 26 7e  b9 07 00 00 00 00 80 02   ··5···&~ ········
0030  fa f0 82 40 00 00 02 04  05 b4 01 03 03 08 01 01   ···@···· ········
0040  04 02                                              ··
```

We check that we oscillate between requests for synchronization and retransmission issued by the Workstation; but that the automaton does not respond to these requests.

6.4.2. Disabling the HTTP protocol

- **Disable the HTTP protocol against the IP address 192.168.0.200**



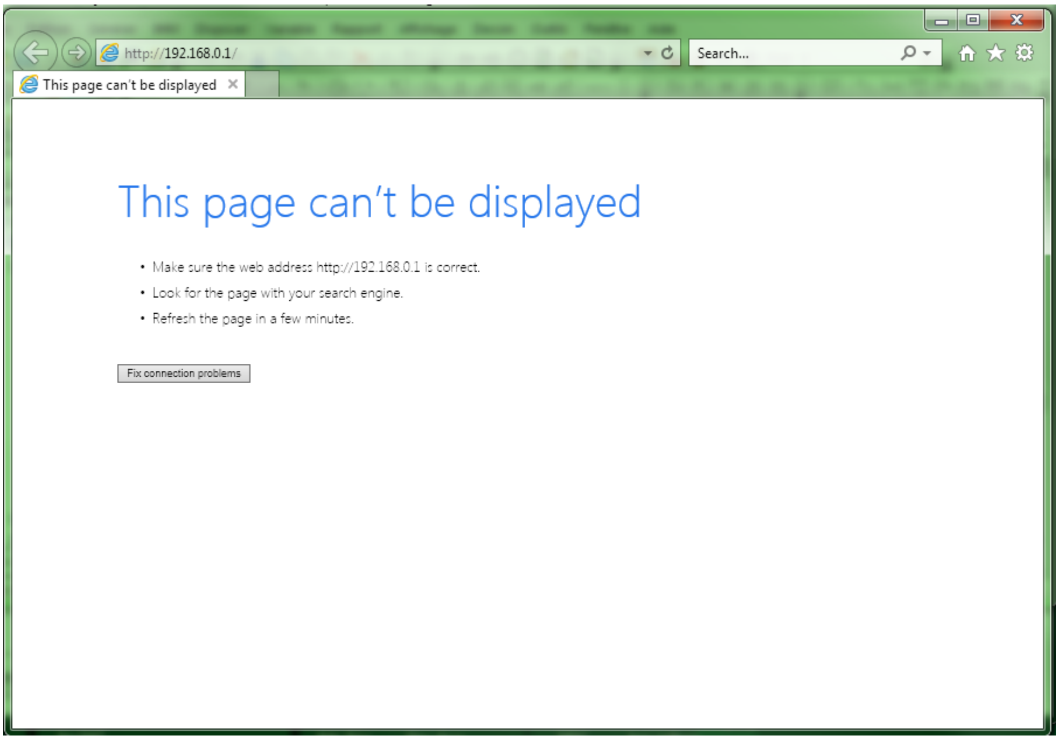
Access Control

Enabled

Subnet	IP Address	Subnet mask	FTP	TFTP	HTTP	Port502	EIP	SNMP
No	192.168.0.200		☑	☑	□	☑	☑	☑
No	192.168.0.30		☑	☑	☑	☑	☑	☑
No	192.168.0.110		☑	☑	☑	☑	☑	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□

If necessary, comply with this configuration, validate (Ctrl-W), generate, and load the PLC and run if necessary.

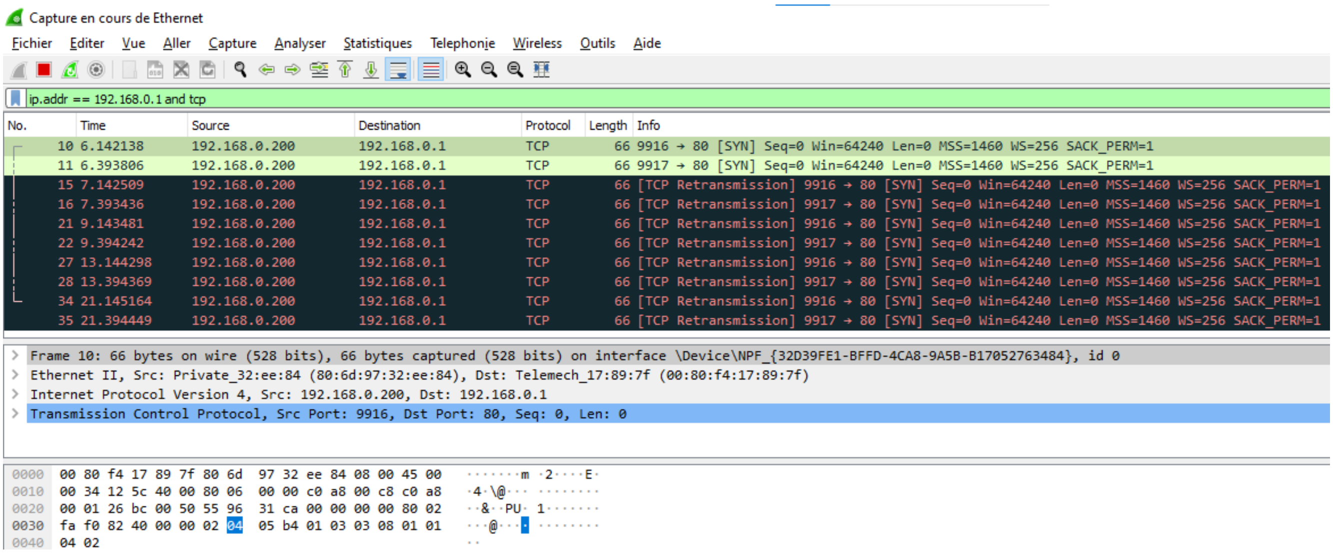
- Under these conditions, check that the workstation is no longer able to access the web pages of the M580 CPU



This page can't be displayed

- Make sure the web address http://192.168.0.1 is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

Example of a Wireshark trace



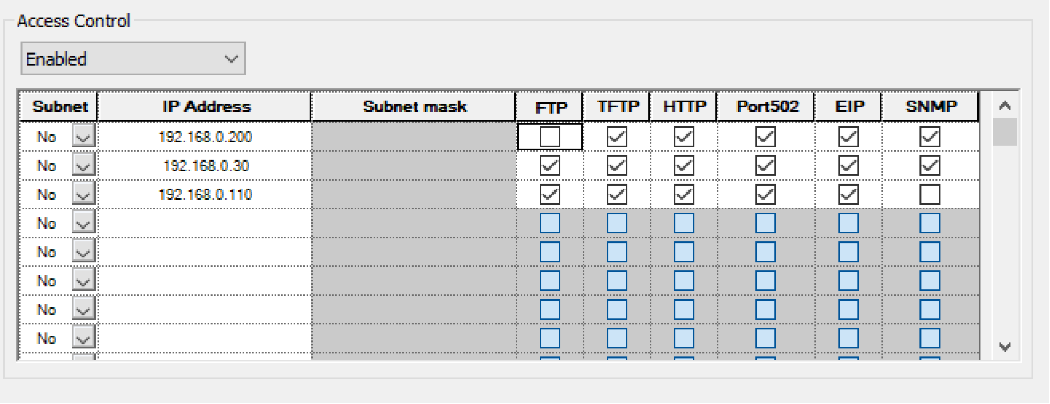
Capture en cours de Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

```
ip.addr == 192.168.0.1 and tcp

No.   Time       Source         Destination   Protocol Length Info
   10 6.142138   192.168.0.200  192.168.0.1   TCP      66 9916 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   11 6.393806   192.168.0.200  192.168.0.1   TCP      66 9917 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   15 7.142509   192.168.0.200  192.168.0.1   TCP      66 [TCP Retransmission] 9916 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   16 7.393436   192.168.0.200  192.168.0.1   TCP      66 [TCP Retransmission] 9917 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   21 9.143481   192.168.0.200  192.168.0.1   TCP      66 [TCP Retransmission] 9916 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   22 9.394242   192.168.0.200  192.168.0.1   TCP      66 [TCP Retransmission] 9917 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   27 13.144298  192.168.0.200  192.168.0.1   TCP      66 [TCP Retransmission] 9916 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   28 13.394369  192.168.0.200  192.168.0.1   TCP      66 [TCP Retransmission] 9917 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   34 21.145164  192.168.0.200  192.168.0.1   TCP      66 [TCP Retransmission] 9916 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   35 21.394449  192.168.0.200  192.168.0.1   TCP      66 [TCP Retransmission] 9917 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 10: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Private_32:ee:84 (80:6d:97:32:ee:84), Dst: Telemech_17:89:7f (00:80:f4:17:89:7f)
> Internet Protocol Version 4, Src: 192.168.0.200, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 9916, Dst Port: 80, Seq: 0, Len: 0

0000  00 80 f4 17 89 7f 80 6d  97 32 ee 84 08 00 45 00   ·······m ·2····E·
0010  00 34 12 5c 40 00 80 06  00 00 c0 a8 00 c8 c0 a8   ·4·\@··· ········
0020  00 01 26 bc 00 50 55 96  31 ca 00 00 00 00 80 02   ··&··PU· 1·······
0030  fa f0 82 40 00 00 02 04  05 b4 01 03 03 08 01 01   ···@···· ········
0040  04 02                                              ··
```

We check that we oscillate between requests for synchronization and retransmission issued by the Workstation; but that the automaton does not respond to these requests.

6.4.3. Disabling the FTP protocol

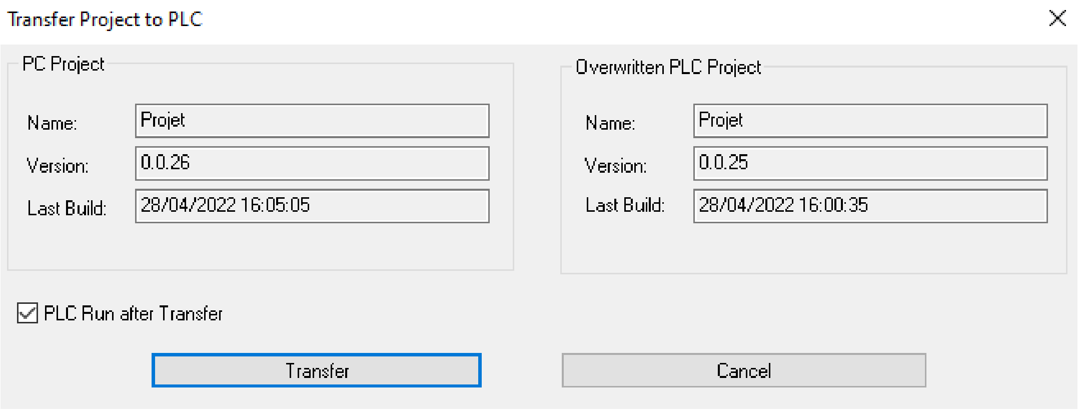
- Disable the FTP protocol for the IP address 192.168.0.200



Access Control

Enabled

Subnet	IP Address	Subnet mask	FTP	TFTP	HTTP	Port502	EIP	SNMP
No	192.168.0.200		□	☑	☑	☑	☑	☑
No	192.168.0.30		☑	☑	☑	☑	☑	☑
No	192.168.0.110		☑	☑	☑	☑	☑	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□
No			□	□	□	□	□	□


Transfer Project to PLC

PC Project

Name: Projet

Version: 0.0.26

Last Build: 28/04/2022 16:05:05

Overwritten PLC Project

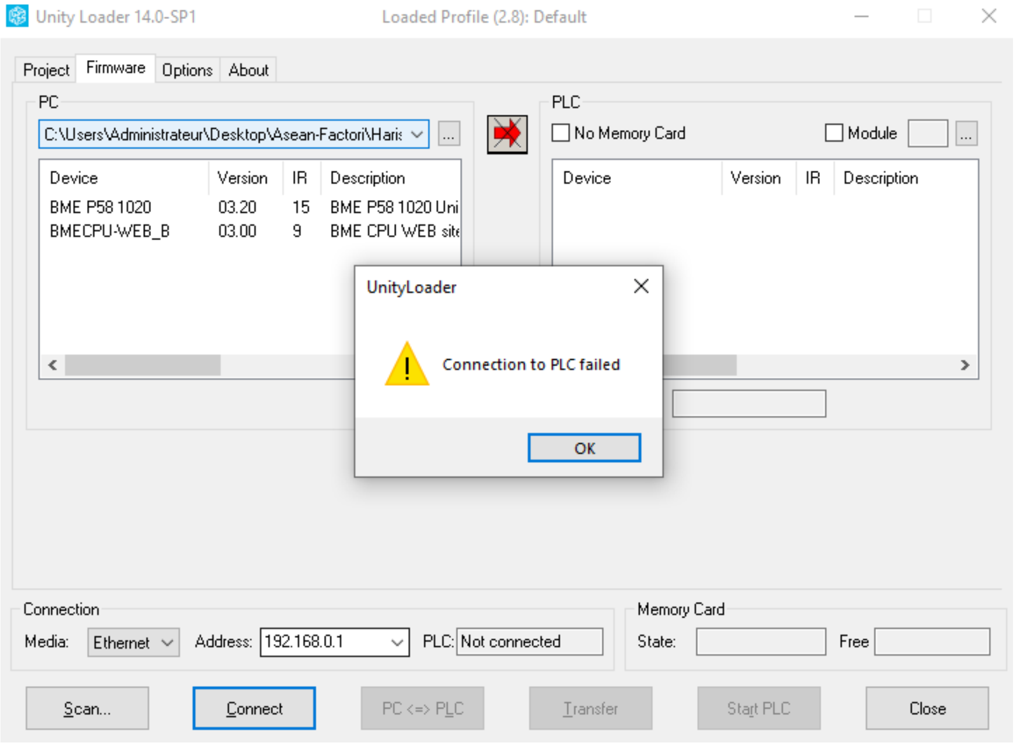
Name: Projet

Version: 0.0.25

Last Build: 28/04/2022 16:00:35

☑ PLC Run after Transfer

- Check that, from the Workstation, you are no longer able to connect to the M580 CPU via Unity Loader.


Unity Loader 14.0-SP1 Loaded Profile (2.8): Default

PC

C:\Users\Administrateur\Desktop\Asean-Factori\Haris

Device	Version	IR	Description
BME P58 1020	03.20	15	BME P58 1020 Uni
BMECPU-WEB_B	03.00	9	BME CPU WEB site

PLC

□ No Memory Card □ Module

Device	Version	IR	Description

UnityLoader

Connection to PLC failed

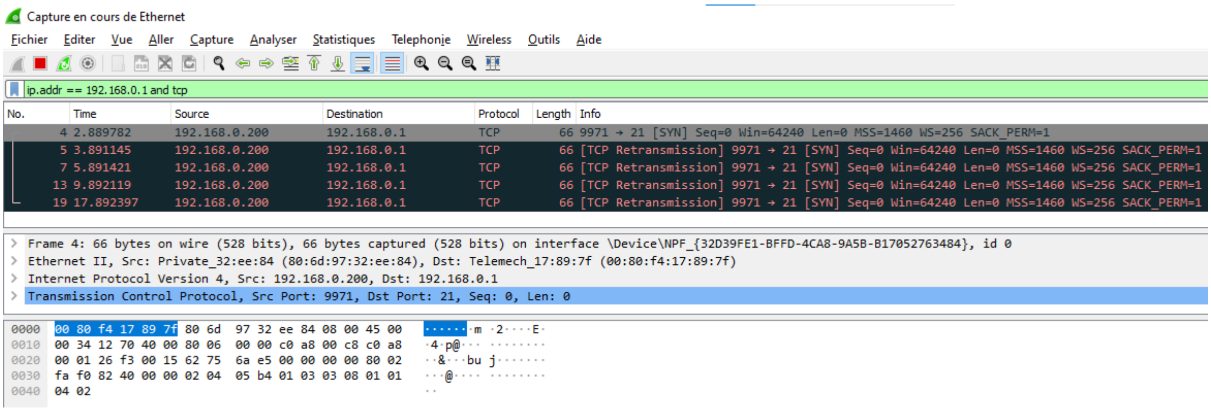
Connection

Media: Ethernet Address: 192.168.0.1 PLC: Not connected

Memory Card

State: Free

- Example of a Wireshark trace

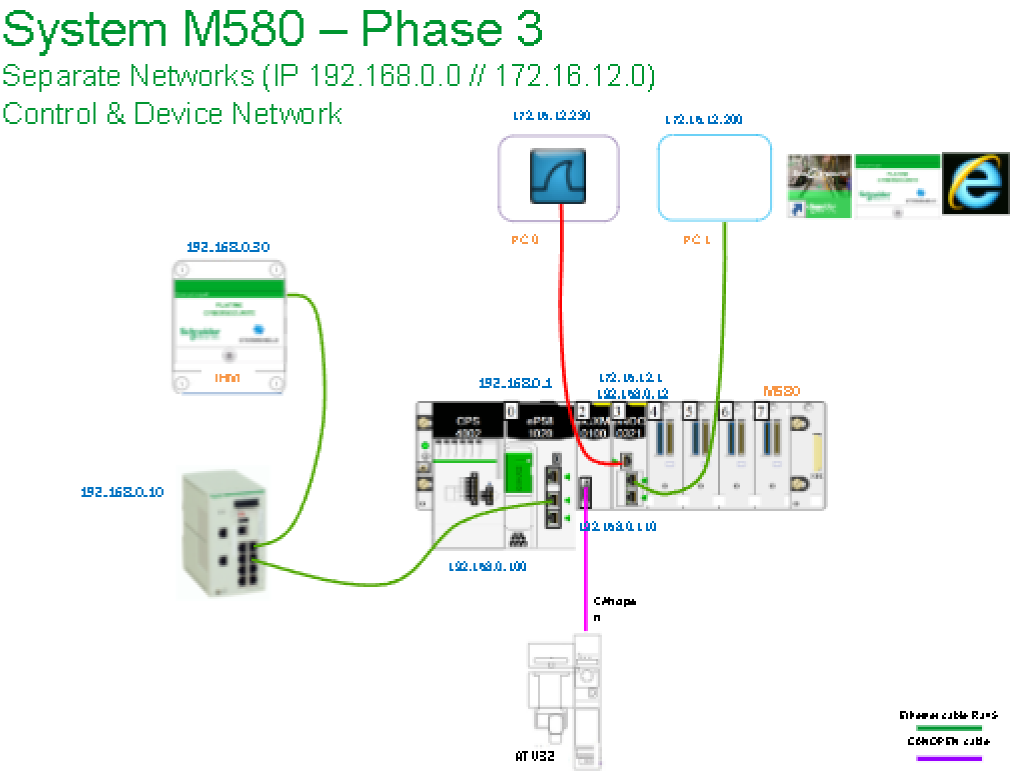

Capture en cours de Ethernet
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

```
ip.addr == 192.168.0.1 and tcp

No.  Time          Source          Destination    Protocol  Length  Info
   4 2.889782      192.168.0.200   192.168.0.1    TCP       66 9971 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   5 3.891145      192.168.0.200   192.168.0.1    TCP       66 [TCP Retransmission] 9971 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
   7 5.891421      192.168.0.200   192.168.0.1    TCP       66 [TCP Retransmission] 9971 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  13 9.892119      192.168.0.200   192.168.0.1    TCP       66 [TCP Retransmission] 9971 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
  19 17.892397     192.168.0.200   192.168.0.1    TCP       66 [TCP Retransmission] 9971 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1

> Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{32D39FE1-BFFD-4CA8-9A5B-B17052763484}, id 0
> Ethernet II, Src: Private_32:ee:84 (80:6d:97:32:ee:84), Dst: Telemech_17:89:7f (00:80:f4:17:89:7f)
> Internet Protocol Version 4, Src: 192.168.0.200, Dst: 192.168.0.1
> Transmission Control Protocol, Src Port: 9971, Dst Port: 21, Seq: 0, Len: 0

0000  00 80 f4 17 89 7f 80 6d  97 32 ee 84 08 00 45 00   ······m ·2····E·
0010  00 34 12 70 40 00 80 06  00 00 c0 a8 00 c8 c0 a8   ·4·p@··· ········
0020  00 01 26 f3 00 15 62 75  6a e5 00 00 00 00 80 02   ··&···bu j·······
0030  fa f0 82 40 00 00 02 04  05 b4 01 03 03 08 01 01   ···@···· ········
0040  04 02                                              ··
```

We check that we oscillate between requests for synchronization and retransmission issued by the Workstation; but that the automaton does not respond to these requests.

7. Architecture components Phase 3

- Identification and commentary on the components of the target architecture (Phase 3)


System M580 – Phase 3

Separate Networks (IP 192.168.0.0 // 172.16.12.0)

Control & Device Network

8. Installation of Ethernet cables according to the architecture Phase 3

9. Modification and verification of new IP addresses

9.1. Workplace

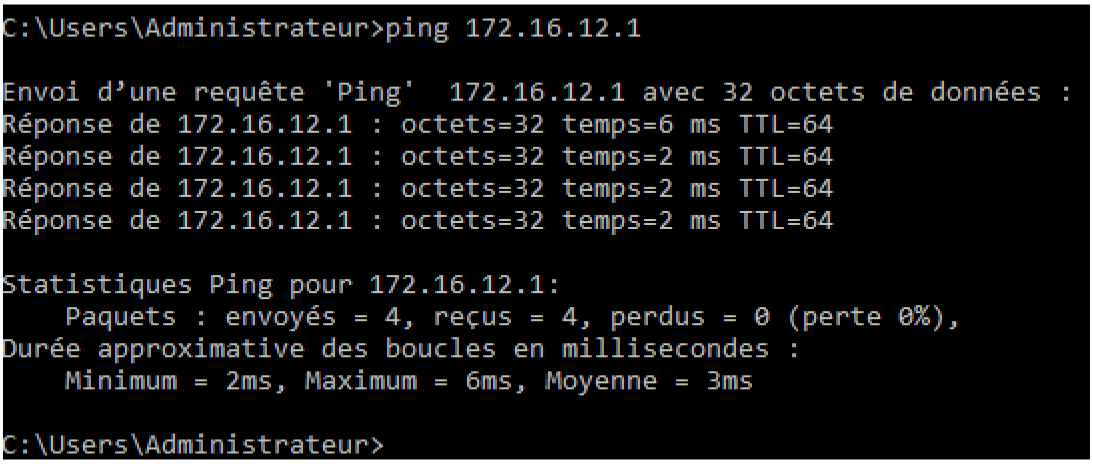
- To find out which routes have been previously defined on the Workstation, view them with the command **route PRINT**
- If necessary, run a route DELETE command to remove the routing used so far, before changing the IP address of the PC, and declaring a new routing

  ex : **route DELETE** 192.168.0.0

- Record the new Workstation address (172.16.12.200) Check via **IPCONFIG**
- Issue the **route** command designating the 'external' address of the NOC coupler (172.16.12.1) as the entry point to the Device Network (192.168.0.0)

  Route ADD 192.168.0.0 mask 255.255.255.0 172.168.12.1

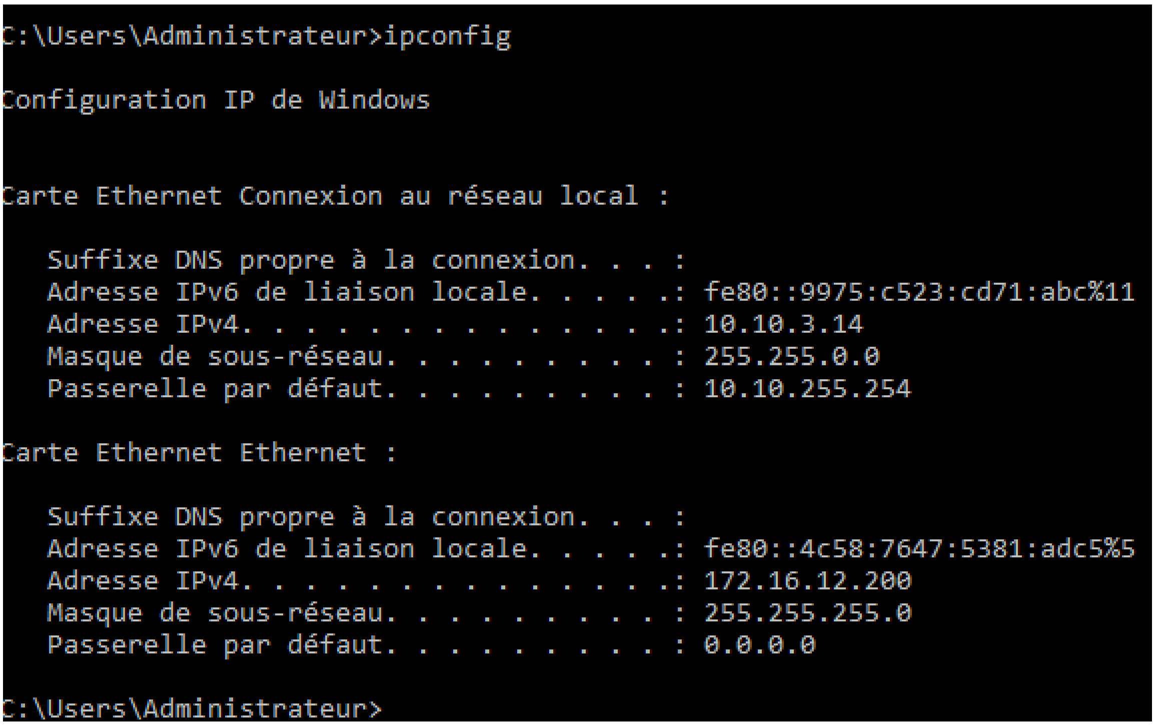
- Check the accessibility of the main address of the M580 CPU (**PING**)



```
C:\Users\Administrateur>ping 172.16.12.1

Envoi d’une requête 'Ping'  172.16.12.1 avec 32 octets de données :
Réponse de 172.16.12.1 : octets=32 temps=6 ms TTL=64
Réponse de 172.16.12.1 : octets=32 temps=2 ms TTL=64
Réponse de 172.16.12.1 : octets=32 temps=2 ms TTL=64
Réponse de 172.16.12.1 : octets=32 temps=2 ms TTL=64

Statistiques Ping pour 172.16.12.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 6ms, Moyenne = 3ms

C:\Users\Administrateur>
```

9.2. Observation post (frame capture)

- Logging of the new Observation Station address (172.16.12.230)
  Verification via **IPCONFIG**



```
C:\Users\Administrateur>ipconfig

Configuration IP de Windows


Carte Ethernet Connexion au réseau local :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::9975:c523:cd71:abc%11
   Adresse IPv4. . . . . . . . . . . . . .: 10.10.3.14
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : 10.10.255.254

Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::4c58:7647:5381:adc5%5
   Adresse IPv4. . . . . . . . . . . . . .: 172.16.12.200
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 0.0.0.0

C:\Users\Administrateur>
```

10. Verification of service availability of Modbus/TCP, HTTP and FTP protocols by the CPU through the BME NOC 0321 coupler

Note:

When requested on its IP address via a protocol for which it has its own resource, the BME NOC 0321 coupler responds with respect to this resource. Thus, when requested through HTTP or FTP protocols, the coupler responds by displaying its web pages and giving access to its firmware, respectively.

On the other hand, if the BME NOC 0321 coupler is requested via a protocol for which it does not have its own resource, as this is carried by the CPU, it responds with regard to this CPU resource. Thus, when requested via the Modbus/TCP protocol, the coupler responds by giving access to the application database.

In any case, the manipulations envisaged below will be limited to soliciting the main address of the M580 CPU, through the BME NC 0321 NOC router module. There will be no question of directly requesting its resources (e.g. HTML pages or coupler firmware).

Replay the previous chapter 4 in the present context:

- Check the accessibility of the ePAC (main address) for Modbus/TCP requests issued by by Vijeo Designer in Simulation Mode
- Verify access to HTML pages served by the M580 CPU (HTTP protocol)
- Check access to the M580 CPU FW download service (FTP protocol)

11. Selective inhibition, by configuration, of the CPU's HTTP and FTP services through the BME NOC 0321 coupler

Replaying the previous chapter 5 in the present context

- Access to HTML pages served by the M580 CPU (HTTP protocol)
- Access to the M580 CPU firmware download service (FTP protocol)

12. IP address filtering: Access control to the CPU through the BME NOC 0321 coupler

Replay the previous chapter 6 in the present context.

- Filtering on IP addresses in the Ethernet configuration on the CPU port :
  - without designated accessor
  - Modbus502 access
  - HTTP access
  - FTP access
- with designated accessor (global and then selective allocation of protocols)
  - Modbus502 access
  - HTTP access
  - FTP access